



**Universidad Austral de Chile**

Facultad de Ciencias de la Ingeniería

Escuela de Ingeniería Civil en Informática

DESARROLLO DE UN SOFTWARE PROTOTIPO DE  
MENSAJERÍA E INTERCAMBIO ELECTRÓNICO DE  
DOCUMENTOS PARA EL SERVICIO DE SALUD  
VALDIVIA

Tesis para optar al título de  
**Ingeniero Civil en Informática**

**PATROCINANTE:**

**MARTÍN SOLAR MONSALVES**

**CO-PATROCINANTE:**

**JUAN REYES DURAN**

**MARÍA VICTORIA SOTO MEZA**

VALDIVIA - CHILE

2005

Valdivia, 30 de Junio de 2005

**De** : Martín Gonzalo Solar Monsalves

**A** : Directora Escuela Ingeniería Civil en Informática

**Ref.** : Informe Calificación Trabajo de Titulación

**Nombre Trabajo de Titulación:**

"DESARROLLO DE UN SOFTWARE PROTOTIPO DE MENSAJERÍA E INTERCAMBIO ELECTRÓNICO DE DOCUMENTOS PARA EL SERVICIO DE SALUD DE VALDIVIA."

**Nombre Alumno:**

María Victoria Soto Meza.

**Evaluación:**

Cumplimiento del objetivo propuesto	7.0
Satisfacción de alguna necesidad	7.0
Aplicación del método científico	6.6
Interpretación de los datos y obtención de conclusiones	7.0
Originalidad	7.0
Aplicación de criterios de análisis y diseño	7.0
Perspectivas del trabajo	7.0
Coherencia y rigurosidad lógica	7.0
Precisión del lenguaje técnico en la exposición, composición, redacción e ilustración	7.0

**Nota Final** **7.0**

Sin otro particular, atte.:



Martín Solar Monsalves

VALDIVIA, julio 04 de 2005

DE : JUAN REYES DURAN  
JEFE DEPTO. SUBDIRECCIÓN RECURSOS HUMANOS

A : SRA. MIGUELINA VEGA R.  
DIRECTORA ESCUELA INGENIERÍA CIVIL EN INFORMÁTICA

MOTIVO: Informo a Ud. evaluación de Tesis , según lo indico a continuación:

Nombre Trabajo de Titulación: Desarrollo de un Software prototipo de Mensajería e Intercambio electrónico de documentos para el Servicio de Salud Valdivia

Nombre del Alumno : María Victoria Soto Meza

Nota : 7.0 (siete coma cero)

Saluda atentamente a Ud.,



~~JUAN REYES DURÁN  
JEFE DEPTO. SUBDIRECCIÓN R. HUMANOS~~

cc.: Archivo.

VALDIVIA, 28 DE AGOSTO DEL 2005

DE: GLADYS MANSILLA GOMEZ

A : DIRECTORA DE ESCUELA INGENIERIA CIVIL EN INFORMATICA

MOTIVO

INFORME TRABAJO DE TITULACION

Nombre Trabajo de Titulación: "DESARROLLO DE UN SOFTWARE PROTOTIPO DE MENSAJERIA E INTERCAMBIO ELECTRONICO DE DOCUMENTOS PARA EL SERVICIO DE SALUD VALDIVIA"

Nombre del alumno: MARÍA VICTORIA SOTO MEZA.

Nota: 7.0


( en números)

siete

(en palabras)

Fundamento de la nota:

- Este trabajo de tesis constituye una aplicación útil para quienes quieran implementar, un servicio de mensajería con algún nivel de seguridad.
- El tema de la firma electrónica viene a ser hoy en día una necesidad, por lo cual es meritorio que la alumna realicen avances en esta vía.
- En la realización de este trabajo de titulación se alcanzan plenamente los objetivos planteados al inicio.
- La presentación y redacción del informe están bien elaboradas, abarcando tópicos que inciden directamente en esta tesis y expresado en un lenguaje formal apropiado.
- La alumna ha sabido introducirse en un tema nuevo, estudiarlo e implementar una aplicación.
- Es también valorable que como producto de este trabajo, la alumna haya conseguido ser premiada entre las mejores 12 tesis nacionales en nuevas tecnologías de informática y comunicaciones ( TIC,s )



---

GLADYS MANSILLA GÓMEZ  
DOCENTE INSTITUTO DE INFORMATICA

Este trabajo de titulación, fue finalista en el concurso "*Tesis Digitales Otoño 2004*", organizado por Fundación País Digital, el portal de los universitarios "Universia" y el Banco Santander Santiago, donde recibe Beca de Financiamiento.

## **AGRADECIMIENTOS**

*Quiero agradecer al Profesor Martín Solar, profesor patrocinante, por su constante motivación y orientación durante el desarrollo de este trabajo de tesis.*

*Al Sr. Juan Reyes profesor co-patrocinante por permitir el desarrollo de este proyecto en el Servicio de Salud Valdivia.*

*A mis amigos por su constante preocupación para que este proyecto concluyera con éxito.*

*Quiero agradecer en forma especial a mis Padres y Hermanas por su incondicional apoyo, cariño y paciencia.*

## INDICE DE CONTENIDO

<b>INDICE DE CONTENIDO</b>	<b>4</b>
<b>INDICE DE FIGURAS</b>	<b>6</b>
<b>INDICE DE TABLAS</b>	<b>7</b>
<b>RESUMEN</b>	<b>8</b>
<b>SUMMARY</b>	<b>10</b>
<b>CAPITULO1 INTRODUCCION</b>	<b>12</b>
<b>1.1. ANTECEDENTES GENERALES</b>	<b>12</b>
<b>1.2. OBJETIVOS DEL PROYECTO</b>	<b>14</b>
1.2.1. OBJETIVO GENERAL	14
1.2.2. OBJETIVOS ESPECÍFICOS	14
<b>1.3. METODOLOGÍA</b>	<b>15</b>
1.3.1. FASES METRICA VERSION3	17
<b>1.4. DEFINICIONES</b>	<b>21</b>
1.4.1. GROUPWARE	21
1.4.2. CRIPTOGRAFIA Y FIRMA ELECTRONICA	23
1.4.2.1. Criptografía	24
1.4.2.2. Firma electrónica	27
<b>CAPITULO 2 ANÁLISIS DE TECNOLOGÍA DE IMPLEMENTACIÓN</b>	<b>30</b>
<b>2.1. TECNOLOGIA IBM</b>	<b>31</b>
<b>2.1.1. LOTUS NOTES 5.0</b>	<b>31</b>
2.1.1.1. Comunicación	32
2.1.1.2. Colaboración	33
2.1.1.3. Coordinación	35
2.1.1.4. Descripción general	36
2.1.1.5. Hardware necesario	38
<b>2.2. TECNOLOGIA MICROSOFT</b>	<b>40</b>
<b>2.2.1. MICROSOFT EXCHANGE 2000</b>	<b>40</b>
2.2.1.1. Comunicación	41
2.2.1.2. Colaboración	41
2.2.1.3. Coordinación	43
2.2.1.4. Descripción general	43
2.2.1.5. Hardware necesario	46
<b>2.3. TECNOLOGIA GNU</b>	<b>47</b>
<b>2.3.1. DEFINICIÓN OPENSOURCE</b>	<b>47</b>
<b>2.3.2. Licencia pública general</b>	<b>47</b>
<b>2.3.3. eGroupware</b>	<b>49</b>
2.3.3.1. Comunicación	50
2.3.3.2. Colaboración	50
2.3.3.3. Coordinación	51
2.3.3.4. Descripción general	51
2.3.3.5. Hardware necesario	52
<b>2.3.4. OpenGroupware</b>	<b>53</b>
2.3.4.1. Comunicación	55
2.3.4.2. Colaboración	56
2.3.4.3. Coordinación	57
2.3.4.4. Descripción general	57
2.3.4.5. Harware Necesario	62
<b>2.4. METODOLOGÍA SELECCIÓN DE LA MEJOR ALTERNATIVA</b>	<b>63</b>
<b>2.4.1. CARACTERÍSTICAS DEL PRODUCTO SELECCIONADO</b>	<b>68</b>

<b>CAPITULO 3 ANALISIS DE TECNOLOGIA IMPLEMENTACION DE FIRMA ELECTRONICA</b>	<b>72</b>
3.1. ASPECTO LEGAL	72
3.2. HERRAMIENTAS DE SEGURIDAD	73
3.2.1. GnuPG y PGP	74
3.2.2. INFRAESTRUCTURA DE CLAVES PÚBLICAS	76
3.2.2.1. La Autoridad Certificadora	78
3.2.2.2. Certificados Digitales	79
3.3. SELECCIÓN DE TECNOLOGÍA FIRMA ELECTRÓNICA	82
3.3.1. CREACIÓN DE UNA AUTORIDAD CERTIFICADORA Y CERTIFICADOS CLIENTES	84
<b>CAPITULO 4 DISEÑO E IMPLEMENTACION DEL PROTOTIPO</b>	<b>88</b>
4.1. IMPLEMENTACIÓN	88
4.1.1. MODELO	88
4.1.2. ARQUITECTURA	91
4.1.3. SOLUCIONES TECNOLÓGICAS	92
4.2. POLÍTICAS DE RESPALDO DE INFORMACIÓN	93
4.3. SEGURIDAD E INTEGRIDAD DEL SISTEMA	95
4.3.1. SEGURIDAD EN EL USO DE CERTIFICADOS DIGITALES	95
4.3.3. SEGURIDAD SECURE SOCKET LAYER	98
<b>CAPITULO 5 DESCRIPCION FUNCIONAMIENTO</b>	<b>101</b>
5.1. DESCRIPCION	101
<b>CAPITULO 6 CONCLUSIONES Y MEJORAS</b>	<b>109</b>
6.1. CONCLUSIONES	109
6.2. MEJORAS	109
<b>CAPITULO 7 BIBLIOGRAFIA</b>	<b>110</b>
7.1. LIBROS Y PUBLICACIONES	110
7.2. DIRECCIONES INTERNET	112
<b>ANEXO A MANUAL DE INSTALACION OGo</b>	<b>113</b>
<b>ANEXO B MANUAL DE OGO</b>	<b>119</b>
<b>ANEXO C Firmar y Encriptar un mensaje con la herramienta Win PT</b>	<b>133</b>



## INDICE DE FIGURAS

Figura N°1: Encriptación Simétrica. _____	25
Figura N°2: Encriptación Asimétrica. _____	26
Figura N°3: Mecanismo de Firma Electrónica. _____	27
Figura N°4: Arquitectura Groupware -.Skyrix. _____	58
Figura N°5: Arquitectura Instalación OpenGrouware _____	91
Figura N°6: Acceso a OGo, _____	101
Figura N°7: Visor de preferencias de un usuario _____	102
Figura N°8: Visor de noticias, para el usuario _____	102
Figura N°9: Listado de proyectos _____	103
Figura N°10: Detalle de un proyecto seleccionado, opción documento _____	103
Figura N°11: Detalle de un proyecto seleccionado, opción tareas _____	104
Figura N°12: Visor de personas, detalle de una cuenta de usuario _____	104
Figura N°13: Listado de citas del usuario(Agenda Compartida) _____	105
Figura N°14: Listado de trabajos del usuario _____	105
Figura N°15: Visor de correo electrónico del usuario _____	106
Figura N°17: Detalle certificado _____	107
Figura N°18: Correo Firmado electrónicamente, con M. Outlook Express _____	108
Figura N°19: Correo Cifrado electrónicamente, con M. Outlook Express _____	108

## INDICE DE TABLAS

Tabla N°1: Efectividad _____	64
Tabla N°2: Plataforma Tecnológica_____	64
Tabla N°3: Calidad técnica de la solución _____	65
Tabla N°4: Ahorro de costos operacionales_____	65
Tabla N°5: Evaluación de alternativas _____	66
Tabla N°6: Conectores para OGo _____	69
Tabla N°7: Funcionalidades de OGo _____	70
Tabla N°8: Distribución de grupos _____	90

## RESUMEN

El desarrollo de tecnologías informáticas del tipo Groupware ha impulsado el desarrollo del trabajo en grupo de forma eficaz, la posibilidad de compartir la información disponible, así como trabajar simultáneamente desde diferentes puestos de trabajo. Permite disminuir los tiempos de trabajo y los costos en forma considerable y además permite optimizar la toma de decisiones.

El desarrollo de aplicaciones basadas en este concepto, permite compartir e impulsar el conocimiento a través de la organización, así como automatizar los procesos estructurados y predefinidos existentes en la empresa.

El objetivo de este trabajo de titulación es implementar un sistema informático, a nivel de prototipo, para apoyar la gestión de mensajería electrónica y el intercambio electrónico de documentos en el Servicio de Salud de Valdivia. Para ello, se utilizarán tecnologías de gestión electrónicas del tipo Groupware, que operen a través de Internet para una mayor utilización por parte de los usuarios, con el fin de mejorar la comunicación entre los miembros de un grupo de trabajo e incrementar la productividad de los mismos, en especial para aquellos grupos distantes físicamente entre Hospitales y Consultorios de la Zona. También se facilitará la recuperación y el acceso a la información, reduciendo en forma considerable los tiempos de recepción y despacho de información.

Como elemento de seguridad y confidencialidad en los correos electrónicos se incorporará la firma electrónica.

El software a utilizar es Opengrouware, de tipo GNU/Linux, el cual cumple con las características de Groupware. Para la generación de la firma electrónica se utilizarán certificados digitales.

Finalmente, con el desarrollo del prototipo se busca liderar en el sector salud, la utilización de documentación y firma electrónica; de tal manera, de establecer las bases que permitan replicar este modelo en otros establecimientos de salud.

## SUMMARY

The development computer science technologies of the type Groupware, impelled the development of the work in group of effective form, the possibility of sharing the information available, as well as of working simultaneously from different work places. It allows to diminish the working times and the costs in considerable form and in addition allow to optimize the decision making

The development of applications based on this concept, allows to share and to impel the knowledge through the organization, as well as to automate the processes structured and predefined existing in the company.

The objective of this work of degree is implement a computer science system, at prototype level, to support the management of electronic messaging and the electronic document interchange, in the Service of Health. For it, electronic technologies of management such as Groupware were used, that they operate through Internet, for a greater use on the part of the users, with the purpose of improving the communication between the members of a work group and increasing the productivity of such, in special for those distant groups between Hospitals and Doctor's offices of the Zone. Also one will facilitate the recovery and the access to the information, reducing in considerable form the times of reception and shipment of information.

As element of security and confidentiality in the electronic mails got up the electronic company/signature.

Software to use is Opengrouware, of GNU/Linux type and fulfills the characteristic of Groupware. For the generation of electronic company/signature digital certificates were used.

Finally, with the development of the prototype one looks for to lead in the sector health, the use of documentation and electronic company/signature; of

such way, to establish the bases that allow to talk back this model in other establishments of health.

## **CAPITULO1 INTRODUCCION**

### **1.1. ANTECEDENTES GENERALES**

El Servicio de Salud se compone de una Dirección de Servicio ubicada en la ciudad de Valdivia; 7 hospitales dependientes, situados en las ciudades de: Valdivia, La Unión, Río Bueno, Paillaco, Los Lagos, Lanco y Corral; 2 hospitales particulares en convenio, localizados en las ciudades de San José de la Mariquina y Panguipulli; 6 consultorios periféricos urbanos; 6 consultorios periféricos rurales; 57 postas rurales, y 73 estaciones de salud rural.

Actualmente no existe en el Servicio de Salud Valdivia herramientas computacionales que permitan la gestión electrónica de documentos y utilización de la firma electrónica.

Lo que realmente existe es un servidor de correo para el servicio de correo electrónico.

Las reuniones son realizadas con la asistencia de los miembros de los grupos de trabajo, estas son necesarias para la toma de decisiones.

Esta forma de trabajo tiene sus desventajas porque reunir el grupo requiere de tiempo y dinero para que todos estén disponibles en el día y hora fijada, tiempo para coordinar las agendas de los participantes y dinero ya sea en gastos en desplazamientos.

Además de los problemas que surgen durante la celebración de reuniones, en ocasiones no hay tiempo para que todos hablen, o la falta de participación, se pueden tomar decisiones arriesgadas o por compromiso, en intercambiar ideas pueden ser necesarias varias reuniones lo que dificulta la toma de decisiones a tiempo.

De esta forma nace la necesidad de implementar un sistema informático que permita una comunicación estrecha y oportuna entre las personas, de manera que puedan compartir información, reducir los tiempos en la toma de decisiones y así mejorar la productividad. También aplicar tecnologías que integren el correo electrónico, las agendas para programar juntas y eventos y que opere a través de Internet.

Se plantea la utilización de firma electrónica como método de comunicación segura para la circulación de documentos, restringiendo accesos no autorizados, identificando a su firmante e impidiendo la alteración del contenido

Describir la implantación de una herramienta Groupware para que mejore la comunicación entre los miembros del grupo de trabajo e incremente la productividad de los mismos.



## **1.2. OBJETIVOS DEL PROYECTO**

### **1.2.1. OBJETIVO GENERAL**

El objetivo general es diseñar e implementar un sistema informático, a nivel de prototipo, para apoyar la gestión de mensajería electrónica y el intercambio electrónico de documentos.

### **1.2.2. OBJETIVOS ESPECÍFICOS**

Para el logro del objetivo general se consideran los siguientes objetivos específicos:

- Investigación, análisis y evaluación de tecnologías relacionadas.
- Diseño y adaptación de un sistema de mensajería y de la arquitectura de comunicaciones del sistema.
- Incorporar la generación y administración de documentos electrónicos.
- Incorporar la firma electrónica como elemento de autenticación.
- Controlar aspectos de seguridad e integridad aplicadas al sistema.

### 1.3. METODOLOGÍA

La metodología empleada para la implantación del prototipo es Métrica Versión 3, abarcando las siguientes fases [URL2]:

- Fase 0: Planificación de sistemas de información (PSI)
- Fase 1: Desarrollo de sistemas de información
  - Fase 1.1: Estudio de viabilidad del sistema (EVS)
  - Fase 1.2 Análisis del sistema (ASI)
  - Fase 1.3 Diseño del sistema (DSI)
  - Fase 1.4 Construcción del sistema (CSI)
  - Fase 1.5 Implantación y aceptación del sistema (ISA)
- Fase 2: Mantenimiento del sistema de información (MSI)

La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software dentro del marco que permite alcanzar los siguientes objetivos:

- Proporcionar o definir Sistemas de Información que ayuden a conseguir los fines de la organización mediante la definición de un marco estratégico para el desarrollo de los mismos.
- Dotar a la Organización de productos software que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos.
- Mejorar la productividad de los departamentos de Sistemas y Tecnologías de la Información y las Comunicaciones, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible.

- Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de software a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos.
- Facilitar la operación, mantenimiento y uso de los productos software obtenidos.

La necesidad de acortar el ciclo de desarrollo de los sistemas de información ha orientado a muchas organizaciones a la elección de productos software del mercado. Esta decisión, que es estratégica en muchas ocasiones para una organización, debe tomarse con las debidas precauciones, y es una realidad que está cambiando el escenario del desarrollo del software.

METRICA Versión 3 facilita la toma de decisión y la realización de todas las tareas que comprende el desarrollo de un sistema de información.

### **1.3.1. FASES METRICA VERSION3**

#### **Fase 0: Plan de sistemas de información**

Para la elaboración del Plan de Sistemas de Información se estudian las necesidades de información de los procesos de la organización afectados por el Plan, con el fin de definir los requisitos generales y obtener modelos conceptuales de información. Por otra parte se evalúan las opciones tecnológicas y se propone un entorno.

Se elabora un calendario de proyectos con una planificación lo más detallada posible de los más inmediatos. Además, se propone una sistemática para mantener actualizado el Plan de Sistemas de Información para incluir en él todos los cambios necesarios, garantizando el cumplimiento adecuado del mismo.

Para el desarrollo de un sistema aislado, cuya necesidad no se derive de un Plan de Sistemas, no se utilizará la Fase 0 de la Metodología.

#### **Fase 1: Desarrollo de sistemas de información**

El proceso de Desarrollo de MÉTRICA Versión 3 contiene todas las actividades y tareas que se deben llevar a cabo para desarrollar un sistema, cubriendo desde el análisis de requisitos hasta la instalación del software.

- **Fase 1.1: Estudio de viabilidad**

El propósito de este proceso es analizar un conjunto concreto de necesidades, con la idea de proponer una solución a corto plazo.

Los resultados del Estudio de Viabilidad del Sistema constituirán la base para tomar la decisión de seguir adelante o abandonar. Se ha considerado que este proceso es obligatorio, aunque el nivel de profundidad con el que se lleve a cabo dependerá de cada caso. En las alternativas se considerarán soluciones "a medida", soluciones basadas en la adquisición de productos software del

mercado o soluciones mixtas. Se evaluaron diferentes tecnologías, Lotus, Exchange, eGroupware y OpenGroupware.

- **Fase 1.2: Análisis del sistema**

Una vez seleccionada la alternativa, se generan las especificaciones formales que describan al sistema y que deben ser aprobadas por el usuario.

Se planifican y se realizan las entrevistas necesarias con los usuarios para obtener una descripción general del funcionamiento actual del sistema. De esta forma, se podrán identificar los problemas existentes en la actualidad definiendo los requisitos que tiene que cumplir el sistema.

Revisión de la forma de trabajar en grupo, que se realiza actualmente y como se pretende mejorar al aplicar un software Groupware y firma electrónica.

- **Fase 1.3: Diseño del sistema de información**

El propósito es obtener la definición de la arquitectura del sistema y del entorno tecnológico que le va a dar soporte, junto con la especificación detallada de los componentes del sistema de información. A partir de dicha información, se generan todas las especificaciones de construcción relativas al propio sistema, así como la especificación técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial, éstos últimos cuando proceda.

Se define la arquitectura de la solución, y para la implantación de firma electrónica, la utilización de Microsoft Outlook Express y certificados digitales.

- **Fase 1.4: Construcción del sistema**

Tiene como objetivo final la construcción y prueba de los distintos componentes del sistema, a partir del conjunto de especificaciones lógicas y físicas del mismo, obtenido en el Proceso de Diseño del Sistema de Información. Se desarrollan los procedimientos de operación y seguridad y se elaboran los manuales de usuario.

- **Fase 1.5: Implantación y aceptación del sistema**

Este proceso tiene como objetivo principal, la entrega y aceptación del sistema en su totalidad, que puede comprender varios sistemas de información desarrollados de manera independiente y un segundo objetivo que es llevar a cabo las actividades oportunas para el paso a producción del sistema.

Para el inicio de este proceso se toman como punto de partida los componentes del sistema probados de forma unitaria e integrados en el proceso Construcción del Sistema de Información, así como la documentación asociada.

El Sistema se someterá a las Pruebas de Implantación con la participación del usuario cuya responsabilidad, entre otros aspectos, es comprobar el comportamiento del sistema bajo las condiciones más extremas.

**Fase 2: Mantención del sistema de información**

El objetivo de este proceso es la obtención de una nueva versión de un sistema de información desarrollado con MÉTRICA, a partir de las peticiones de mantenimiento que los usuarios realizan con motivo de un problema detectado en el sistema o por la necesidad de una mejora del mismo.

Como consecuencia de esto, sólo se considerará en MÉTRICA Versión 3 los tipos de Mantenimiento Correctivo y Evolutivo. Se excluyen los tipos de Mantenimiento Adaptativo y Perfectivo, que abarcan actividades tales como la migración y la retirada de software que precisarían el desarrollo de un tipo de metodología específica.

## **Tipos de Mantenimiento**

- *Correctivo*: Son aquellos cambios precisos para corregir errores del producto software.
- *Evolutivo*: Son las incorporaciones, modificaciones y eliminaciones necesarias en un producto software para cubrir la expansión o cambio en las necesidades del usuario.
- *Adaptativo*: Son las modificaciones que afectan a los entornos en los que el sistema opera, por ejemplo, cambios de configuración del hardware, software de base, gestores de base de datos, comunicaciones, etc.
- *Perfectivo*: Son las acciones llevadas a cabo para mejorar la calidad interna de los sistemas en cualquiera de sus aspectos: reestructuración del código, definición más clara del sistema y optimización del rendimiento y eficiencia.

En este caso, para el software OpenGroupware (OGo) se considera un tipo de mantenimiento evolutivo, a futuro se pretende incorporar la firma electrónica y que los correos sean emitidos firmados electrónicamente, directamente desde la interfaz de correo de OGo,(sobre Web) sin la necesidad de utilizar un cliente de correo como Microsoft Outlook Express.

## 1.4. DEFINICIONES

### 1.4.1. GROUPWARE

El desarrollo de nuevas tecnologías de informática, ha impulsado el desarrollo del trabajo en equipo, la posibilidad de compartir la información disponible, así como trabajar simultáneamente desde diferentes puestos de trabajo, esta acortando en forma considerable, los costos y los tiempos de trabajo.

La utilización y desarrollo de herramientas de software que apoyen estas formas de trabajo, conlleva necesariamente a un cambio cultural de la organización

El Groupware es un tipo de software colaborativo que apoya a grupos de trabajo a realizar sus actividades a través de una red. Estas aplicaciones aportan poco o casi nada cuando se utiliza en modalidad monousuaria ya que apoyar el trabajo colaborativo implica aumentar la productividad grupal, pero no debe sacrificar la productividad individual, deben facilitar una amplia comunicación para los miembros del grupo, independiente de la ubicación física o de la plataforma computacional que se esté usando.

Debido a esto los Groupware deben proporcionar tres funciones esenciales

- **La comunicación:** Es la función más importante del Groupware, ya que es el medio en que la información es compartida. Los miembros de un grupo de trabajo necesitan comunicarse para intercambiar información. En la comunicación se encuentran el correo electrónico y la mensajería instantánea.
- **La colaboración:** Mediante el intercambio de información, los miembros del grupo pueden tomar decisiones, combinar opiniones y generar documentación en forma conjunta. Proporciona la ventaja de resolver problemas de reuniones



tradicionales como, lugar y tiempo para la realización de la misma o la disponibilidad de información, ya que proporciona un espacio de trabajo virtual.

En la colaboración se encuentran las conferencias y las bases de datos compartidas.

- **La coordinación:** Es la acción de asegurar que el equipo esta trabajando eficientemente y en conjunto para alcanzar una meta. Esto incluye la distribución de tareas y revisión de su ejecución. En la coordinación, los Workflows o cualquier otra aplicación que permita el seguimiento y revisión de trabajos.

Estas tres funciones esenciales unidas permiten que la información fluya más rápidamente, y con precisión, existen menos barreras entre cada departamento, se mejora la toma de decisiones. Para lograr todo esto es necesario contar con una Intranet o una conexión a Internet y poder comunicar las máquinas clientes con el servidor de las aplicaciones Groupware [Cer97].

## 1.4.2. CRIPTOGRAFIA Y FIRMA ELECTRONICA

Internet es por naturaleza un medio de comunicación no seguro, por lo que es de especial importancia establecer ciertos criterios de protección y seguridad en el envío y recepción de la información.

En ocasiones es necesario que dicho mensaje solo pueda ser interpretado correctamente por el emisor y a quien va dirigido, el receptor, siendo imposible la interceptación por terceros del mensaje, o que si se produce ésta, el mensaje capturado sea incomprensible para quien tenga acceso a él.

En la transferencia de información hay que considerar varios aspectos para lograr una comunicación segura [URL3]:

1. *Autenticidad*: Consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser. El método más usado para proporcionar autenticidad es la firma digital, basada, en la criptografía.
2. *Confidencialidad*: Se trata de la seguridad de que los datos que contiene el documento permanecen ocultos para terceras personas durante su viaje por el medio desde A a B.
3. *Integridad*: Consiste en la seguridad de que los datos del documento no sufren modificación a lo largo de su viaje por el medio inseguro desde A a B. La comprobación de la integridad se suele realizar mediante firmas electrónicas, generalmente basadas en funciones Hash. La Autenticidad es condición suficiente para la Integridad, por lo que si un documento es auténtico es integro, pero no al revés.
4. *No repudio*: Se trata de que una vez enviado un documento por A, éste no pueda negar haber sido el autor de dicho envío. El No repudio es condición suficiente para la Autenticidad, por lo que si un documento es no repudiable es auténtico, pero no al revés.

#### **1.4.2.1. Criptografía**

La criptografía es la técnica de transformar un mensaje inteligible, denominado texto en claro, en otro que sólo puedan entender las personas autorizadas a ello, denominado criptograma o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina algoritmo de encriptación.

Con la aparición de los computadores, se desarrollaron nuevos métodos de encriptación que basan su funcionamiento en la utilización de potentes y complejas herramientas de hardware como de software. Utilizan también claves secretas de gran longitud para controlar una compleja secuencia de operaciones, que pueden incluir tanto transposiciones como sustituciones de los datos.

Dentro de los sistemas criptográficos actuales se encuentran, los de clave simétrica y los de clave asimétrica.

Ambos tienen características bien diferenciadas, lo que permite su uso para diferentes fines, de hecho ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr la mayoría de los objetivos de seguridad.

## Criptografía Simétrica

La criptografía simétrica o de clave privada se caracteriza porque el emisor y receptor del mensaje utilizan la misma clave para encriptar y para desencriptar, el mensaje.

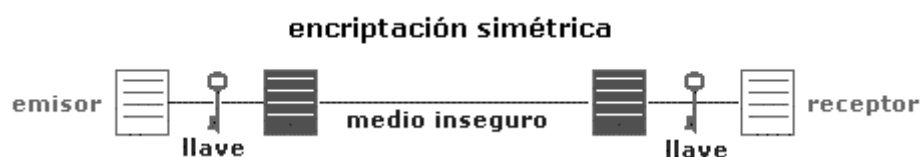


Figura N°1: Encriptación Simétrica.

Para mantener la efectividad de este sistema de encriptación es necesario, que la clave privada sea mantenida en secreto por el emisor y receptor. Si esta llave cae en manos de terceros el sistema deja de ser seguro por lo que es necesario desechar dicha llave y generar una nueva.

Este sistema permite la confidencialidad y la autenticidad, solo si la clave es conocida por el emisor y el receptor del mensaje.

Los principales algoritmos simétricos actuales son *DES*, *IDEA*, *AES* y *RC5*.

## Criptografía Asimétrica

La criptografía asimétrica o de clave pública, se basa en el uso de dos claves diferentes, una clave puede desencriptar lo que la otra ha encriptado.

Generalmente una de las claves de la pareja, denominada *clave privada*, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada *clave pública*, es usada para desencriptar el mensaje cifrado.

Ambas claves, pública y privada, están relacionadas matemáticamente, siendo una la inversa de la otra, se generan siempre a la vez, por parejas, de tal forma

que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

La base de la seguridad del sistema es que el propietario debe mantener la clave privada en secreto y la clave pública difundirla ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

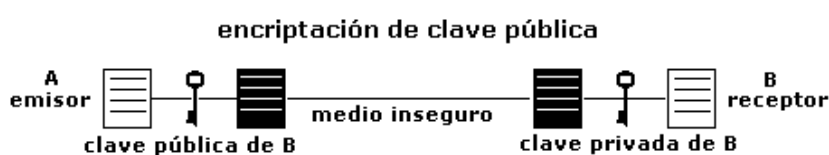


Figura N°2: Encriptación Asimétrica.

En la encriptación de clave pública, para enviar un documento con seguridad, el emisor (A) encripta el documento con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por (B). Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje original.

Este sistema permite garantizar la confidencialidad de la comunicación, pero no garantiza su autenticidad, dado que todos pueden tener acceso a la clave pública del receptor, por lo que cualquier usuario podría ser el emisor de un mensaje.

Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

Generalmente, y debido a la lentitud de proceso de los sistemas de llave pública, estos se utilizan para el envío seguro de claves simétricas, y las simétricas se usan para el envío de datos encriptados.

Los principales algoritmos Asimétricos actuales son *RSA*, *DSA* Y *ECC*.

### 1.4.2.2. Firma electrónica

Una firma electrónica es un conjunto de caracteres que acompaña a un documento, acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no repudio). De esta forma, el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

El mecanismo de firma electrónica es el siguiente [URL3]:



Figura N°3: Mecanismo de Firma Electrónica.

1. El emisor aplica una función Hash conocida al documento, con lo que obtiene un resumen Hash del mismo.
2. Encripta dicho resumen con su clave privada.
3. Envía al receptor el documento original plano y el resumen Hash encriptado.
4. El receptor B aplica la función Hash al resumen sin encriptar y descifra el resumen encriptado con la llave pública de A.

5. Si ambos coinciden, está seguro de que ha sido A, el que ha enviado el documento. Si no coinciden, está seguro de que no ha sido A o que el envío ha sido interceptado y modificado.

El caso de que ambos resúmenes no coincidan contempla también la posibilidad de que el mensaje haya sido alterado en su viaje de A a B, lo que conlleva igualmente el rechazo del documento por no válido.

Como la clave pública del emisor fue utilizada para descifrar la firma, el resumen debe haber sido cifrado con la clave privada correspondiente, conocida sólo por el emisor del mensaje (autenticidad). Además si la propiedad de las claves está certificada por un ente confiable, el emisor de un mensaje firmado con este esquema no puede desconocer su firma, ya que nadie salvo él podría haber generado el resumen cifrado con tal clave privada (No repudio).

### **Principales beneficios de la firma electrónica**

- Ya no será necesario desplazarse desde el lugar de trabajo o de la casa para realizar trámites que a veces requieren largas esperas, puesto que no se necesita desde ahora de la presencia física de las partes para la suscripción de acuerdos.
- Se abre paso a una multitud de nuevas formas de contratación de trámites públicos y privados que podrán realizarse digitalmente.
- Una vasta gama de trámites públicos y compras gubernamentales podrán efectuarse electrónicamente.
- Se fomenta la competitividad de las empresas pasando de usos simples a usos complejos. Constituye un impulso a la innovación.

## Funciones Hash

Las funciones Hash, son funciones matemáticas que realizan un resumen del documento a firmar. Su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real.

Las funciones de resumen deben poseer ciertas características para ser consideradas como tales [Val02]:

- Cualquier cambio en el mensaje, por mínimo que sea, debe producir un resumen distinto.
- Debe tener compresión, o sea a partir de un mensaje de cualquier longitud, el resumen debe tener una longitud fija y lo normal es que sea menor que la del mensaje.
- La función no debe poder invertirse, debe ser unidireccional para que impida obtener el mensaje original a través del resumen.
- Debe ser fácil y rápida de calcular.

Los algoritmos Hash no emplean claves de ningún tipo, sino que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud variable, o sea cada cierta cantidad de texto elegido de forma arbitraria se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra, esta palabra tiene una extensión de X bits preestablecidos, de esta forma el texto se hace irreconocible, al poder leer sólo números secuenciales que no guardan relación alguna entre si.



## CAPITULO 2 ANÁLISIS DE TECNOLOGÍA DE IMPLEMENTACIÓN

Se analizaron 4 productos desde la perspectiva de Groupware en sus tres funciones esenciales.

- *Comunicación*: Correo electrónico.
- *Colaboración*: Bases de información compartida, agendas, calendarios, tareas y proyectos.
- *Coordinación*: Flujos de trabajo (Workflow), o cualquier otra aplicación que si permita hacer consultas sobre determinado trabajo o seguimiento de una determinada tarea.

Se dió mayor énfasis en las herramientas GNU debido a que el Servicio de Salud es una institución pública, que no tiene presupuesto asignado para adquirir productos comerciales demasiados costosos.

Los productos son los siguientes

- Lotus Notes
- Microsoft Exchange
- Egroupware
- OpenGroupware

## 2.1. TECNOLOGIA IBM

### 2.1.1. LOTUS NOTES 5.0

Es un *software* para trabajo en grupo que permite crear, compartir y organizar documentos: textos, gráficos de presentación, imágenes escaneadas, sonido y vídeo. Combina las aplicaciones para Internet como correo electrónico, calendarios y agenda, administración de documentos personales y grupos de noticias, por medio de cualquier servidor Internet.

Es recomendable para el trabajo en equipo porque abarca tres puntos: *la comunicación, colaboración y coordinación*, el primer punto se cubre con sistemas de *correo electrónico*, que lo hace poder comunicarse de forma fácil y rápida con otras personas.

El segundo se basa en un sistema organizado de carpetas donde se almacena información y donde cualquiera puede leer y escribir *mensajes*, la existencia de las Bases de Datos, genera que sea sencillo compartir datos desde cualquier lugar. El último punto se lleva a cabo mediante *agendas electrónicas* donde se puede compartir la planificación diaria con los demás, se puede construir flujos de trabajo completamente controlados con Aplicaciones Workflows.

Es un entorno *Cliente/Servidor* para el desarrollo de aplicaciones de Trabajo en Grupo. Es considerado como una exclusiva y segura implementación de base de datos abierta y distribuida, ya que permite el acceso a bases de datos tanto locales como remotas. Su facilidad de su uso se basa en un entorno gráfico intuitivo adaptable al modo de trabajo del usuario.

Permite la comunicación de los usuarios independientemente de la plataforma que utilicen o el lugar donde se encuentren.

### **2.1.1.1. Comunicación**

- **Correo Electrónico**

El correo de Notes es una base de datos más dentro del sistema Notes. Su principal objetivo es el de servir de almacén y transmisor de los mensajes de correo. El correo Notes puede ser utilizado desde usuarios Notes o desde usuarios del Web.

El servidor POP3 de Notes habilita a sus servidores para distribuir correo a los usuarios de correo de POP3.

Por medio de la creación de carpetas y vistas personales, es posible ordenar y categorizar los correos, pueden ser creadas por los propios usuarios.

Es posible incorporar en los mensajes enlaces a documentos, vistas o base de datos, que se encuentran en el servidor. Se pueden establecer en los mensajes niveles de importancia, codificación, acuse de recibo y prioridades a los mensajes.

Los destinatarios del correo se pueden seleccionar a partir del Libro Público, donde se encuentran los usuarios, se puede utilizar la escritura anticipada de nombres.

Por medio de los agentes (*procesos que se ejecutan en el servidor*) permiten manipular y responder a correos cuando un usuario se encuentre fuera de la oficina.

### 2.1.1.2. Colaboración

- **Bases de información compartida**

En Lotus Notes es posible, visualizar y gestionar la información de forma sencilla y personalizable.

La Información se almacena en Bases de Datos Notes, estas se representan como iconos en el cliente Notes, los cuales son Correo, Agenda, Libreta de Direcciones y Tareas, y la podemos visualizar en los propios formularios o en vistas.

*Base de Datos:* Conjunto de documentos relacionados, los cuales son visibles a través de vistas y creados a partir de formularios definidos en la base de datos que puede ser local (almacenada en el PC) o compartida (almacenada en el Servidor Notes, que puede ser o no accesible a los usuarios)

Una base de datos de Notes contiene documentos relacionados con un área de interés. La mayoría de las bases de datos están diseñadas especialmente para un uso específico, pero en Notes se incluyen las bases de datos Correo, Marcadores, Navegadores de Web, y Direcciones.

Además con la integración del correo, hace fácil el envío de dicha información a otros usuarios.

Los elementos más importantes de la base de datos Notes son:

- *Formularios:* Definen la estructura de un documento. Pueden contener campos, textos, gráficos, etc.
- Documentos, donde introducimos, modificamos o visualizamos los datos.
- Vistas, muestra la información de los formularios de una forma ordenada, permitiendo acceder a los mismos [Cer97].

Para empezar a trabajar con las bases de datos tenemos que agregar sus iconos al Área de trabajo (*El área de trabajo está compuesto por hojas personalizadas por pestañas, donde se ubicarán los iconos de las bases de datos.*)

Cada una de las bases de datos se encuentran en uno o más servidores Notes y pueden ser accesadas por los usuarios previamente definidos en la lista de control de acceso a la información.

La generación de índices sobre una base de datos permite, por medio de una barra de búsqueda, encontrar información en forma rápida.

Se puede realizar búsqueda de texto en documentos y en vistas y búsqueda rápida en vistas.

Los usuarios pueden publicar, con el producto DOMINO (*tecnología que convierte a Lotus Notes en un servidor de aplicaciones de Internet, para crear, desplegar y mantener aplicaciones interactivas para Internet o Intranets corporativas.*) [URL5] la información almacenada en bases de datos, y así los usuarios de Internet a través de algún Browser pueden acceder al servidor y navegar por los documentos Notes.

A través del Cliente Notes es posible navegar por Internet, cada usuario se conecta al Servidor Notes, el cual ejecuta un proceso (Web), que se encarga de traer la página y transformarla al formato Notes. Los documentos que obtenemos del Web se pueden almacenar en bases de datos documentales. Una vez en ellas podemos buscarlos y utilizarlos sin necesidad de estar conectados a Internet.

- **Planificación y Calendarización**

La agenda compartida permite gestionar y planificar citas, reuniones, notas, actividades y aniversarios, reprogramar alguna reunión [URL6].

### **2.1.1.3. Coordinación**

- **Aplicaciones Workflow**

Lotus Workflow es una herramienta de desarrollo que trabaja en Lotus Domino, que permiten a la organización planificar, programar, seguir, supervisar y archivar trabajos basados en documentos y proyectos.

Esta herramienta proporciona el diseño de procesos sistemáticos o un conjunto de reglas para encaminar una carpeta de uno o más documentos a través de una serie de actividades. La carpeta se encamina con las actividades de un trabajo. Los documentos en las carpetas pueden ser modificados, adicionados, aprobados etc. por la persona que fue autorizada para realizar la actividad.

El dueño del trabajo puede supervisar, recibir avisos del E-mail de su progreso, e intervenir si no va según lo planificado.

Cada actividad puede ser solicitada y entonces realizada por una persona en la organización, o puede ser automatizada de acuerdo a las características definidas para la actividad. Cuando se termina cada actividad, la carpeta es encaminada a la actividad siguiente, hasta que se termina el trabajo entero. Cuando se termina el trabajo, estos documentos pueden ser archivados para referencia futura o para generar informes.

Los participantes del Workflow tienen una visión global del proceso un diagrama con la descripción gráfica de las actividades anteriores, actuales y subsecuentes en un trabajo. Se representan los pasos de un proceso como un diagrama similar a un organigrama. Las actividades son nodos en el diagrama, y los conectores entre los nodos son asignados para que encaminen las relaciones que determinan qué trayectoria tomará la carpeta a partir de una actividad a la siguiente.

Los conectores pueden pasar a través de puntos de decisión para ver que decisiones deben ser tomadas.

#### **2.1.1.4. Descripción general**

- **Aplicaciones**

Las aplicaciones se realizan desde el mismo cliente Notes, no es necesario otro producto.

Cada base de datos posee vista de diseño donde se definen formularios, vistas, agentes y ayudas.

Dentro de cada formulario se pueden definir formulas o código, que permite la construcción de formularios inteligentes, en que se pueden ejecutar acciones de validación. Además en un formulario se pueden incluir elementos tales como textos, campos, botones, secciones, barras de acción, etc.

Toda aplicación queda dentro de la definición de la base de datos ya sea en el servidor o en el PC (*sí la base de datos es local*), esta se traduce en el cliente y permite que el código sea transportable a las plataformas que apoya Notes.

Además se incluye aplicaciones de ejemplo (*Templates*) que permiten ser adaptadas a lo que la empresa necesita.

- **Arquitectura**

Los servidores de Notes se ejecutan en distintas plataformas, agrupándose en dominios.

Un dominio se crea al definir el primer servidor, generándose un certificado (*archivo de identificación para el dominio*). Luego con el archivo del dominio se procede a crear los subdominios a los que pertenecerán cada uno de los servidores.

La ventaja de agrupar servidores en dominios es que el ruteo de mails se produce inmediatamente.

- **Infraestructura de Lotus (Servidor y Cliente)**

**Servidor Lotus Notes:** Esta clasificado como un servidor bien diseñado escalable y robusto para intranets corporativas. Es totalmente compatible con los estándares de Internet (HTTP, HTML, TCP/IP y Java) y además soporta todas las interfaces de navegación -browsers- de Web.

**Cliente Notes:** Máximo potencial Intranet

Cuando se utiliza un servidor Lotus Notes en el centro de una red Intranet, tanto los desarrolladores como los usuarios tienen la flexibilidad de elegir las mejores opciones de acuerdo a sus necesidades. La utilización de Notes en conjunto con el servidor Notes ofrece notables beneficios.

- **Seguridad**

Cada usuario posee en su estación de trabajo un archivo de identificación (ID), que le permite acceder a un servidor por medio de una contraseña, el usuario tiene acceso al servidor, generación de firma electrónica y encriptación de datos, listas de control de acceso a las bases de datos, que permite el acceso a la información contenida en ellas.

Cada usuario se crea por el administrador a través del Cliente Notes, por medio del Panel de Control, donde se tiene acceso a la información de los Servidores del Dominio. Donde se pueden monitorear las actividades relacionadas con el correo y las bases de datos, específicamente: Monitoreo de réplicas, Estado de los procesos servidores, Espacio en disco en el servidor, usuarios conectados, estadísticas que permiten conocer el porcentaje de recursos utilizados en algún instante de tiempo.



### 2.1.1.5. Hardware necesario

- **Requerimientos de memoria para Lotus Notes 5.0 y 6.0**

- Microsoft Windows 95 (segunda edición, mínimo con instalador) y Windows 98, 64MB RAM requeridos; 128MB o más recomendados
- Windows NT, Versión 4.0 con Sp6a 64MB RAM requeridos; 128MB o más recomendados
- Windows 2000, Edición Profesional y Windows XP 128MB RAM requeridos; 256MB o más recomendados
- Macintosh OS 9.x y OS X (10.1 solamente) 128MB RAM requeridos; 256MB o más recomendados

- **Requerimientos de espacio en disco**

*Windows*

- 275MB de espacio en disco requeridos

*Macintosh OS 9.x*

- 175MB de espacio en disco requeridos

*Macintosh OS X (10.1 solamente)*

- 250MB de espacio en disco requeridos

- **Plataformas Clientes**

- Windows 95, NT, 3.X,2000,XP
- UNIX(Sun, Solaris, HP-UX, IBM AIX)
- Macintosh OS.9X,OS.X (10.1 solamente)

- **Plataformas Servidores**

- Windows 95, NT
- UNIX(Sun, Solaris, HP-UX, IBM AIX)

- **Protocolos**

- TCP/IP,
- Apple Talk
- NetBEUI/NetBIOS
- IPX/SPX

## 2.2. TECNOLOGIA MICROSOFT

### 2.2.1. MICROSOFT EXCHANGE 2000

Permite a los usuarios acceder, organizar e intercambiar información desde cualquier lugar.

Se utilizan carpetas, para almacenar todo tipo de información: documentos, archivos mensajes de correo y telefónicos etc. Definiéndose dos tipos de carpetas de información: Personales(*Almacenan ordenan documentos y mensajes de correo que el usuario no desea compartir con el grupo, estas pueden residir en el servidor o en el PC.*) y Públicas(*Estas se encuentran en el servidor, permite a los usuarios acceder, incluir o eliminar información* ). En el cliente aparecen ambos tipos de carpetas, que forman parte del árbol jerárquico al cual tiene acceso, el árbol representa carpetas y subcarpetas que son independientes del servidor sobre el cual residen.

Las carpetas pueden ser personalizadas por los usuarios. Se pueden crear vistas personales que especifican lo que aparecerá en el cliente, una vista puede almacenar el contenido de una carpeta en base al autor, día, palabras clave o algún campo que contengan los documentos.

Exchange 2000 proporciona una plataforma que permite a los desarrolladores generar soluciones de mensajería y colaboración.

El *software cliente*, Microsoft Outlook 2000, facilita una infraestructura de mensajería y colaboración altamente confiable, escalable y fácil de administrar.

### **2.2.1.1. Comunicación**

- **Correo electrónico**

Permite el envío y recepción de documentos, memos y adjuntar información a un usuario o a un grupo de usuarios.

Incorpora documentos adjuntos o archivos creados con otras aplicaciones.

El *Inbox* permite la recepción de correo y se comporta como otra carpeta permitiendo organizar la información en función de lo que el usuario desea.

Se pueden incluir prioridades a los mensajes y acuses de recibo, para así conocer si un usuario ha leído el correo que se envía.

El libro de direcciones incluye a los miembros de una organización, donde se encuentran usuarios grupos, números de teléfono e información relacionada.

Los destinatarios del correo se pueden seleccionar a partir del Libro de Direcciones, se puede utilizar la escritura anticipada de nombres.

Un usuario puede revisar su correo sobre cualquier estación de trabajo que tenga el cliente Exchange.

### **2.2.1.2. Colaboración**

- **Bases de información compartida**

Generación de aplicaciones de colaboración, programar grupos, grupos de discusión y publicación, carpetas de grupo conocidas también como Carpetas Públicas que permiten almacenar información de distinto tipo y formato.

Se pueden crear vistas personales donde se especifican los campos que desean desplegar.

Los elementos se presentan por medio de carpetas ordenadas jerárquicamente, la información que se presenta, puede residir en uno o más servidores.

Posee un servicio de indexación y búsqueda por contenido integrado, los usuarios pueden localizar y compartir información rápidamente.

- **Planificación y Calendarización**

A través de la agenda de Outlook, se puede organizar una reunión. Para ello, se realiza una serie de consultas sobre el tipo de reunión, personas involucradas, horas del día, en que están disponibles, para ver si se encuentra un punto de unión. El uso de carpetas compartidas, nos permite tener documentación bien útil para toda la compañía o solo accesible para un determinado departamento .

Los usuarios pueden administrar su tiempo, tareas y organizar reuniones entre las personas que integran un grupo de trabajo .

A través de Listas de Tareas se pueden definir las tareas realizadas por el usuario, tiempo de inicio, tiempo de duración, porcentaje de avance los cuales pueden ser agrupadas por proyecto duración o prioridad

Existen distintas vistas ya sea por día, semana y mensual que permite a los usuarios ver sus tareas y tiempos así como el estado en que se encuentra cada una de ellas

### 2.2.1.3. Coordinación

- **Aplicaciones Workflow**

Para desarrollar flujos de trabajo con Exchange 2000 es necesario el sistema de almacenamiento Web y las herramientas Microsoft Workflow Designer for Exchange 2000 Server (*Diseñador de flujo de trabajo para Exchange 2000 Server de Microsoft*) y Collaboration Data Objects (CDO) Workflow Objects (*Objetos de flujo de trabajo de CDO*) [URL7].

### 2.2.1.4. Descripción general

- **Aplicaciones**

Para generar aplicaciones se requiere de las herramientas Folder y Forms Designer, que se utilizan para definir vistas, carpetas, reglas, permisos formularios y atributos de una carpeta pública.

En los formularios se pueden incluir:

- Campos preprogramados: to, from, cc, bcc, subject
- Controles: labels, text box, check box y option buttons
- Validación y alertas
- Menú, barra de herramientas, help y barra de estado

El Form Designer compila el formulario y crea un archivo ejecutable, el cual se almacena en una carpeta personal, pública o en una librería de formularios.

Con estas herramientas se pueden construir aplicaciones que utilizan distintas carpetas y formularios, permitiendo el seguimiento por ejemplo de ordenes de compra, además se incluyen aplicaciones de ejemplo que pueden ser adaptadas a las necesidades de la empresa.

- **Arquitectura**

Los servidores Exchange se agrupan en uno o más Nodos (sites) para mantener centralizada la administración, seguridad y los servicios de comunicación.

Un nodo consiste de uno o más servidores Exchange que entregan servicios de comunicación a un conjunto de usuarios y comparten la misma información de directorio. Los nodos corresponden a áreas dentro de la organización que están conectadas a través de la red corporativa.

Dentro de un nodo, el ruteo de mensajes y la replicación ocurre automáticamente.

La topología de servidores se visualiza a través del *Arbol de Información de Directorio*.

- **Seguridad**

Exchange 2000 Server está totalmente integrado con el modelo de seguridad de Windows 2000. Al utilizar Microsoft Active Directory, puede otorgar a los usuarios y administradores de Exchange permisos para llevar a cabo tareas específicas y acceder a recursos específicos.

Windows 2000 proporciona un acceso único y autenticación, lo cual le libera de tener que mantener un esquema de autenticación por separado.

Garantizar la seguridad en los mensajes por medio de la Encriptación de los contenidos para obtener un máximo de privacidad en la información confidencial.

Las firmas digitales proporcionan autenticación, integridad y no repudio de los mensajes de correo electrónico, garantizan la identidad del remitente y aseguran que los contenidos del mensaje no se alteren en tránsito.

En cuanto a la privacidad del contenido, los usuarios pueden elegir encriptar los mensajes individuales o elegir encriptar todos los mensajes de receptores específicos. Exchange 2000 Server encripta los mensajes utilizando el protocolo de Extensiones de correo en Internet seguras/multipropósito (S/MIME) estándar en la industria. Outlook además soporta los *plug-ins* clientes de terceros para Pretty Good Privacy (PGP) y otros métodos de encriptación.

Exchange 2000 Server utiliza el sistema de Infraestructura de clave pública (PKI) flexible para distribuir y administrar las claves, utilizando firmas digitales y encriptación.



### **2.2.1.5. Hardware necesario**

- **Requisitos de hardware mínimo y recomendado**

- *Hardware Mínimo*

Procesador: Pentium 200 MHz

Memoria: 128 MB

Espacio de disco: 2 GB para Exchange, 500 MB disponibles en la unidad del sistema

- *Hardware Recomendado*

Procesador: Pentium II a 400 MHz

Memoria: 256 MB

Espacio de disco: Espacio para correo electrónico y carpetas públicas

- **Infraestructura de Exchange**

Arquitectura cliente/servidor

#### **Plataformas servidores**

- Windows 2000 Server o Advanced Server
- Microsoft Exchange 2000 Server

#### **Plataformas clientes**

- Microsoft Office XP Professional Ed.
- Microsoft Windows XP Professional

#### **Protocolos**

- TCP/IP
- NetBeui/NetBIOS
- IPX/SPX

## 2.3. TECNOLOGIA GNU

### 2.3.1. DEFINICIÓN OPENSOURCE

Código fuente libremente disponible.

- Se puede corregir, personalizar, mejorar, distribuir, sin recurrir al creador o proveedor.
- Es la Suma de muchos programadores que contribuyen a la mejora del producto.
- General Public License (GPL): copyleft. [URL8]

### 2.3.2. Licencia pública general

El software de código abierto está disponible mediante un sistema de licencia que permite el libre uso, distribución y copia del código fuente. Esto se denomina *licencia pública general (General Public License)* y se conoce por la sigla GNU.

Nadie puede restringir la libre circulación del software original y sus modificaciones.

El usuario tiene libertad de utilizar el código, modificarlo, corregirlo, personalizarlo y redistribuirlo, siempre y cuando cumpla con las condiciones que se han fijado para ello [Rau04].

Las condiciones más relevantes son:

- a) El código fuente debe estar disponible sin restricciones para el usuario, ya sea por entrega directa o por hallarse disponible en Internet.
- b) El código fuente puede ser modificado, ya sea para cambiar sus funciones o para personalizarlo.
- c) El nuevo producto que podría surgir de las modificaciones debe regirse por el mismo sistema de licenciamiento que el código fuente original.

- d) El usuario tiene derecho a la libre reproducción y redistribución del código original y las modificaciones introducidas.
- e) No debe hacer discriminación de personas o grupos de personas.
- f) No debe restringir el uso del programa en un campo específico de aplicación. Por ejemplo, no puede restringir su uso en negocios, o en investigación genética.
- g) No debe imponer restricciones sobre otro software que es distribuido junto con él. Por ejemplo, la licencia no debe insistir en que todos los demás programas distribuidos en el mismo medio deben ser software Open-Source.
- h) La Licencia publica general ofrece la seguridad legal que el software de código abierto se mantendrá disponible para todos y que ninguna empresa o persona se apoderará de su propiedad.
- i) Se puede registrar un producto derivado del código original pero todo cambio al código original debe hacerse público.

Los productos que se analizaron se encuentran

- EGroupware
- OpenGroupware

### 2.3.3. eGroupware

eGroupware es una suite Groupware multiusuario, basado en web, desarrollado sobre un conjunto personalizado de PHP-basis APIs. Actualmente los módulos disponibles incluyen email, addressbook, calendario, infolog (notas, listas, llamadas telefónicas), contenido de gerencia, foro, bookmarks.

Egroupware es desarrollado por un equipo de personas [URL9].

- Andreas Krause
- Alejandro Pedraza
- Angelo Tony Puglisi
- Jerry Ruhe
- Joao
- Jonas Goes
- Lars Kneschke (project admin)
- Miles Lott
- Pim Snel
- Ralf Becker (project admin)
- Reiner Jung (project admin)
- Greg Haygood
- Zhang Weiwu

### **2.3.3.1. Comunicación**

- **Correo electrónico**

El correo electrónico puede ser configurado, como Pop3 o Imap

Es posible crear carpetas para organizar mejor el correo y configurar mas de una cuenta. En la comunicación también se encuentra habilitada la opción mensajería instantánea.

### **2.3.3.2. Colaboración**

- **Bases de información compartida**

En la opción registro, base del conocimiento, y administrador de archivos permiten incorporar y compartir información ordenada por tópicos de interés, y su posterior búsqueda por medio de criterios establecidos,

La opción Fudforum (*foros de discusión*) que planteado un tema se espera que los miembros involucrados emitan su opinión.

- **Planificación y Calendarización**

Calendario compartido, permite gestionar y planificar citas, reuniones, actividades, etc.

En Tareas y Proyectos se definen las actividades a realizar por un usuario o grupos de usuarios, estos pueden ver los tiempos y el estado en que se encuentran sus actividades.

### **2.3.3.3. Coordinación**

- **Aplicaciones Workflow**

Egroupware no posee una herramienta que permita hacer diagramas de seguimiento de actividades, el flujo de trabajo es monitoreado por medio del correo electrónico, mensajería instantánea, calendario compartido, foros de discusión, tareas y/o proyecto, donde es posible intervenir en una actividad o visualizar el estado avance de un trabajo.

### **2.3.3.4. Descripción general**

- **Arquitectura**

En el caso de las herramientas con la estructura cliente-servidor, no se requiere la instalación del software en el PC del usuario, sino que este se conecta al servidor que lo contiene, a través de un navegador.

EGroupware no necesita ser compilado. Se compone solamente de PHP, HTML y de archivos de imagen. Necesita un servidor web que permita php4. Apache1.3.x con PHP4.3.x preferido. Puede necesitar un servidor email IMAP o POP, que pueden ser local o remoto,

- **Seguridad**

El acceso al espacio de trabajo es restringido, el usuario debe disponer de un nombre de usuario y una contraseña, el administrador o un usuario en particular puede conceder acceso a otras personas a los datos de un usuario o un grupo en particular por Lista de Control de Acceso, el objetivo de ACL es conceder acceso, que significa:

- usted puede decir: se permite al usuario x o el grupo y a leer mis datos.
- el administrador puede decir: todos los miembros del grupo x permite a otro grupo o usuario a acceder a estos datos.

### **2.3.3.5. Hardware necesario**

Estado de desarrollo: 5 –productos/estables RC5

Entorno: entorno web

Audiencia objetivo: desarrolladores, usuarios finales

Lenguaje natural; ingles, alemán

Lenguaje de programación: PHP

- **Requerimientos mínimos para instalar eGroupware**

- WebServer [Rei03]

Apache 1.3x, 2.x

- Bases de datos

Mysql

PostgreSQL

MSSQL

- Sistema operativo

Linux,

Windows NT/2000

#### 2.3.4. OpenGroupware

OpenGroupware es la solución para trabajo en grupo orientado a empresas utilizando tecnologías libres. Permite la colaboración segura entre los usuarios del sistema, ofrece los componentes de servidor necesarios para la colaboración.

Debido a las características del software utilizado (*software libre*) no hay límite de usuarios y no existe el concepto de licencias de uso, por lo que no hay costo de utilización adicional independientemente del número de usuarios. Además se entrega el código fuente de todo el sistema al cliente.

La importancia de OpenGroupware (OGGo) es que se tiene por primera vez una aplicación en software libre que reemplaza a Microsoft Exchange, esta mas centrado en el trabajo en grupo y la colaboración en lugar de la mensajería, OGo no incluye un servidor de correo, sino que emplea uno de los existentes como Cyrus [URL11].

El software OGo permite compartir calendarios, libreta de direcciones e información de email; compartir carpetas, cambiar documentos, rastrear cambios, y navegar por el Web de forma sincronizada y simultánea, todo ello con estándares abiertos de Internet y sin pagar o gestionar licencias propietarias.

Las características principales de OpenGroupware son las siguientes:

- *Resumen para hoy*: Indica vía Web las tareas pendientes, últimos mensajes recibidos y agenda de hoy.
- *Correo electrónico*: Solución completa de correo electrónico, incluyendo webmail (*acceso al correo desde un navegador*)
- *Agenda/diario*: Gestión vía Web de la agenda incluyendo vistas diarias, semanales, mensuales o anuales.



- *Notas*: Almacenamiento de notas vía Web.
- *Tareas*: Gestión de las tareas pendientes.
- *Gestión de bookmarks* y acceso a estos desde cualquier máquina.
- *Gestión de contactos*: Incluyendo contactos compartidos por distintos grupos de personas.

La administración de OpenGroupware se realiza íntegramente vía Web. Cada usuario puede personalizar su interfaz. Además el administrador puede habilitar o deshabilitar funcionalidades globales para todo el sistema.

En OpenGroupware la información se almacena en una base de datos Postgres, el beneficio de que la información se almacene en una base de datos es su capacidad para administrar la concurrencia y el control de las versiones de los documentos compartidos, además de permitir guardar de una mejor manera la información histórica.

#### **2.3.4.1. Comunicación**

- **Correo electrónico**

Para una mejor flexibilidad e independencia, la comunicación del E-mail es manejada por un servidor Imap. La ventaja de esta solución es que permite el almacenaje centralizado del Email. El Inbox permite la recepción de correo y se comporta como otra carpeta permitiendo organizar la información en función de lo que el usuario desea, permite crear su propio árbol de carpetas y manejar sus Emails en cualquier lugar.

El árbol de carpetas que se utiliza para clasificar los Emails, esta situada dentro de la carpeta en el servidor Imap.

*Internet Message Access Protocol (IMAP)*: Es un protocolo de acceso a correo usado por las aplicaciones de correo cliente para recuperarlos desde los servidores de correo, a diferencia de SMTP, este protocolo requiere autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para este protocolo son pasadas a través de la red de forma encriptada.

#### **2.3.4.2. Colaboración**

- **Bases de información compartida**

En la aplicación proyectos y tareas es posible compartir documentos y carpetas con otros usuarios, que estén involucrados de forma directa a la tarea o proyecto.

Se puede definir las tareas realizadas por el usuario, tiempo de inicio, tiempo de duración, porcentaje de avance. Además permite integrar personas o equipos para asignación de tareas. Los usuarios pueden consultar en la aplicación proyectos y tareas, su participación y estado de avance en que se encuentra cada una de ellas.

- **Planificación y Calendarización**

El calendario permite gestionar y planificar citas, reuniones, actividades, reprogramar alguna reunión, para organizar una reunión se realiza una serie de consultas sobre el tipo de reunión, personas involucradas, horas del día, en que están disponibles, para ver si se encuentra un punto de unión. Una vez decidida fecha y hora, se convoca a los asistentes y se espera respuesta. El sistema permite enviar un correo con acuse de recibo a los participantes para obtener la confirmación de la asistencia. Si es aceptada la información se actualiza automáticamente en el calendario y en el calendario del remitente, existen distintas vistas ya sea por día, semanal y mensual.

#### **2.3.4.3. Coordinación**

- **Aplicaciones Workflow**

Para facilitar los flujos de trabajo e información dentro de la compañía.

El correo electrónico permite intercambiar información de forma ordenada entre los distintos usuarios, sin necesidad de que el receptor requiera buscar el archivo que necesita para realizar su trabajo, generalmente viene unido al mensaje del remitente.

A través del calendario, es posible organizar una reunión, la posibilidad de compartir archivos y carpetas, nos permite tener documentación útil para toda la compañía o solo accesible para un determinado departamento.

#### **2.3.4.4. Descripción general**

- **Aplicaciones**

En la aplicación crear *nuevo documento*, permite escribir directamente código XML y HTML y verificarlo de forma inmediata, esta característica permite crear de una manera rápida archivos HTML/XML.

- **Arquitectura**

Aplicación cliente - servidor no se requiere la instalación del software en el PC del usuario, sino que este se conecta al servidor que lo contiene, a través de un navegador.

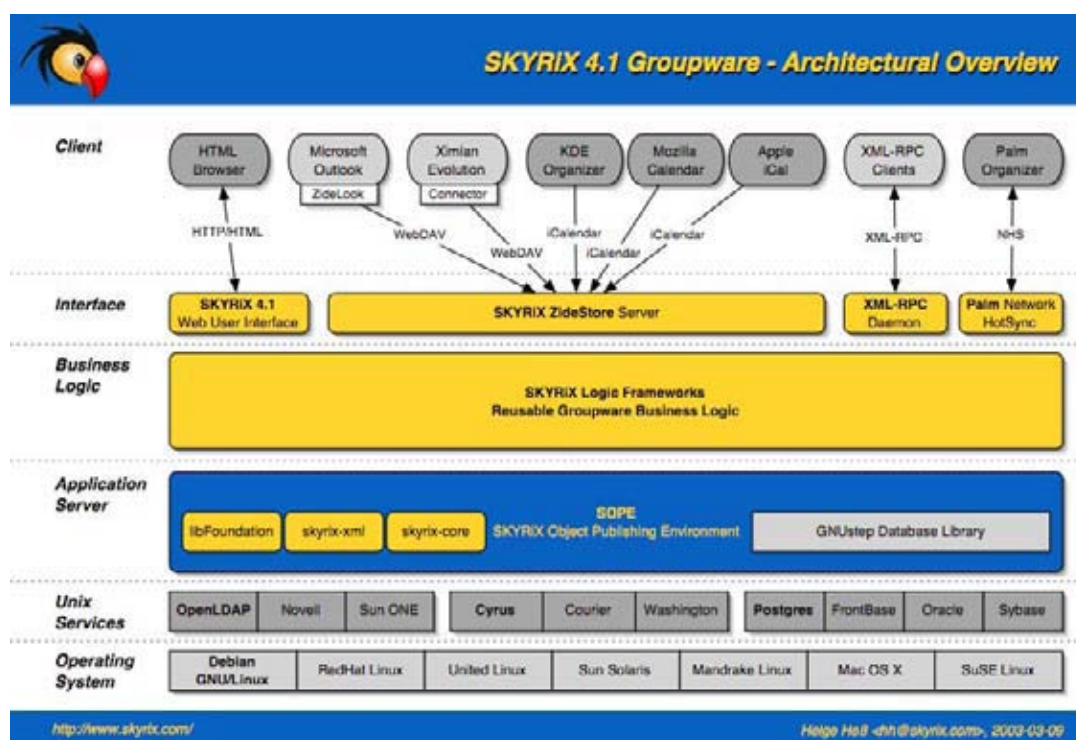


Figura N°4: Arquitectura Groupware -.Skyrix.

La figura muestra un diagrama de la arquitectura de *Skyrix* (versión comercial), en el cual OGo está basado [Tom03].

OGo es construido sobre la base de las librerías de libFoundation y de GNUstep.

En el corazón de OGo contiene, el entorno de publicación de objetos SKYRIX (SOPE). SOPE donde la página Web es generada y desplegada a través del WebUI.

Además del WebUI, OGo puede conectarse con distintos tipos de clientes. Según lo demostrado en el diagrama, un conector es necesario para que OGo se conecte con Microsoft o evolución de Ximian, y estos conectores

son actualmente fuentes cerradas. Sin embargo, hay esfuerzos para proporcionar un conector basado opensource.

GNUstep-db soporta un mecanismo de acceso a distintos motores de base de datos a través de *plugins*. La distribución en código fuente de OGo incluye adaptadores de base de datos para PostgreSQL y FrontBase. Los adaptadores para Sybase y Oracle forman parte de la distribución comercial de SKYRIX 5 y no se incluyen con OGo.

A pesar de la popularidad de MYSQL aun no ha sido necesario extender el soporte de OGo a MySQL o cualquier otro motor de bases de datos.

Se prefiere PostgreSQL por el hecho de ser realmente gratuito, es más robusto y soporta funciones que todavía se encuentran apenas en desarrollo en MySQL.

- **Seguridad**

OpenGroupware es un sistema innovador, para las empresas que requieren una herramienta eficaz y estable para manejar su comunicación interna según los requisitos actuales. Para tener acceso a los datos, se requiere de un navegador Web (e.g. Internet Explorer del MS o Netscape Navigator). El acceso al espacio de trabajo es restringido, el usuario debe disponer de un nombre de usuario y una contraseña, el administrador o un usuario en particular puede conceder acceso a otras personas a los datos de un usuario o un grupo en particular por Lista de Control de Acceso.

Los datos de la empresa se almacenan en el servidor de la compañía, donde pueden ser accedidos por cualquier funcionario que posea una cuenta de usuario.

El administrador, puede crear nuevos usuarios del sistema, grupos y recursos, el administrador puede otorgar a los usuarios, grupos y equipos permisos para llevar a cabo tareas y acceder a recursos específicos.

Cada usuario puede crear nuevos trabajos, proyectos y asignar a personas que colaboren con ellos además estos pueden realizar ciertas modificaciones, si poseen ciertos permisos otorgados por el creador de dichos trabajos.

Existen en la actualidad conectores para los clientes *Ximian Evolution* y *Microsoft Outlook*, para conectarse al servidor de OGo, por medio de estos clientes es posible la aplicación de firma electrónica que permita dar seguridad en el envío de información.

#### ***Lista de control de acceso: ACL***

Permite conceder acceso a otras personas a los datos de un usuario o un grupo en particular.

El principio de ACL es conceder acceso, que significa:

Usted puede decir: se permite al usuario X o el grupo Y a leer mis datos

El administrador puede decir: todos los miembros del grupo X permite a otro grupo o usuario a acceder a estos.

En la aplicación proyectos, los permisos pueden ser concedidos de la siguiente manera:

- *m-manager*: Este derecho garantiza acceso completo al proyecto. el usuario/equipo tienen acceso de administrador, puede administrar el proyecto automáticamente, como administrador del proyecto tiene todos los permisos, puede adicionar cuentas, crear carpetas y documentos etc.
- *r-read*: Para un respectivo proyecto, las carpetas o documentos pueden ser leídos.

- *d-delete*: Carpetas o documentos pueden ser borrados, Para borrar un objeto específico por ejemplo un archivo, se requiere tener acceso de escritura, para el objeto superior por ejemplo una carpeta.
- *i-insert*: Los objetos pueden ser insertados dentro de un objeto específico (por ejemplo archivos y carpetas dentro de un proyecto)
- *w-write*: Las personas / equipos tienen acceso a escritura en un proyecto a sus carpetas y archivos.
- *f-form*: Este acceso permite crear y editar formularios.
- *privado*: Acceso a datos marcados como privado.
- *Registro(Logs)*: En cada aplicación del programa OGo, contiene la funcionalidad de registro, el cual contiene el historial de modificaciones, si un usuario que tiene derecho de hacer cualquier cambio, automáticamente se registra la fecha, el usuario y la acción. Esta funcionalidad es útil por razones de seguridad si alguna modificación es causa de error, aquí se registra el último usuario que realizó una modificación y cual fue esta.

Para las otras aplicaciones del programa OGo existen los derechos de acceso de lectura, escritura y privado.

***Donde otorgar los permisos, el ACL***

- un usuario: cada usuario puede otorgar permisos en las preferencias de cada aplicación (otorgar permisos).
- un grupo: un administrador puede fijar permisos a un grupo.



#### **2.3.4.5. Hardware Necesario**

- **Hardware Mínimo**

Los recursos de hardware se deben medir según la cantidad de usuarios que trabajan.

Procesador Pentium Intel o compatible, 500 MHz, 512 MB RAM, 40 MB de espacio de disco libre [Sky02].

- **Hardware Recomendado**

- Doble-procesador Pentium Intel o compatible, 700 MHz, 1024 MB RAM
- 40 MB de espacio de disco libre.
- SPARC/Solaris

- **Plataformas Clientes**

- Navegador Internet
- Conexión a Internet recomendada: ISDN o módem 56k
- Resolución de pantalla recomendada: 800x600, mejor es 1024x768

- **Plataformas Servidores**

WebServer Extern: Apache 1,3,9

En cualquier distribución de linux (SuSe Linux 6.2 o superior, RedHat 7 o superior, Mandrake Linux 7.2 o superior, Debian)

- **Protocolos**

Tcp ip.

## 2.4. METODOLOGÍA SELECCIÓN DE LA MEJOR ALTERNATIVA

El Servicio de Salud Valdivia es una institución pública, el cual no tiene presupuesto asignado para adquirir productos comerciales demasiados costosos como lo son Lotus y Exchange, de ambas tecnologías la mejor que existe en el mercado es Lotus Notes/Domino que son el paquete más completo, administra el e-mail, aplicaciones sobre Web, aplicaciones Workflow y aplicaciones de comercio electrónico, en cambio Exchange 2000 es un producto del e-mail con algunas características de colaboración. [Cer97]

Por lo tanto, el producto a escoger es una tecnología Gnu. Entre los productos estudiados de esta categoría se encuentran eGroupware y OpenGroupware y la metodología a aplicar es metodología de proyectos informáticos MIDEPLAN [Met03].

Para la evaluación de alternativas se medirán ciertos atributos de la solución propuesta y se definirán ponderadores para dichos atributos, que permitirá evaluar las distintas alternativas planteadas.

La dificultad del modelo radica justamente en la definición de atributos y la estimación de los ponderadores.

- **Atributos imprescindibles**

Son los atributos que deben cumplirse obligadamente para que la alternativa pueda ser considerada.

- La alternativa de solución está de acuerdo con la política informática (si es que existe) de la institución.
- La institución dispone de las capacidades técnicas y administrativas para soportar la solución. ( por ejemplo para administrar la red)

- **Atributos evaluables**

Los factores de evaluación a considerar son los siguientes:

- A) Efectividad
- B) Plataforma Tecnológica
- C) Calidad Técnica de la Solución
- D) Ahorro de costos operacionales

A) Efectividad

<b>FUNCIONALIDADES DEL SISTEMA</b>	<b>eGroupware</b>	<b>OGo</b>
<b>MUY DESEABLES 0.7 (Cumplimiento)</b>	80%	100%
Información en Línea	1	1
Interfaces Gráficas	1	1
capacidad de comunicación	0	1
procesamiento distribuido	1	1
procesamiento centralizado	1	1
<b>DESEABLES 0.3 (%Cumplimiento)</b>	66.6%	100%
Emisión de documentación	0	1
Control de cambios	1	1
Facilidad de instalar	0	1
Facilidad de operar	1	1
La solución fue diseñada para ayudar al cambio organizacional	1	1
Las funciones proveídas mejoran la eficiencia del usuario	1	1
<b>Total</b>	<b>EF1=75.98</b>	<b>EF2=100</b>

Tabla N°1: Efectividad

B) Plataforma Tecnológica

<b>ASPECTOS PLATAFORMA TECNOLÓGICA</b>	<b>Ponderador</b>	<b>eGroupware</b>	<b>OGo</b>
Confidencialidad	18.18%	18.18	18.18
Integridad	36.36%	21.816	29.088
Disponibilidad	9.095	9.095	9.095
Confiabilidad	27.27%	16.362	27.27
Información Externa	9.09%	7.272	7.272
<b>TOTAL</b>	<b>100%</b>	<b>PT1=72.725</b>	<b>PT2=90.905</b>

Tabla N°2: Plataforma Tecnológica

### C) Calidad Técnica de la Solución

ASPECTOS TÉCNICOS SISTEMA	Ponderador	eGroupware	OGo
<b>SEGURIDAD(% cumplimiento)</b>	X% 57.08	42.8	57.08
Sistemas de Respaldos	9.5	1	1
Sistema de recuperación	14.28	0	1
Control de acceso	23.8	1	1
Encriptación de datos	9.5	1	1
<b>PORTABILIDAD (%Cumplimiento)</b>	Y% 9.5	9.5	9.5
Herramientas para importación y exportación de datos	9.5	1	1
<b>DISPONIBILIDAD</b>	Z% 23.8	23.8	23.8
Up time garantizado de más de 98%	23.8	1	1
<b>ACCESIBILIDAD(%Cumplimiento)</b>	U% 9.5	0	9.5
Canales de comunicación en línea con otras aplicaciones	9.5	0	1
<b>TOTAL</b>	<b>100%</b>	<b>CT1=76.1</b>	<b>CT2=100</b>

Tabla N°3: Calidad técnica de la solución

### D) Ahorro de costos operacionales

COSTOS OPERACIONALES	eGroupware	OGo
Ahorro de papel	100	100
Ahorro en distribución de la información	70	100
Ahorro en reparaciones	70	80
Materiales de uso y consumo corriente (diskettes, hojas perforadas, cintas de impresoras, etc.)	70	100
<b>SUMA</b>	<b>310</b>	<b>380</b>
<b>Promedio</b>	<b>77.5</b>	<b>95</b>

Tabla N°4: Ahorro de costos operacionales

## Evaluación de alternativas

$$P_i = \sum_j \frac{PA_{ji} * Ponderador_j}{100}$$

Donde:

- P<sub>i</sub> : Puntaje Alternativa i
- PA<sub>ji</sub> : Puntaje del atributo j de la alternativa i
- Ponderador<sub>j</sub> : Ponderador del atributo j (corresponde a efectividad, Plataforma tecnológica, calidad técnica y ahorro de costos Op.)

<b>ATRIBUTOS EVALUABLES</b>	<b>Ponderador</b>	<b>eGroupware</b>	<b>OGo</b>
Efectividad	33.3%	75.98	100
Plataforma Tecnológica	16.66%	72.725	90.905
Calidad Técnica	33.3%	76.1	100
Ahorro de Costos Op.	16.66%	77.5	95
<b>TOTAL</b>	<b>100%</b>	<b>75.6688</b>	<b>97.571</b>

Tabla N°5: Evaluación de alternativas

Como ambas alternativas son tecnologías GNU, esto significa que el software puede usarse, mejorarse, y redistribuirse sin ningún coste, basta con los puntajes de los atributos evaluables para decidir cual alternativa es mejor.

Según los resultados obtenidos en la Tabla N°5, la alternativa OGo, cumple adecuadamente con los atributos ya señalados, en el anexo A se describe como se instala este software, en cambio eGroupware cumple los atributos con restricciones. Por lo tanto la alternativa seleccionada es OpenGroupware, que es considerado una solución completa de trabajo en grupo, completamente libre que reemplaza Exchange.

Una vez instalado la herramienta eGroupware, no todas sus funcionalidades operaron correctamente, además la herramienta escogida satisface las necesidades que pretende el objetivo de esta tesis.

## 2.4.1. CARACTERÍSTICAS DEL PRODUCTO SELECCIONADO

### OpenGroupware

OpenGroupware es una herramienta sólida que lleva 7 años en el mercado, inicialmente con el producto comercial SKYRIX, que es el contribuyente del código fuente de OGo, luego en Julio del año 2003 es lanzada la versión libre OpenGroupware[URL10].

La misión de este proyecto es crear, una comunidad líder en servidores de trabajo en grupo de código abierto que se integre con las suites ofimáticas de código abierto y en todos los clientes de trabajo en grupo, proporcionando acceso a toda la funcionalidad y datos, utilizando interfaces y APIs (*Application Programming Interface - Programación de la interfaz de una aplicación*) abiertas basadas en XML.

El autor original del software de OpenGroupware fue MDlink GmbH, fundada en Alemania en 1994, creadores de SKYRIX 4.1 Groupware Server, el contribuyente del código fuente de OGo. SKYRIX es una solución que ha estado en desarrollo durante 7 años, y uno de los más antiguos productos Groupware para el sistema operativo Linux.

Las fuentes de OGo están escritas en Objective-C.

- Licencias

OGo se ha licenciado bajo dos licencias de software libre, la *Lesser General Public License* (LGPL) y la *General Public License* (GPL). Las bibliotecas y componentes están licenciados bajo los términos de la *LGPL* y las aplicaciones están licenciadas bajo la *GPL*. Para los usuarios, esto significa en parte que el software de OGo puede usarse, mejorarse, y redistribuirse sin ningún costo.

En OpenGroupware no existe el concepto de licencias de uso, ni limite de usuarios, por lo que no hay costo de utilización adicional independientemente del número de usuarios.

- *Servidor de Correo*

Existen servidores de correo código abierto. Cyrus, Courier, Washington IMAP, OGo se integra perfectamente con un servidor IMAP, Cyrus IMAP4 oficialmente.

- *Apoyo a Clientes*

Como Internet no esta disponibles en todos los sitios, es necesario dar soluciones para situaciones de desconexión.

Actualmente apoya a los siguientes clientes. Algunos clientes pueden requerir un conector extra para trabajar con el servidor Ogo [Tom03].

CLIENTE	CONECTOR	FUNCIÓN
Apple Ical	Ninguno	Solo de revisión
Mozilla Calendar	Ninguno	Solo de revisión
Ximian Evolution	Conector Ximian es requerido	Fase pre-alfa.
Microsoft Outlook	Zidelook Conector de SKYRIX	Funciona completamente

Tabla N°6: Conectores para OGo

Un conector es necesario para que OGo se conecte con Microsoft Outlook o Ximian Evolution, y estos conectores son actualmente de código cerrado.

Sin embargo, hay esfuerzos para proporcionar un conector Opensource.

El conector para OpenGroupware está muy restringido en funcionalidades, es necesario extender el desarrollo a todos los datos posibles



que pueden ser compartidos entre Evolution y OpenGroupware (correo, agenda de contactos, calendario tareas y citas).

- *Funcionalidades cubierta por Ogo, en el Anexo B se describe con detalle como operan estas funcionalidades.*

<b>FUNCIONALIDAD</b>	<b>DETALLES</b>
Agenda de contactos	Búsqueda, acceso a objetos LDAP, descargas de vCard de cada contacto, acceso rápido a tareas/proyectos relacionados con el contacto. Importa CSV/TSV de MS Outlook, Mozilla y otros.
Noticias	Con roles de editor/revisor. Las noticias pueden ser enlazadas entre ellas.
Instituciones ( <i>enterprises</i> en Ogo)	Las instituciones representan organizaciones, empresas, etc. Cada persona y cada proyectos puede ser asociado con una institución. A cada institución se le asigna un proyecto, para las tareas específicas de ella no relacionadas con otros proyectos y para facilitar la asociación de documentos.
Proyectos	Es un contenedor de tareas, documentos y notas. Puede ser asociado a varias instituciones y contactos individuales. Posee control de tiempos/recursos, incluido el de proyectos subordinados a otro.
Tareas ( <i>jobs</i> en OGo)	Cinco estados posibles: creada, aceptada, procesada, hecha y archivada. Las tareas tienen fechas para cada estado, prioridades y rigores requeridos.
Gestión de documentos	Cada documento puede ser asignado a una ACL. Posee un sistema de control de versiones. Pueden organizarse en subdirectorios, pueden ser comprobados y publicados.
Programación de calendario(scheduler en OGo)	Se integra la gestión de citas, invitaciones, gestión de recursos y alarmas. Gestión de conflictos de calendario
Webmail	Interfaz totalmente funcional a IMAP y SIEVE (filtros)
Gestión de PalmPilot	Control de sincronización directa con PalmPilot y del estado de los recursos compartidos entre PDA y OGo.

Tabla N°7: Funcionalidades de OGo

Se ha elegido OpenGroupware (OGo) al ser el software de trabajo en grupo mas completo, orientado a protocolos estándares, abiertos y libre según la GPL/LGPL, de los que existen.

Respecto a los protocolos soportados, son todos abiertos y estándares, y los procesos que los soportan, son ligeros, flexibles y adaptados a la filosofía UNIX de usar pequeñas aplicaciones conectadas con otras ya existentes, para cumplir la funcionalidad completa prevista.

## **CAPITULO 3 ANALISIS DE TECNOLOGIA IMPLEMENTACION DE FIRMA ELECTRONICA**

### **3.1. ASPECTO LEGAL**

La ley que soporta los procedimientos de firma electrónica es la Ley número 19.799 –Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma [Ley02].

Esta ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Al implementar la firma electrónica en el Servicio de Salud Valdivia, se pretende legalizar el uso de esta, en los distintos Servicios de Salud, de modo que cualquier documento que este firmado electrónicamente se considere válido.

## 3.2. HERRAMIENTAS DE SEGURIDAD

### Algunas definiciones

- **S/MIME** (Secure Multipurpose Internet Mail Extension)

El protocolo S/MIME fue una propuesta de la empresa RSA **Data Security Inc. "RSAINC"**, y está basado en los estándares de Criptografía pública creados por esta empresa, proporciona seguridad en el intercambio de mensajes mediante correo electrónico y uno de sus objetivos era ser fácilmente integrable en las aplicaciones de correo ya existentes.

Este estándar permite la confidencialidad, autenticación, integridad y no repudio, ya que trabaja con certificados y firmas digitales, por lo que necesita de autoridades de certificación para la emisión de certificados. También permite la utilización de listas de revocación de certificados que se utilizan para anular la validez de los mismos y tiene la capacidad de envolver tanto al mensaje como su firma en un sobre de datos cifrado.

- **PKCS#12** (Personal Information Exchange Syntax Standard)

El Estándar de Sintaxis de Intercambio de Información Personal, este estándar especifica un formato para almacenar y transportar claves privadas y certificados de un usuario desde un equipo a otro. PKCS #12 es apropiado para transportar, hacer copias de seguridad y restaurar un certificado y su clave privada asociada [Val02].

### 3.2.1. GnuPG y PGP

PGP, es una herramienta de encriptación asimétrica, diseñado especialmente por Philip Zimmermann en 1991 para proporcionar una forma segura de intercambio de correo electrónico. Implementa el cifrado del correo y archivos como la firma digital de documentos. Para enviar un mensaje encriptado, ambas partes deben tener el software PGP y deben intercambiar sus claves públicas.

GnuPG (*Gnu Privacy Guard*) es un programa, al igual que PGP (*Pretty Good Privacy*) para cifrar y firmar archivos o correos electrónicos.

La diferencia entre PGP y GnuPG es que PGP es un producto no libre en cambio GnuPG es completamente libre y la licencia que lo acompaña es totalmente gratuita incluso para usos comerciales, la versión 1.0.0 fue publicada en el año 1999.

De ambos hay versiones para entornos Windows como para entornos Linux.

La instalación y utilización de GnuPG o GPG en Windows es bastante sencilla, utilizando el paquete de instalación WinPT (*Windows Privacy tools*), la instalación de GnuPG se reduce a solo seguir los pasos guiados por el asistente.

- **Herramientas de privacidad para Windows (WinPT)**

Windows Privacy Tools (WinPT) es una aplicación para facilitar el cifrado y firma digital de contenidos.

Se basa en GnuPG, que es compatible con PGP, además es gratis para uso comercial y personal, bajo la licencia GPL.

WinPT posee módulos de correo electrónico, para integrar GPG con clientes de correo como Outlook Express y Eudora permitiendo así cifrar y descifrar correos simplemente haciendo unos cuantos clicks.

Además es independiente del cliente de correo, ya que presenta un menú de opciones que nos permite cifrar y firmar, mensajes y archivos y ser transportados por medio de disquetes o directamente desde el correo Web.

En el menú de opciones de WinPT, permite exportar la clave pública para que otras personas puedan enviar mensajes encriptados al destinatario e importar la de otras personas y establecer anillos de confianza donde podemos firmar estas claves públicas, además de firmar y encriptar archivos.

En el Anexo C se describe como Firmar y encriptar un mensaje con WinPT [URL1].

### 3.2.2. INFRAESTRUCTURA DE CLAVES PÚBLICAS

La utilidad de la firma electrónica se limita a la habilidad del receptor de asegurar la autenticidad de la clave usada para verificar la firma, en ocasiones estas claves pueden ser erróneamente atribuidas a un individuo o pueden ser descubiertas por una mala administración por parte del propietario. Esta problemática aumenta si ambos usuarios A o B son extraños y no existe un medio de comunicación que les permita identificarse de forma exacta, la única manera de autenticarse sería mediante la asistencia de una tercera parte confiable externa a ellos, que enlace sus identidades con sus claves públicas.

Para solucionar este problema surgen las Autoridades de Certificación o terceras partes de confianza, que son aquellas entidades que merecen la confianza de los demás usuarios, en un medio donde no existe una confianza directa. De esta forma el emisor de un mensaje firmado con este esquema no puede desconocer su firma, ya que nadie salvo él podría haber generado el resumen cifrado con tal clave privada, por lo tanto el no repudio.

Una infraestructura **PKI** "Public Key Infrastructure" (Infraestructura de Clave Pública), es un sistema necesario para la gestión de certificados digitales y aplicaciones de la Firma Digital. Su objetivo es dotar a los miembros de una organización los mecanismos básicos de seguridad que esta necesita, esto es

- *Autenticidad.* La firma digital tendrá la misma validez que la manuscrita.
- *Confidencialidad,* de la información transmitida entre las partes.
- *Integridad.* Debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.
- *No Repudio,* de un documento firmado digitalmente

Seguridad tanto para las conexiones Web (*con el protocolo Secure Socket Layer*) como para las comunicaciones a través de correo electrónico (*con el protocolo S/MIME*).

Para que una PKI pueda realizar todas estas actividades, su *propósito* es proveer claves y manejo de certificados confiables y eficientes, para lograr la autenticación del firmante y del documento, y la confidencialidad.

Los sistemas basados en clave pública deben estar seguros de que, cada vez que ellos confían en una clave pública, la clave privada asociada pertenece al sujeto con el cual ellos se están comunicando. Esta confianza se basa en el uso de certificados de clave pública los cuales son estructuras de datos que vinculan valores de clave pública a los usuarios. Este enlace se realiza a través de una autoridad de certificación, la cual verifica la identidad del usuario y firma digitalmente cada certificado.

Los certificados pueden usarse tanto para firmar documentos como para establecer un canal seguro y privado entre el cliente y el Servidor (*a través del uso de Secure Socket Layer*) y para encriptar datos que se envían a un tercero.

PKI permite a los usuarios interactuar con otros usuarios y aplicaciones, obtener y verificar identidades y claves, y realizar registración.



### **3.2.2.1. La Autoridad Certificadora**

La Autoridad Certificadora, es la entidad que asegura la identidad de los usuarios de los certificados digitales. Posee su propio par de claves y firma digitalmente los certificados con su clave privada. Confiando en la Firma Digital de la Autoridad Certificadora, puede confiarse en cualquier certificado generado por la misma.

Esta autoridad puede ser un organismo público o privado que busca llenar la necesidad de una tercera parte de confianza y que se hace responsable por la información contenida en sus certificados, ya que con su firma garantiza la validez de éstos.

Toda la fiabilidad de la Autoridad de Certificación se basa en la inviolabilidad de su propia clave privada, la cual resulta crítico proteger empleando medios técnicos y humanos.

### 3.2.2.2. Certificados Digitales

¿Cómo se puede asegurar que una clave pública pertenece a un usuario dado?. Es necesario poder vincular la clave pública de un usuario con su identidad y para esto surge el concepto de "Certificado Digital", un tipo de pasaporte o cédula pero digital que forma una asociación entre la identidad de un individuo y su pareja de claves. Un certificado digital contiene además de la clave pública del propietario, la información suficiente para satisfacer a un tercero acerca de la correcta identidad que en él se presenta.

Un certificado digital contiene la siguiente información:

- El nombre distinguido del propietario.
- La clave pública del propietario.
- Periodo de Validez del Certificado.
- El nombre distinguido de la autoridad de certificación (del emisor)
- La firma de la autoridad de certificación sobre esos campos

Esta información se encapsula en un formato estándar, normalmente se utiliza el protocolo Secure Socket Layer, que utiliza certificados digitales X.509.

La distribución de la clave pública entre varios interlocutores constituye un paso conflictivo por el problema de verificar correctamente la propiedad real de las claves públicas, ya que un intruso podría suplantar una determinada clave pública y con ello se infiltraría en comunicaciones encriptadas. Las Autoridades de Certificación (AC) verifican y certifican que la propiedad de las claves públicas es de sus legítimos propietarios. El certificado digital de usuario emitido por la AC sirve para garantizar que una determinada clave pública corresponde a su propietario.

Los certificados digitales dependen de su funcionalidad entre ellos se encuentran:

- *Certificados SSL para cliente*

Identifica a un cliente frente a un servidor

- *Certificados SSL para servidor*

Identifica a un servidor frente a un cliente

- *Certificados S/MIME*

Firmado y cifrado de correo electrónico

- *Certificados de firma de objetos*

Firmado de ejecutables o porciones de código

- *Certificados para CAs*

Identifica a una AC frente a otra AC.

- **Certificados X.509**

El protocolo X.509, desarrollado por la comunidad ISO e ITU(*unión internacional de comunicaciones*).

El modelo de certificación propuesto por X.509 identifica una estructura jerárquica de certificadores que se encuentran interconectados por niveles, formando “líneas de confianza” entre los niveles superiores e inferiores, partiendo de un certificador raíz, se generan certificadores dependientes que, a su vez, pueden generar otros certificadores hijos. La relación de parentesco que se establece entre los certificadores, que se traduce en la utilización de una información común para la generación de las claves públicas y privadas, hace que los certificados otorgados en un determinado nivel, sean perfectamente reconocidos y admitidos por los certificados emitidos en cualquier otro nivel o rama del árbol de certificadores, y, lo más importante, sin necesidad que las entidades implicadas tengan que intercambiar dato alguno.

Los certificadores X.509, denominados AC (*Autoridad de Certificación*), emiten certificados que tienen un formato concreto donde se incluyen, además de las correspondientes claves dobles, información adicional que permite delimitar el tiempo de validez del certificado, información sobre el certificador que lo ha generado y otros datos que permiten aplicar directivas para su gestión y control, extensiones que pueden ser independientes para cada AC.

### 3.3. SELECCIÓN DE TECNOLOGÍA FIRMA ELECTRÓNICA

#### Diferencias entre (PGP/GPG) y X.509

##### En PGP

- Cada usuario es su AC  
Firma a las personas en quién confía  
Otros usuarios, no tienen porqué confiar
- No hay jerarquía de AC s  
No existe ningún «superusuario» que firme al resto
- Dependencia (*al perder la clave privada*)
- Niveles de confianza  
¿Confío en los amigos de mis amigos?  
¿Que hacemos con las claves firmadas por terceras personas?

##### En X.509

- Confiamos en la AC  
y por tanto en todos los usuarios que haya firmado
- La ACs (legales) confían entre sí  
y por tanto confiamos en todos los usuarios certificados
- Los certificados no se limitan sólo a personas  
Servidores, clientes y código
- El encargado de nuestro certificado es la AC
  - Admisión de certificados
  - Autenticación del usuario
  - Distribución de certificados
  - Anulación de certificados.
  - Almacén de certificados

Para el trabajo de tesis se utilizará Certificados S/MIME, en el estándar X.509, para crear estos certificados de utilizara OpenSSL cuya herramienta en línea de comandos hace posible realizar operaciones necesarias con certificados. Estos certificados que son usados para servicios de correo electrónico firmado y cifrado, que se otorgan generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Rechazo. También se puede cifrar el mensaje con la llave pública del destinatario, lo que proporciona Confidencialidad al envío.

Estos certificados se utilizarán a través del cliente de correo Microsoft Outlook Express y serán instalados en Internet Explorer.

### **3.3.1. CREACIÓN DE UNA AUTORIDAD CERTIFICADORA Y CERTIFICADOS CLIENTES**

Para crear un certificado válido necesitamos una autoridad certificadora que nos dé un certificado raíz o nos firme los certificados a usar. Si queremos que nuestros certificados tengan validez en todo el mundo, sin interacción del usuario debemos contratar una entidad certificadora. Si es para uso interno podemos crear nosotros un certificado raíz AC para nuestra red e instalarlo.

Para crear un certificado raíz se utilizará OpenSSL cuya herramienta de la línea de comandos del mismo nombre, permite realizar todas las operaciones necesarias con certificados y el certificado que crea es un certificado del estándar x509.

- **Pasos para crear una autoridad certificadora y certificados digitales**

Crear una autoridad certificadora

1. Crear la Autoridad Certificadora

```
# ./CA.pl -newca
```

2. Exportar el certificado de la CA a formato DER

```
# openssl x509 -inform PEM -outform DER -in demoCA/cacert.pem -out  
demoCA/cacert.der
```

3. Solicitar un certificado nuevo

```
# ./CA.pl -newreq
```

4. Firmar el certificado con la Autoridad Certificadora

```
# ./CA.pl -sign
```

5. Exportar la clave privada del certificado sin contraseña

```
# openssl rsa < newreq.pem > servidor-key.pem
```

6. Convertir a PKCS12 (no teclear clave de exportación)

```
# openssl pkcs12 -export -in newcert.pem \ -inkey servidor-key.pem -out  
servidor.p12 \ -certfile demoCA/cacert.pem -noiter -nomaciter
```

7. Renombrar el certificado en formato PEM

```
# mv newcert.pem servidor.pem
```

8. Convertir el certificado a formato DER

```
# openssl x509 -inform PEM -outform DER -in servidor.pem -out  
servidor.der
```



Repetir desde el paso 3, para generar el certificado del cliente cambiando los nombres de archivo "servidor" por el nombre del "usuario".

Con los pasos anteriormente descritos se tiene la autoridad certificadora y los certificados clientes. Si el cliente es Windows se importa directamente el archivo pkcs12 que incluye la clave privada y el certificado de la AC, el cual será instalado en el navegador Internet Explorer [URL4].

- **Autoridades Certificadoras chilenas**

Los distintos certificados que emiten estas autoridades certificadoras tienen diferente valor.

- <http://www.acepta.com>: Certificado de correo seguro tiene un valor de \$ 9.990 IVA incluido anualmente.
- <http://www.cnc-once.cl>: Certificado de correo seguro tiene un valor de US\$10 anualmente.
- <https://www.e-certchile.cl>: Certificado de correo seguro tiene un valor de US\$ 10 + IVA anualmente.

La manera más sencilla de crear certificados X.509 en Linux es mediante el mandato openssl y sus herramientas auxiliares. Generalmente en la distribución de Red Hat se instala en `/usr/share/ssl/misc/CA`.

## **CAPITULO 4 DISEÑO E IMPLEMENTACION DEL PROTOTIPO**

### **4.1. IMPLEMENTACIÓN**

Seleccionada la tecnología GroupWare que es el software OpenGroupware y la tecnología de firma electrónica a utilizar, los certificados digitales, ambas tecnologías se implementaron en el Servicio de Salud de Valdivia.

#### **4.1.1. MODELO**

El acceso al software OpenGroupware es a través de un visualizador (browser), como por ejemplo Internet Explorer de Microsoft o Netscape Navigator de Netscape. Se integra al sitio oficial del Servicio de Salud Valdivia en la dirección, <http://www.ssvvaldivia.cl/OpenGroupware>.

La implantación de este software permite:

- Facilitar la comunicación (mayor rapidez, claridad y persuasión).
- Ahorro de tiempo y costos.
- Permitir juntar múltiples experiencias y perspectivas.
- Formar grupos con intereses comunes.
- Facilitar la resolución de problemas en grupo.
- Permitir nuevas formas de comunicación.
- Gestión de proyectos.

La implementación de firma electrónica se realizó por medio del cliente de correo Microsoft Outlook Express. Los certificados a usar se crearon de la forma descrita en la página 85 (*Pasos para crear una autoridad certificadora y certificados digitales*).

La distribución de estos certificados, se realizó a través de una autoridad certificadora en el Servicio de Salud Valdivia, que emitirá los certificados necesarios, bajo la responsabilidad de un administrador. Estos certificados tendrán validez de un año por razones de seguridad, y serán utilizados en el envío seguro de correo electrónico a través de Outlook Express.

El acceso al programa OGo y la distribución de grupos para el diseño del prototipo inicialmente se realiza en las oficinas internas del Servicio de Salud. Tendrán acceso los jefes o directores de cada departamento, más adelante se pretende distribuir de la siguiente manera (*Tabla N°8: Distribución de grupos*).

Cada funcionario tendrá en su PC su certificado digital que le otorga la facultad de firmar y/o encriptar su correspondencia.

Para optimizar el envío de correos, la creación de listas de correo tiene la ventaja de agrupar a múltiples direcciones. Cuando se envía un mensaje a la dirección electrónica de la lista, el mensaje se distribuye automáticamente a todos los miembros ó suscriptores de la misma. Se utilizó *Majordomo*, programa gestor de listas de correo, para los grupos de Informática, recursos humanos y otros.

<b>SERVICIO DE SALUD VALDIVIA</b>				<b>GRUPOS</b>									
				<b>CIRA</b>	<b>AUGE</b>	<b>Diplomado</b>	<b>Sigfe</b>	<b>Sirh</b>	<b>CBC</b>	<b>PE</b>	<b>Coldas</b>	<b>Centro Oncológico</b>	<b>CG</b>
Dr.	Joel Arriagada G.	Director Servicio de Salud Valdivia	jarriaga@ssvaldivia.cl	X	X	X				X	X	X	X
Dra.	Mónica Gil Diez de Medina	Subdirector Médico	mgil@ssvaldivia.cl	X	X	X				X	X		X
Sr	Bernardo Villablanca LL.	Subdirector Administrativo	bavillab@ssvaldivia.cl	X	X	X				X	X		X
Sr.	Marco Rosas Leal	Asesor Jurídico	mrosas@ssvaldivia.cl									X	
Sra.	Marianela Beltrán E.	Auditora	mbeltran@ssvaldivia.cl		X	X				X			
Sr.	José Eduardo Barrientos N.	Jefe Depto. Recursos Humanos	ebarrien@ssvaldivia.cl	X		X		X	X	X			X
Sr.	Juan Reyes Durán	Jefe Depto. Informática	jreyes@ssvaldivia.cl	X	X	X	X	X	X	X		X	
Sr.	José Bertulini C.	Jefe Depto. Recursos Físicos	ebertuli@ssvaldivia.cl			X							
Sra.	Sara Saavedra A.	Jefe Bienestar de Personal	bienessv@ssvaldivia.cl					X					
Sra.	Guisela Isla V.	Jefe Depto. Finanzas	gisla@ssvaldivia.cl	X	X	X	X		X	X			X
Dra.	María Enriqueta Bertrán V.	Jefe Depto. Programa de las Personas	mbertran@ssvaldivia.cl										X
Dra.	Katy Heise Mora	Jefe Depto. Atención Primaria	kheise@ssvaldivia.cl										X
Sr.	Waldo Gallardo Gallardo	Jefe Depto. Prog. Sobre el ambiente	wgallard@ssvaldivia.cl										X
Dra.	Helga Jacque Azabe	Presidente Compín	hjacque@ssvaldivia.cl										X
Sra.	Eugenia Coronado V.	Jefe Unidad Farmacia	ecoronad@ssvaldivia.cl										X
Sra.	Norma Isla Victoriano	Jefe Unidad de Estudios y Proyectos	nisla@ssvaldivia.cl			X				X		X	
Sra.	Astrid Scheuch Ferman	Jefe Unidad de Capacitación	ascheuch@ssvaldivia.cl					X	X				X
Sra.	Erica Medina Díaz	Jefe Unidad de Abastecimiento	emedina@ssvaldivia.cl			X	X			X			
Sr.	Daniel Torres Muñoz	Jefe Unidad de Subsidios	dtorres@ssvaldivia.cl					X					
Sr.	Carlos Campillo Catalán	Jefe Oficina de Sueldos	ccampill@ssvaldivia.cl					X					
Srta.	Veronica Tuchie Jadure	Jefe Unidad de Estadísticas e Inf. Salud	vtuchie@ssvaldivia.cl										X
Srta.	Rosa Leal Velasquez	Periodista Unidad Comunicaciones	rleal@ssvaldivia.cl										X
<b>HOSPITALES AREA</b>													
Dr.	Javier León Rivera	Director Hospital Base Valdivia	jleon@ssvaldivia.cl	X	X	X				X	X	X	X
Dr	Rodrigo Cabrera Seguel	Director Hospital Corral (101)	somecorr@telsur.cl	X	X	X				X	X	X	X
Dr	Hernan F. Sade Calles	Director Hospital Los Lagos (102)	somelagos@telsur.cl	X	X	X				X	X	X	X
Dra	Carolina Sepulveda Villegas	Directora Hospital Lanco (103)	somelanco1@telsur.cl	X	X	X				X	X	X	X
Dr	Alberto Bilbao Labrin	Director Hospital La Unión (104)	someunion@telsur.cl	X	X	X				X	X	X	X
Dr	Jaime Vallejos Vallejos	Director Hospital Río Bueno (105)	someriob@telsur.cl	X	X	X				X	X	X	X
Dr	Rodrigo Bertín L.	Director Hospital Paillaco (106)	somepai@telsur.cl	X	X	X				X	X	X	X
Hna.	Franciska Häring Schneider	Directora Hospital Panguipulli (201)	hospangui@telsur.cl	X	X	X				X	X	X	X
Sra.	Alicia Schirmer Ijrra	Directora Hospital Santa Elisa	hos_staelisa@surnet.cl	X		X							X
<b>CONSULTORIOS VALDIVIA</b>													
Dra.	Carmen Barudi Labrín	Directora Consultorio Externo Valdivia	somextval@telsur.cl	X	X	X			X	X			X
Sr.	Patricio Hermosilla A.	Director Consultorio Gil de Castro	cesfamgl@telsur.cl	X		X				X			X
Srta.	Cecilia Veliz Jofré	Directora Consultorio Las Animas	cesfamla@telsur.cl	X		X				X			X
Sr.	Patricio Rojas B.	Director Consultorio Angachilla	cefamangachilla@telsur.cl	X		X				X			X
Sra.	Claudia Quiroga Q.	Directora Consultorio Niebla	cesfamnbla@telsur.cl	X		X				X			X

Tabla N°8: Distribución de grupos

#### 4.1.2. ARQUITECTURA

La arquitectura global del modelo propuesto se compone de un, Servidor Groupware y Cliente Web, tal como se aprecia en fig. N° 5.

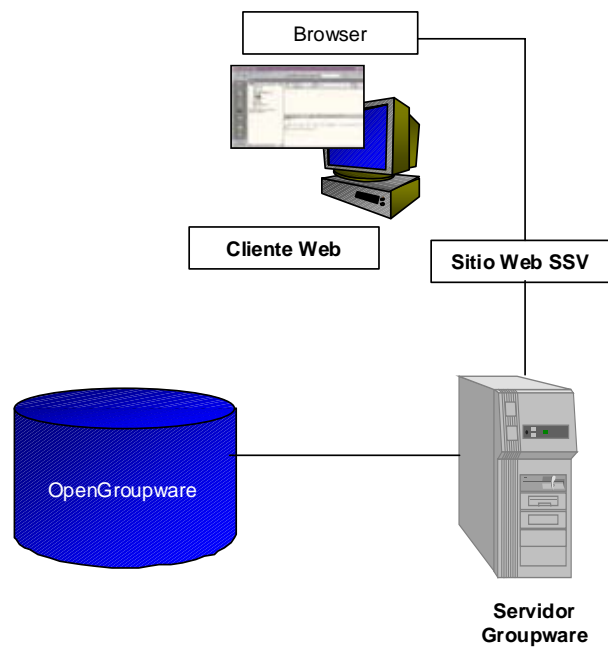


Figura N°5: Arquitectura Instalación OpenGroupware

### 4.1.3. SOLUCIONES TECNOLÓGICAS

- **Recursos**

Los recursos tecnológicos utilizados en la solución propuesta son:

#### **Software Cliente**

- Microsoft Windows 98 o superior
- Internet Explorer 5.
- Microsoft Outlook Express 5

#### **Software servidor Groupware**

- *Linux Red Hat9*
- Apache Server 2.0.40
- Servidor de correo Sendmail 8.12.8
- Openssl

#### **Hardware servidor Groupware**

- Pentium IV, 2,8 mhz, 512 Ram, 80 Gb de disco duro

- **Costos del hardware y software**

#### **Costo del Software:**

- OpenGroupware (GRATIS): m\$ 0
- Sistema Operativo (GRATIS): m\$ 0
- Browser (GRATIS): m\$ 0

#### **Costo del Hardware:**

- Servidor: m\$ 800

## **4.2. POLÍTICAS DE RESPALDO DE INFORMACIÓN**

Actualmente es indispensable mantener una copia de los archivos más importantes de todos los usuarios de la red, dicho procedimiento es responsabilidad del Encargado de Soporte que es el encargado de respaldar el Servidor Groupware, el cual debido a la gran cantidad de requerimientos por parte de los usuarios puede de algún modo, no realizar dicho respaldo de manera constante, originando esto un desastre en el momento de un daño físico a cualquier dispositivo de almacenamiento.

Es importante considerar 2 servidores uno en el mismo establecimiento del Servicio de Salud Valdivia y el segundo en otro establecimiento, para evitar la pérdida de información en caso de algún daño en el edificio.

El medio de Respaldo a utilizar son cintas DAT(Digital Audio Tape o Cinta Digital de Audio). Estos medios son de un uso muy extendido, con enormes capacidades de almacenamiento y además son reutilizables.

- **Respaldo de servidores**

Realizar respaldos de Base de Datos y servidor de correo, con una frecuencia diaria de Lunes a Viernes, reutilizando la cinta correspondiente la semana siguiente.

En forma semanal realizar respaldos reutilizando las cintas al mes siguiente. Además realizar respaldo mensual reutilizando las cintas al año siguiente. Una vez al mes realizar un respaldo de Seguridad que se traslada a otro edificio reutilizando la cinta al mes siguiente.

Realizar reemplazo de cintas cada 7 meses en los respaldos con mayor frecuencia.

Los jefes de cada departamento dentro del Servicio de Salud Valdivia son los responsables de hacer respaldo a sus equipos, el envío y recepción de



correos y firma electrónica de estos se realiza en el cliente de correo Microsoft Outlook Express, respaldar los mensajes enviados y recibidos, de la forma ya descrita, con la opción exportar mensajes que trae el cliente de correo Microsoft Outlook.

- **Para recuperar un correo específico**

Al realizar respaldo de información en forma diaria, es posible recuperar un correo específico.

En el programa Outlook es posible crear carpetas que quedan almacenadas en el PC. local y realizar búsquedas especificando una carpeta, entre fechas por asunto, por emisor, receptor, por contenido.

En OGo es posible realizar búsquedas por carpetas, subcarpetas, remitente, asunto, contenido, estado del correo(*leído, no leído*).

### 4.3. SEGURIDAD E INTEGRIDAD DEL SISTEMA

Aquí se describe la seguridad que involucra la utilización de certificados digitales, además se recomienda utilizar el protocolo Secure Socket Layer para proporcionar seguridad durante la transmisión de datos.

#### 4.3.1. SEGURIDAD EN EL USO DE CERTIFICADOS DIGITALES

- **Proteger el uso del certificado con una contraseña**

Las contraseñas son importantes si se está trabajando en un entorno donde otros pueden acceder a su sistema, ya sea físicamente o a través de la red, por eso se recomienda que el propietario de un certificado digital no de su contraseña a nadie, ya que les permitiría utilizar su certificado para suplantarle.

Las contraseñas más seguras tienen como mínimo 8 caracteres, que pueden incluir letras, números y símbolos

Internet Explorer, permite añadir una contraseña para cada certificado, esta contraseña es requerida cada vez que se usa ese certificado (*en la firma y encriptación de correos, en la lectura de correo cifrado o firmado y en la exportación de certificados*) para evitar que alguien utilice el PC para realizar operaciones.

La contraseña sólo se puede poner a la hora de la importación o instalación del certificado personal seleccionando el nivel *Alto* de los tres niveles de seguridad que se permiten:

1. Nivel *Alto*: Con este nivel el sistema avisa al usuario que el certificado se va a usar y pide una contraseña para ello (*se recomienda utilizar este nivel*).
2. Nivel *Medio*: Con este nivel el sistema avisa que el certificado se va a usar

3. Nivel *Bajo*: Con este nivel el sistema utiliza automáticamente el certificado, sin comunicación al usuario

advertencia: la contraseña no puede recuperarse. Si es olvidada, se perderá el certificado.

#### **4.3.2. REVOCACIÓN DE CERTIFICADOS**

La Autoridad de Certificación (AC) es el órgano que se encarga de firmar digitalmente los certificados, garantizando la total integridad del mismo y la propiedad de la clave pública contenida. La confianza de los usuarios es una cuestión primordial para el éxito de su funcionamiento, y toda entidad que pretenda expedir este tipo de mecanismos de seguridad tiene que contemplar no sólo su expedición sino también su posible revocación.

Un certificado puede dejar de ser válido y, por lo tanto, ser revocado, si los datos de propiedad han dejado de ser válidos, o se han comprometido por cualquier causa las claves privadas que contiene, o ha finalizado el tiempo o ha variado en contexto para el que fue emitido.

Al estar basados en el uso de claves no conviene que éstas sean válidas por periodos de tiempo largos, ya que uno de los principales problemas del manejo de claves es que cuanto más vida tienen más fácil es que alguien extraño se apodere de ellas. Además, con el paso del tiempo los equipos informáticos van teniendo cada vez más poder de cálculo, por lo que es conveniente que cada cierto tiempo se vaya aumentando el tamaño de las claves criptográficas. Por este motivo los Certificados Digitales tienen estipulado un periodo de validez, que suele ser de un año.

### **4.3.3. SEGURIDAD SEGRE SOCKET LAYER**

El Segure Socket Layer (SSL) es un protocolo muy utilizado y de carácter abierto que desarrolló la empresa Netscape para proporcionar seguridad durante la transmisión de datos, este protocolo fue aceptado como un estándar Web para la autenticación y encriptación de las comunicaciones en un sistema cliente-servidor asegurando un canal de comunicaciones entre éstos.

Este protocolo define una interfaz en la que un cliente y un servidor pueden realizar codificación de información, asegurar la integridad del mensaje y validar la autenticación del usuario.

Este esquema es típicamente utilizado entre navegadores y servidores Web sobre todo en los sistemas de pago por Internet que utilizan tarjetas de crédito. Esta herramienta sirve para comunicaciones bidireccionales y está basado en la aplicación conjunta de criptografía asimétrica y simétrica que lo convierte en protocolo híbrido en cuanto a encriptación, además utiliza certificados y firmas digitales.

SSL proporciona funciones de seguridad necesarias, que una solución de seguridad debe tener para el comercio electrónico actual, como son:

a) Confidencialidad, mediante conexiones cifradas, ya que aunque la información caiga en manos incorrectas, ésta será indescifrable.

b) Autenticación del servidor, ya que el usuario puede asegurarse de la identidad del servidor al que se conecta, opcionalmente puede autenticar al cliente para que el servidor conozca la identidad del usuario con el fin de decidir si le permite el acceso a áreas protegidas.

c) Integridad de los mensajes, ya que detecta modificaciones en la información después que ésta viaja por la red.

- **SSL funciona de la siguiente manera:**

El cliente se conecta a través de su navegador a un servidor que soporte SSL y envía una solicitud para iniciar una comunicación o sesión segura [Val02].

1. El servidor envía una respuesta si soporta o no SSL.
2. El cliente y el servidor comienzan a negociar la conexión SSL e intercambian información de seguridad, donde se hace la autenticación del servidor y opcionalmente del cliente, se determinan que algoritmos de criptografía serán utilizados, el identificador de sesión, los algoritmos de compresión y se genera una clave secreta por parte del navegador del cliente, para ser utilizada durante el intercambio de mensajes en la comunicación SSL. Después de verificar la identidad del servidor y de la generación de la clave aleatoria distinta para cada sesión, ésta se cifra con la llave pública del servidor y es enviada a éste.
3. El servidor y el cliente pueden ahora intercambiar información de forma segura utilizando la clave secreta acordada en la sesión, adicionalmente cada vez que el servidor o el cliente deseen enviar un mensaje al otro se genera un resumen del mensaje utilizando un algoritmo denominado Hash, el que también se cifra y se envía para la verificación de la integridad del mensaje.

Un sitio Web seguro mediante SSL se reconoce por una imagen de un candado, que aparece en esquina inferior izquierda de la página Web. La mayoría de los navegadores Web son compatibles con el protocolo SSL y una característica a destacar es la capacidad de encriptación de la comunicación la que puede ser de 56 o 128 bits dependiendo del navegador del cliente y del certificado digital instalado en el servidor Web.

## CAPITULO 5 DESCRIPCION FUNCIONAMIENTO

### 5.1. DESCRIPCION

Se describe la funcionalidad del Software OpenGroupware a través de un ejemplo que muestra como opera, al ser accedido por un usuario desde un navegador.

En la figura N°6, se muestra la pantalla inicial del Software, el usuario debe ingresar su nombre de usuario y contraseña.



Figura N°6: Acceso a OGo,

En el “visor de preferencias” como se muestra en la Figura N°7, el usuario puede personalizar la interfaz del programa, cambiar lenguaje, horarios, contraseña y otras. Además es posible personalizar el programa activando y desactivando funcionalidades de acuerdo a sus requerimientos.



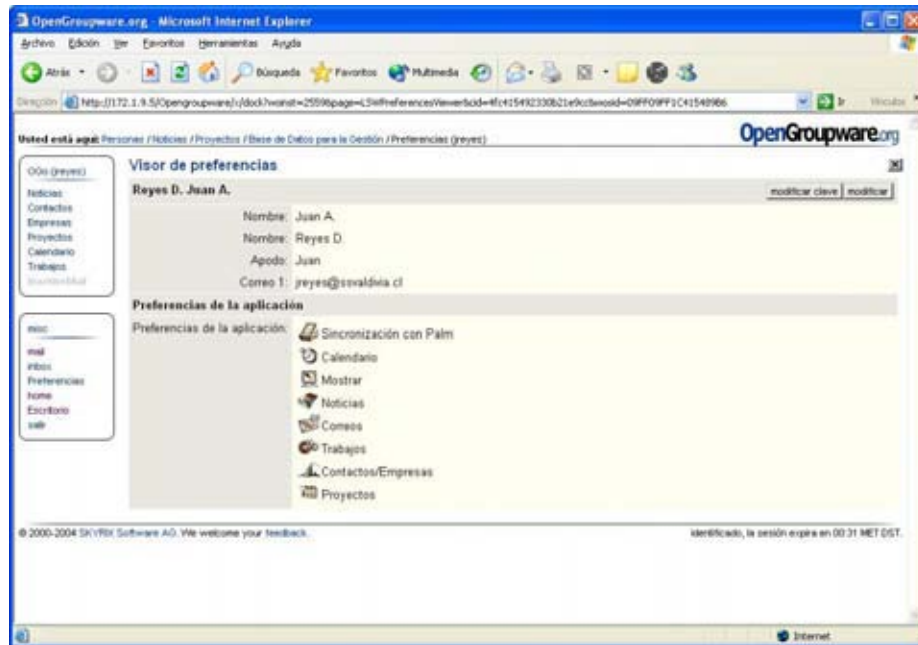


Figura N°7: Visor de preferencias de un usuario

En la figura N°8 se muestra la pantalla de “Noticias”, esta opción entrega información que el usuario necesita, despliega las citas y trabajos pendientes.

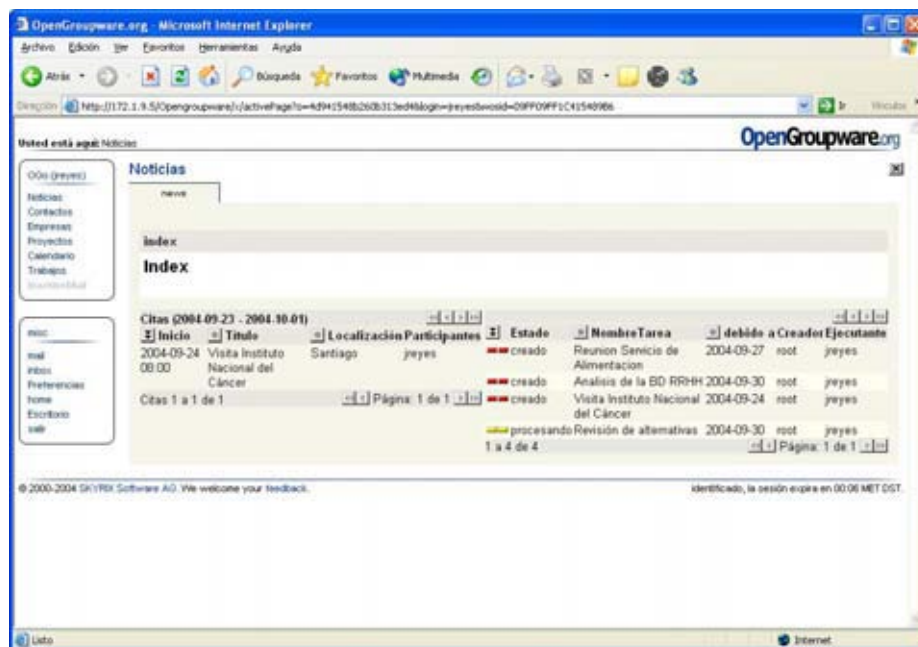


Figura N°8: Visor de noticias, para el usuario

En la aplicación proyectos, se despliegan todos los proyectos que el usuario esta involucrado, como se muestra en la Figura N°9.

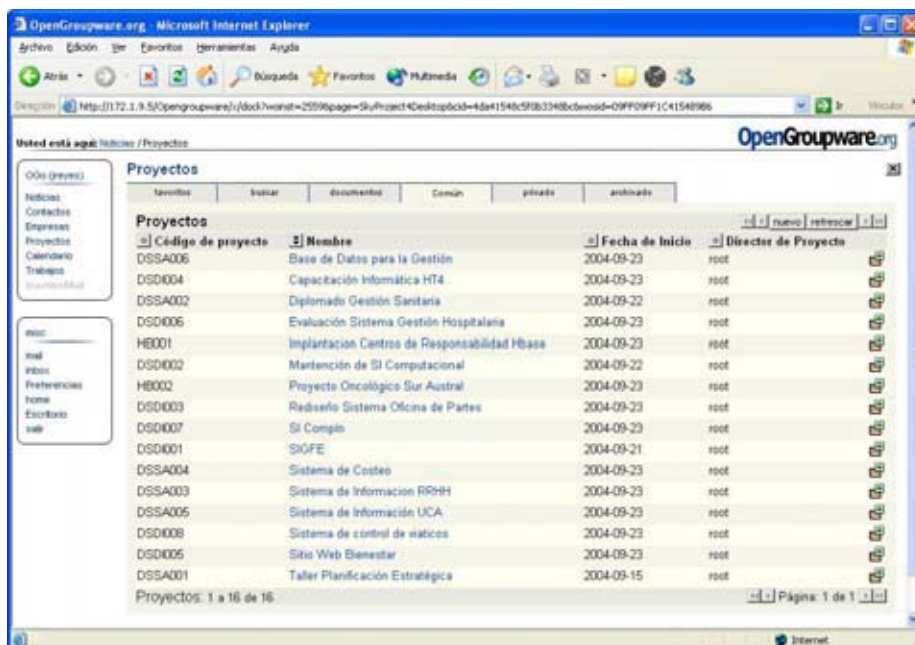


Figura N°9: Listado de proyectos

A cada proyecto es posible asignar documentos y tareas, como se muestran en las Figuras N°10 y N°11.

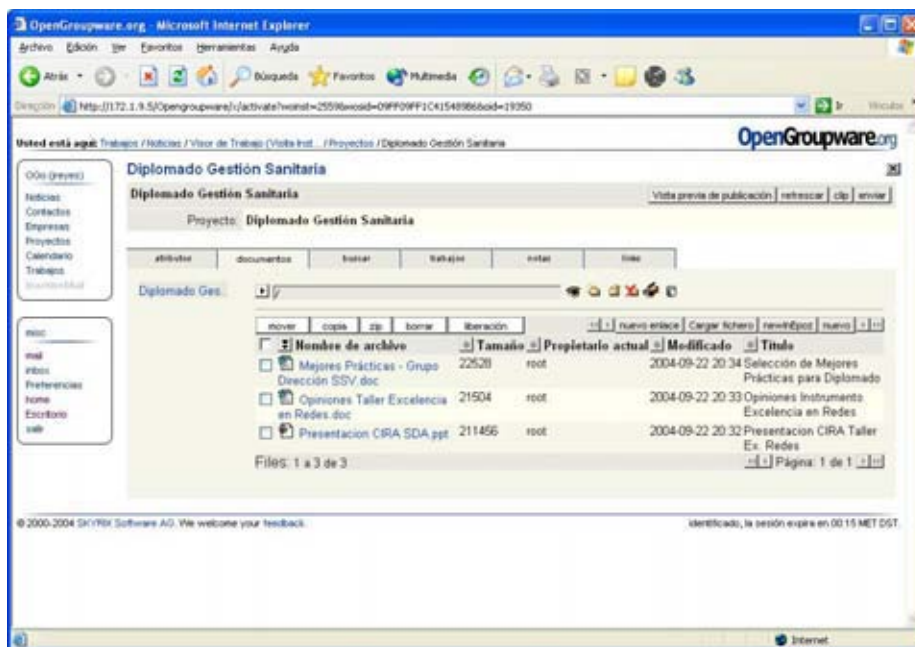


Figura N°10: Detalle de un proyecto seleccionado, opción documento

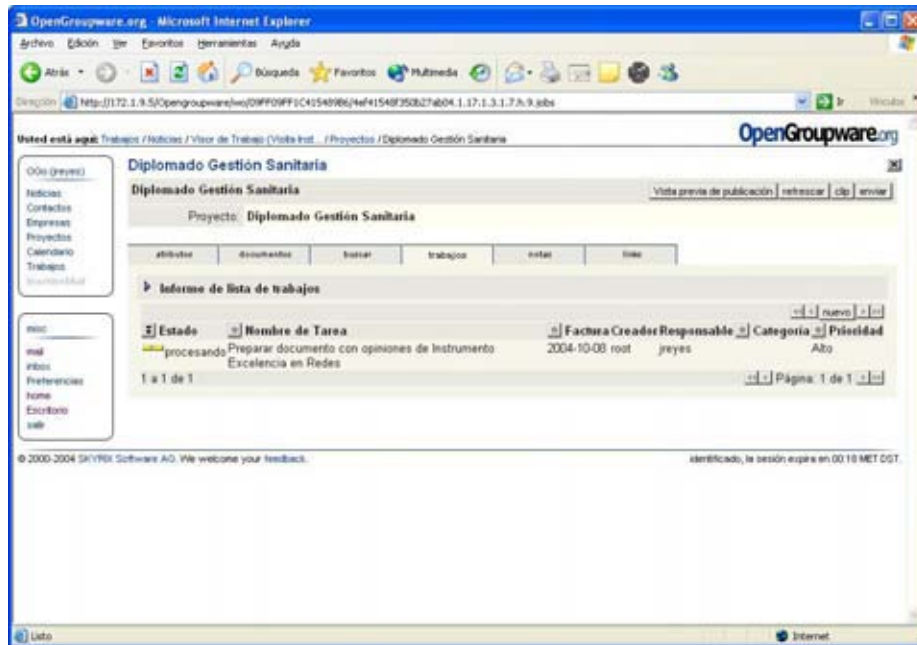


Figura N°11: Detalle de un proyecto seleccionado, opción tareas

En la opción Contactos, es posible visualizar datos de un contacto específico, información personal, u otra información relacionada. Como se muestra en la Figura N°12.

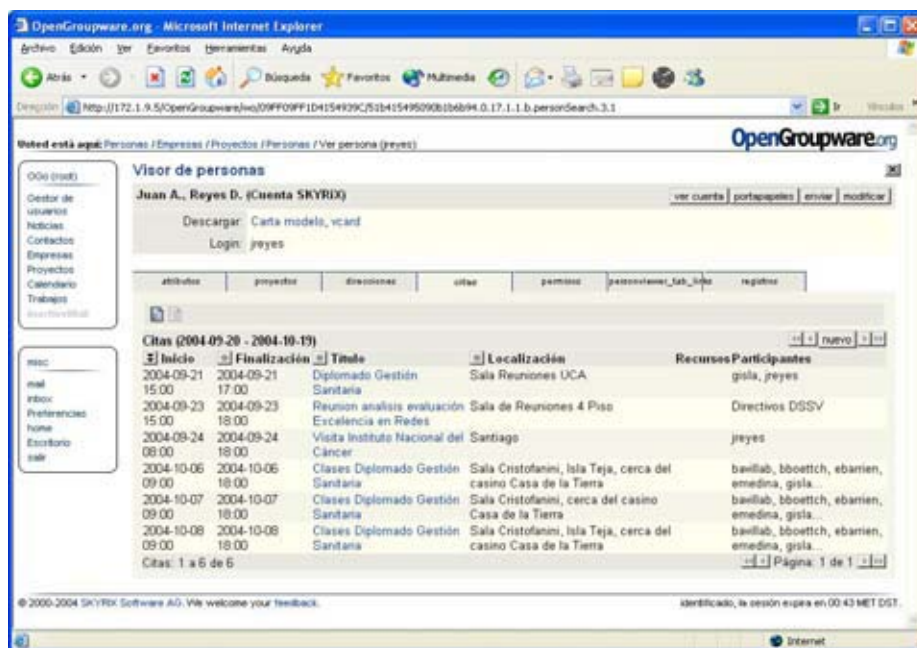


Figura N°12: Visor de personas, detalle de una cuenta de usuario

El calendario de Ogo, Figura N°13, muestra las citas del usuario, esta información se puede mostrar por día, semana, mes y año.

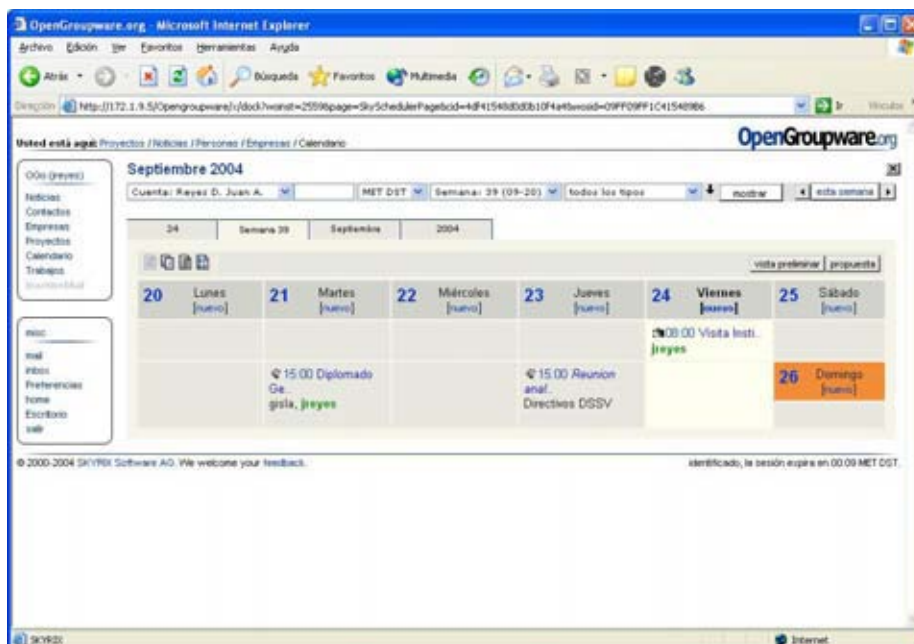


Figura N°13: Listado de citas del usuario(Agenda Compartida)

En la Figura N°14, se muestran los trabajos de un usuario, los trabajos pendientes, y su estado de avance, los trabajos que le han sido delegados y los trabajos ya realizados.

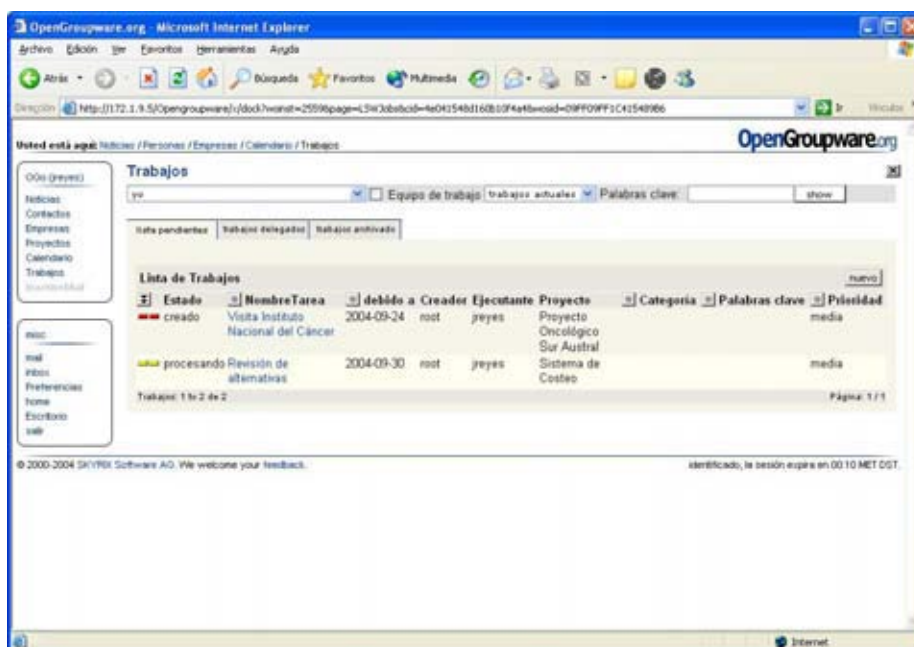


Figura N°14: Listado de trabajos del usuario

En la Figura N°15 se visualiza el correo de OGo, el usuario puede crear un árbol de carpetas para manejar ordenadamente sus correos.



Figura N°15: Visor de correo electrónico del usuario

En la Figura N°16 y Figura N°17, se muestra un Certificado digital de un usuario, creados con los pasos descritos en la página 85(Pasos para crear una autoridad certificadora y certificados digitales).



Figura N°16: Certificado Digital.

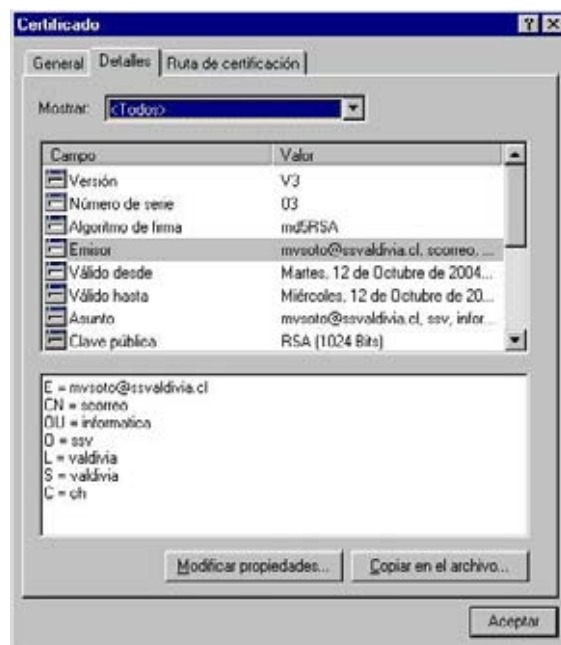


Figura N°17: Detalle certificado

Una vez instalado el certificado digital, se configura una cuenta de correo de Outlook Express para que se puedan enviar mensajes firmados digitalmente utilizando esa cuenta. En la Figura N°18 y Figura N°19 se muestra un correo electrónico firmado y cifrado digitalmente.

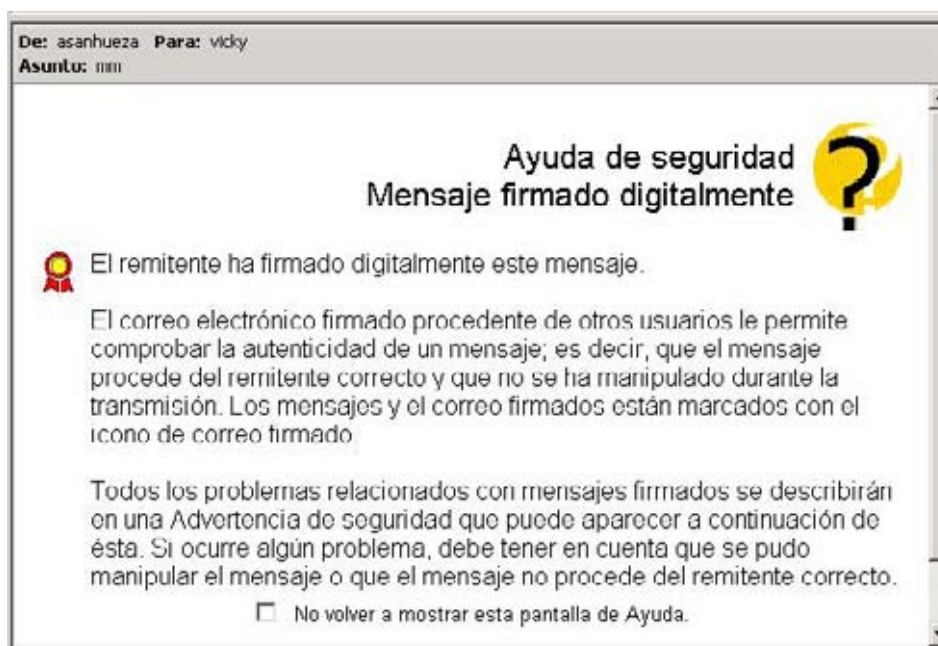


Figura N°18: Correo Firmado electrónicamente, con M. Outlook Express

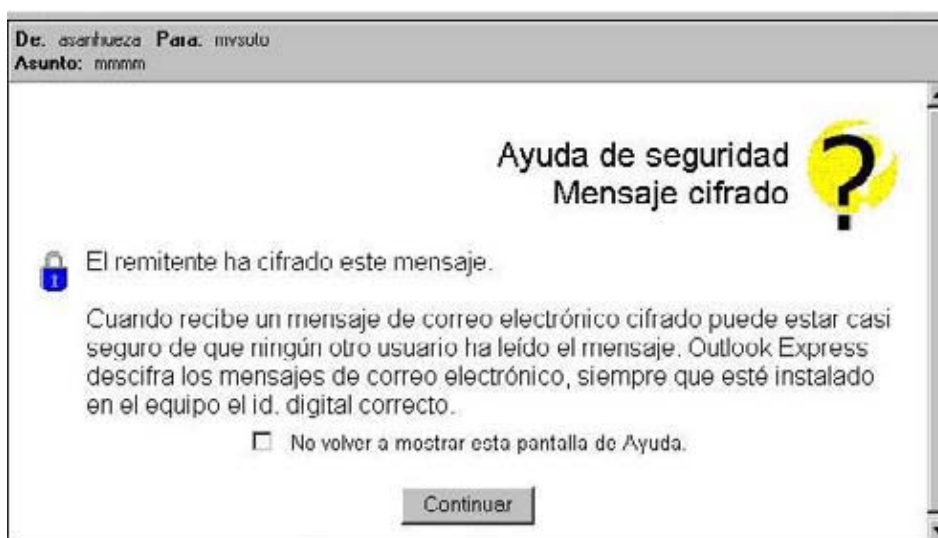


Figura N°19: Correo Cifrado electrónicamente, con M. Outlook Express

## **CAPITULO 6 CONCLUSIONES Y MEJORAS**

En este capítulo se discuten las conclusiones y las mejoras a efectuar sobre el prototipo de mensajería e intercambio electrónico de documentos desarrollado en este trabajo de tesis.

### **6.1. CONCLUSIONES**

La implementación del prototipo Groupware en el Servicio de Salud de Valdivia, permitirá:

- Mejorar la comunicación entre los miembros de diferentes grupos de trabajo, incrementando la productividad de los mismos.
- Disminuir la papelería interna al reemplazarla por correo electrónico debidamente validado a través de la firma electrónica.
- Facilitar los procesos de recuperación mediante un respaldo diario de la información. Esto posibilitará una completa disponibilidad cuando el administrador requiera un documento.
- Servir de prototipo base para replicar este modelo en otros Servicios de Salud.

### **6.2. MEJORAS**

Una posible mejora es que los correos emitidos por medio del cliente Web de OGo sean automáticamente firmados, sin utilizar un cliente de correo como intermediario, en este caso, Microsoft Outlook Express.



## **CAPITULO 7 BIBLIOGRAFIA**

Esta sección contiene una lista de los libros, documentos electrónicos y principalmente trabajos de investigación encontrados en la red y consultados durante la elaboración del presente trabajo de tesis, también contiene una lista de direcciones en Internet donde se puede encontrar información adicional respecto de los distintos temas tratados.

### **7.1. LIBROS Y PUBLICACIONES**

- [Aut03]Autoridad de certificación de la Generalitat Valenciana, Dirección General de telecomunicaciones y Modernización, Presidencia de la Generalitat Valenciana “Manual de instalación de certificados digitales en fichero” fecha de publicación 11 de abril de 2003.
- [Cer97]Cerdeira Bravo Claudio Andrés, “Análisis y diseño de una red GroupWare para Holding VTR ” Tesis de grado para optar al título de ingeniero civil en informática, Universidad Austral de Chile 1997.
- [Eva04]Evaluación de Lotus Notes, Elaborado por: Subdirección de Sistemas L.I María Guadalupe Guadiana García -Febrero 2004
- [Ley02]Ley chilena 19799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma. Publicación 25 de Marzo 2002.
- [Mar00]Mario G. Piattini, José A. Calvo Manzano, Joaquín Cervera, Luis Fernández 2000] “Análisis y diseño detallado de Aplicaciones Informáticas de Gestión” ALFAOMEGA GRUPO EDITOR, s.a
- [Sky02] Manual de Administrador SKYRIX\_adminmanual. Versión 4.1. Publicación 23 de Enero 2002.

- [Sky01] Manual de usuario, SKYRIX\_WebGroupware. versión 4.0. Publicación 01 Agosto 2001.
- [Rei03] Reiner Jung Project Manual de instalación eGroupWare How\_to\_install\_and\_secure\_eGroupWare\_03. Publicación 23 de Noviembre 2003 .
- [Rau04] “Software de Código abierto” Raul Saroka rsaroka@ciudad.com.ar. Publicación Marzo 2004.
- [Val02] Vallejos Arcos Carlos Alberto, “Diseño de una pki para el desarrollo de aplicaciones bancarias seguras sobre internet mediante firma digital”. Tesis de grado para optar al título de ingeniero civil en informática, Universidad Austral de Chile 2002.
- [Met03] Metodología de proyectos Informáticos MIDEPLAN, Publicación 22 Agosto 2003.
- [Tom03] Tommy Tsui. Opengroupware.org, *A brief introduction of Opensource groupware solutions*. Publicación Noviembre 2003.

## 7.2. DIRECCIONES INTERNET

- Windows Privacy Tools, Herramientas de privacidad para Windows

[URL1] <http://winpt.sourceforge.net/es/index.php>.

- Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información.

[URL2] <http://www.csi.map.es/csi/metrica3/index.html>.

- Criptografía y firma electrónica

[URL3] [http://www.htmlweb.net/seguridad/cripto/cripto\\_4.html](http://www.htmlweb.net/seguridad/cripto/cripto_4.html)

- Creación de una autoridad certificadora

[URL4] <http://www.wireless-station.com/print.php?sid=80>

- Características del producto Notes

[URL5] <http://www.druidics.com.ar/dsi/druidics/home.nsf/0/739076e25fd589fa032568f800740da0?OpenDocument>

- Manual de referencia Lotus Notes 5

[URL6] <http://club.telepolis.com/roccorocco/>

- Características de Exchange

[URL7] <http://www.sie.es/redes05.htm>

- Software Libre, eGroupware y OpenGroupware

[URL8] <http://www.opensource.org.ar/es-osd.html>

[URL9] <http://www.egroupware.org/>

[URL10] <http://www.opengroupware.org/>

[URL11] <http://www.softwarelibre.cl/print.php>

- Instalar Ogo en Rh9

[URL12] [http://sukka.jct.ac.il/~yedidia/ogo\\_rh.html](http://sukka.jct.ac.il/~yedidia/ogo_rh.html)

## ANEXO A MANUAL DE INSTALACION OGo

### Instalación de OpenGroupware en redhat9

Para instalar Ogo se debe seguir los siguientes pasos: [URL12]

- Descargar todos los rpms

<http://www.opengroupware.org/packages/rpm-all-latest.tar.bz2> (21MB)

<ftp://ftp.opengroupware.org/packages/rpm-all-latest.tar.bz2> (21MB)

- Instalar los Paquetes RPM

Instalar todos los rpm, escribiendo: `rpm -iUvh *.rpm`

- Configurar la Base de Datos

OGo almacena la mayoría de sus datos en una base de datos relacional. OGo tiene soporte para PostgreSQL y FrontBase, y se recomienda PostgreSQL al estar disponible en casi todas las distribuciones GNU/Linux y ser por lo tanto más sencilla de instalar.

Para conectar OGo con PostgreSQL, es necesario inicializar Postgresql

```
# /sbin/service postgresql start
```

1) Configurar el servidor PostgreSQL para que acepte conexiones TCP. Estableciendo la variable "`tcpip_socket`" al valor "`true`" en el archivo `postgresql.conf`, (`/var/lib/pgsql/data/`).

2) Modificar el archivo `pg_hba.conf`, (`/var/lib/pgsql/data/`), para permitir conexiones TCP desde la máquina en que esta instalado OpenGroupware.org (normalmente localhost).

--snip--

```
local all all trust
host all all 127.0.0.1 255.255.255.0 trust
host all all 0.0.0.0 255.255.255.255 reject
```

--snap--

- Reiniciar PostgreSQL después de aplicar los cambios (por ej.

```
# /sbin/service postgresql restart.
```

- Continuar con los siguientes pasos como usuario root.

```
# su - postgres
```

```
$ createdb ogo
```

```
$ createuser -A -D ogo
```

```
$ exit
```

```
# su - opengroupware
```

```
$ cd /opt/opengroupware.org/Database/PostgreSQL
```

```
$ psql ogo -U ogo
```

```
Welcome to psql 7.3.3, the PostgreSQL interactive terminal.
```

```
Type: \copyright for distribution terms
```

```
  \h for help with SQL commands
```

```
  \? for help on internal slash commands
```

```
  \g or terminate with semicolon to execute query
```

```
  \q to quit
```

```
ogo=> \i pg-build-schema.psql
```

```
[output cut]
```

```
ogo=> \q
```

```
$ source $HOME/OpenGroupware.org.sh
```

```
$ Defaults write NSGlobalDomain LSAdaptor PostgreSQL72
```

```
$ Defaults write NSGlobalDomain LSModelName
```

```
OpenGroupware.org_PostgreSQL
```

```
$ Defaults write NSGlobalDomain LSConnectionDictionary '{databaseName = ogo; hostName = localhost; password = ""; port = 5432; userName = ogo}'
```

```
$ Defaults write NSGlobalDomain NGBundlePath
```

```
/opt/opengroupware.org/Library/OpenGroupware.org
```

```
$ Defaults write NSGlobalDomain LSAttachmentPath
```

```
/opt/opengroupware.org/documents
```

```
$ exit
```

```
# mkdir /opt/opengroupware.org/documents
```

```
# chown opengroupware.skyrix /opt/opengroupware.org/documents
```

```
# ln -s ~opengroupware/WebServerResources/*
```

```
~opengroupware/WOApps/OpenGroupware.woa/WebServerResources/
```

- Edite el archivo (/etc/ld.so.conf ) y agregar las siguientes líneas:

*/opt/opengroupware.org/Libraries/ix86/linux-gnu/gnu-fd-nil*

*/opt/skyrix/system/Libraries/ix86/linux-gnu/gnu-fd-nil*

- Run ldconfig para aplicar los cambios

- Obtener el archivo *opengroupware*

*http://sukka.jct.ac.il/~yedidia/opengroupware* y copiarlo en el

directorio(/etc/init.d/). Y cambie los permisos del archivo u+x

- Como *opengroupware* (su - *opengroupware*) realice estos dos comandos

*echo "source /opt/opengroupware.org/OpenGroupware.org.sh" >>*

*~/.bash\_profile*

*echo "export LD\_ASSUME\_KERNEL=2.4.1" >> ~/.bash\_profile*

- Como root creamos el siguiente enlace para que encuentre la biblioteca de objetos compartida.

*# cd /lib*

*# ln -s libssl.so.0.9.7a libssl.so.0.9.6*

*# ln -s libcrypto.so.0.9.7a libcrypto.so.0.9.6*

- Inicio de OGo OpenGroupware en modo standalone (es decir, sin Apache).

Las desventajas de este paso - sólo la máquina [la suya] es capaz de acceder al servidor de OGo.

Como root inicie *opengroupware* escribiendo:

*# /etc/init.d/opengroupware start*

Ahora en el navegador escribir *http://localhost:20000*, es posible comenzar hacer pruebas (mozilla , internet explorer).

- En el archivo log.OMGo aparece

*May 20 04:25:20 OpenGroupware [3823]: SNS disabled.*

*May 20 04:25:26 OpenGroupware [3823]: |OpenGroupware| CTI Dialers:*

*May 20 04:25:51 OpenGroupware [3823]: |OpenGroupware| SKYRIX instance initialized ..*

*May 20 04:25:51 OpenGroupware [3823]: |OpenGroupware| WOHttpAdaptor listening on address <InetAddress: \*:20000>*

- Configurar apache

Para que funcione OGo con Apache

Inicializar httpd

```
# /sbin/service httpd start
```

1) En modo= proxy es necesario

Adicionar al final del archivo httpd.conf (/etc/httpd/conf) las siguientes líneas

```
#####
```

```
# OpenGroupware proxy
```

```
#####
```

```
ProxyPass /OpenGroupware http://localhost:20000/OpenGroupware
```

```
ProxyPassReverse /OpenGroupware http://localhost:20000/OpenGroupware
```

```
ProxyPass /OpenGroupware.woa http://localhost:20000/OpenGroupware.woa
```

```
ProxyPassReverse /OpenGroupware.woa
```

```
http://localhost:20000/OpenGroupware.woa
```

```
ProxyPass /OpenGroupware.org http://localhost:20000/OpenGroupware.org
```

```
ProxyPassReverse /OpenGroupware.org
```

```
http://localhost:20000/OpenGroupware.org
```

```
#####
```

```
# Activar el modo proxy
```

```
#####
```

```
<IfModule mod_proxy.c>
```

```
ProxyRequests On
```

```
</IfModule>
```

```
#####
```

- Reiniciar Httpd después de aplicar los cambios.

```
# /sbin/service httpd restart
```

Al escribo `http://localhost/OpenGroupware` ¡funciona!

- 2) Lo siguiente es probar en `mod_ngobjweb` para Apache 2, descargar las fuentes que están en

```
http://www.opengroupware.org/sources/opengroupware.org-mod_ngobjweb-latest.tar.gz
```

- Abrir el archivo tar-gzipped

```
# tar -zxvf opengroupware.org-mod_ngobjweb-latest.tar.gz
```

- Abrir el directorio creado

```
# cd opengroupware.org-mod_ngobjweb
```

- Compile escribiendo `make` (nota: es necesario instalar el `httpd-devel` package, para obtenerlo escribir: `up2date httpd-devel`).

Al finalizar la compilación un fichero `ngobjweb-x.xx.so` será creado, dónde `x.xx` es su versión de Apache).

- Crear un directorio para este modulo de apache,

```
# mkdir /opt/opengroupware.org/WebServer
```

- Mover la librería compilada

```
# mv ngobjweb-x.xx.so opt/opengroupware.org/WebServer
```



- Adicionar al final del archivo httpd.conf (/etc/httpd/conf/).

```
#####
# mod_ngobjweb Apache 2 Configuration
#####
LoadModule ngobjweb_module
/opt/opengroupware.org/WebServer/ngobjweb_2.0.40.so #OpenGroupware
WebUI
SetHandler ngobjweb-adaptor
SetAppPort 20000
Alias /OpenGroupware.woa/WebServerResources/
/opt/opengroupware.org/WebServerResources/
#ZideStore
SetHandler ngobjweb-adaptor
SetAppPort 20000
Alias /zidestore/so/images
/opt/opengroupware.org/WOApps/ZideStore.woa/WebServerResources
```

- Reiniciar Httpd despues de aplicar los cambios (por ej.

```
# /sbin/service httpd restart
```

Al escribir `http://servername/OpenGroupware` en el navegador, es posible comenzar a trabajar con Ogo

## **ANEXO B MANUAL DE OGO**

### **CARACTERISTICAS GENERALES**

Según las características de Groupware que son: Comunicación, Colaboración y Coordinación, OpenGroupware contiene[Sky01]:

#### **1. NOTICIAS**

Esta aplicación puede ser usada para proveer a los usuarios de información importante, ya que siempre despliega las citas o trabajos pendientes.

Esta aplicación entrega información que el usuario necesita de una sola vez.

#### **2. CORREO ELECTRÓNICO**

Para una mejor flexibilidad e independencia, la comunicación del correo electrónico es manejada por un servidor Imap. La ventaja de esta solución es que permite el almacenaje de correos en forma centralizada. Permite al usuario crear su propio árbol de carpetas, para manejar sus correos, desde cualquier lugar como cliente (por ejemplo Netscape, Explorer), ya que los datos son almacenados en un servidor central.

### **3. AGENDA**

El Calendario de OGo puede mostrar las citas de una sola persona, de un grupo entero o de todos los empleados. Las citas son desplegadas en cuatro formas diferentes: día, semana, mes y año.

El calendario ofrece acceso rápido a las fechas del año entero, haciendo clic en uno de los días subrayados, el membrete día exhibirá las citas del día escogido. Además al seleccionar uno de los nombres del mes, en el calendario se activará el membrete mes, que exhibe las citas del mes escogido.

El calendario muestra generalmente el día actual de color rojo. Además muestra el nombre en negritas de todas las citas en que el usuario este involucrado.

El calendario proporciona tres cajas de selección.

#### **3.1. Caja de selección para cuentas, equipos y recursos**

Utilizar esta caja de selección para filtrar las citas de una cuenta, un equipo o un recurso específico. Por ejemplo, para la cuenta personal, el calendario exhibirá solo sus citas, si se selecciona toda la intranet, se desplegaran todas las citas de la compañía. Además si en alguna cita se ocupara un recurso, primero hay que seleccionarlo de la caja de selección y verificar si estará disponible o no.

- *Buscar cuentas y recursos*

Para buscar una cuenta o un recurso específico, es posible utilizar el campo vacío al lado de la caja de la selección. Donde se puede ingresar una cuenta del programa OGo y se desplegará todas las citas del usuario específico.

### 3.2. Caja de selección zona horaria

El programa ha sido diseñado para prevenir resultados malentendidos de diferentes zonas horarias, así como también periodos de invierno y verano.

La caja de selección zona horaria permite fijar citas, en cualquier parte del mundo sin tener problemas de horario.

### 3.3. Caja de selección semana

Esta caja de selección, sirve para desplazarse de forma rápida entre las distintas semanas del calendario, la semana del calendario es mostrada por el número de semana, el respectivo mes y el día.

- **El botón Imprimir**

A veces es necesario tener la actual cita impresa, para eso es necesario presionar el botón, printview(vista preliminar) en la esquina superior derecha, y seguir las instrucciones. Una ventana del navegador es abierta, viendo las citas. Para imprimir utilizar la función de la impresión del navegador.

### 3.4. Fijar y editar una cita

Para abrir el editor de citas hacer clic en “nuevo“. Al expandir las áreas del editor, el usuario debe completar los datos que se le solicitan.

Algunas opciones especiales:

- *Reminder(recordatorio):* Utilizado para recordar una cita, desde 10 minutos hasta 8 días de anticipación, el programa puede enviar un correo recordatorio de la cita a las personas involucradas.
- *Acceso a lectura(acces read):* Se utiliza para que un grupo de usuarios específicos puedan ver la cita en su calendario, los otros usuarios solo verán un símbolo (\*)

- *Reserva de recursos:* Es posible reservar cualquier recurso para una cita, de esta forma se puede prevenir problemas de que el recurso ya este ocupado.
- *Seleccionar participantes:* Permite adicionar un usuario o equipo a participar de una cita, es posible enviar un correo informándoles que son parte de ella.
- *Permitiendo acceso a escritura:* Solo el autor de la cita tiene los derechos de modificarla, él puede escoger un grupo de personas, que puedan modificar la cita otorgándoles permisos de escritura.

### **3.5. Visor de citas**

Al seleccionar una cita especifica, se despliega el visor de citas, que contiene los siguientes membretes.

- *Membrete participantes:* Aquí se muestra a todas las personas que están involucradas en la cita, en los botones mostrar detalles y mostrar miembros se ven los detalles de los participantes como nombre, grado, correo electrónico, teléfono etc.
- *Membrete notas:* Es posible adicionar una nota relacionada a una cita.
- *Membrete atributos:* Contiene diversos datos de la cita actual seleccionada, (tiempo de inicio, tiempo de término, recursos, acceso de lectura, escritura, etc.)
- *Membrete registros(logs):* Este membrete contiene el historial de modificaciones de una cita, si un usuario tiene derecho de hacer cualquier cambio, automáticamente se registra la fecha, el usuario y la acción. Este membrete es útil por razones de seguridad si alguna modificación es causa de error, aquí se registra el último usuario que realizo una modificación y cual fue esta.

#### 4. TRABAJOS

Esta aplicación facilita la administración de los trabajos de un usuario. Los filtros despliegan solo aquellos trabajos que el usuario está involucrado o que el usuario haya creado.

Existen distintas formas de filtrado, filtro por persona, grupos o equipos (*yo, toda la intranet, etc.*) y al marcar la opción equipo de trabajo, se muestran todos los trabajos relacionados con la opción anterior (*los trabajos en que yo estoy involucrado y el equipo*). Además es posible buscar algún trabajo según su estado (*trabajo actual o trabajo futuro*) o buscar alguno escribiendo, una palabra clave.

Esta compuesto por los siguientes mimbres:

- *Membrete trabajos pendientes*: Despliega todos los trabajos creados por el usuario e incluso aquellos trabajos que han sido delegados al usuario, aquí se especifica el estado actual del trabajo a través de diferentes colores

*Rojo*: El trabajo no ha sido notificado todavía.

*Amarillo*: El trabajo ha sido notificado y se está trabajando.

*Verde*: El trabajo se ha completado.

*Gris*: El trabajo es archivado.

- *Membrete tareas delegadas y Membrete tareas archivadas*

Ambas sirven para un mejor orden de las tareas

- *En tareas delegadas*: Se pueden encontrar aquellos trabajos que el usuario actual ha creado y aquellos que ha delegado a otros usuarios.
- *En tareas archivados*: Los trabajos ya realizados, pueden ser archivados para propósito de información solamente, una vez archivados ellos no pueden ser re-archivados.

#### **4.1. Crear un nuevo trabajo**

Para abrir el editor de trabajos hacer clic en “nuevo“. Al expandir las áreas del editor, el usuario debe completar los datos que se le solicitan. por ejemplo nombre del nuevo trabajo, fecha de inicio y término, palabras claves ,seleccionar una prioridad(*alta, media, baja, muy alta*), asignar un proyecto a un trabajo, etc.

#### **4.2. Visor de trabajos**

Al hacer clic sobre el nombre del trabajo se despliega el visor de trabajos, es posible modificar el estado del trabajo seleccionando los botones siguientes:

*Aceptado:* Has notificado el trabajo, el estado cambia de rojo a amarillo.

*Hecho:* El trabajo es hecho.

*Archivado:* El trabajo es archivado y no puede ser rearchivado.

*Anotar:* Escribir un comentario relacionado a un paso o algún progreso actual del trabajo.

## 5. PROYECTOS

En la aplicación proyecto, es posible asignar trabajos(*tareas*), usuarios y documentos a muchos proyectos.

Al abrir la aplicación proyectos se despliegan todos los proyectos, que actualmente el usuario esta involucrado.

Este formulario esta compuesto por los siguientes membretes.

- *Membrete común:* Despliega todos los proyectos que el usuario esta involucrado.
- *Membrete privado:* Despliega todos los proyectos creados por el usuario y marcados como privado para que los otros usuarios no puedan verlos.
- *Membrete archivado:* Se encuentran los proyectos que están terminados.
- *Membrete buscar:* Escribir el nombre del proyecto dentro del campo y luego presionar el botón “ buscar” y se recibirá una lista con todos los resultados del dato de entrada correspondiente.
- *Membrete documentos:* Permite buscar documentos que pertenezcan a un proyecto.



## 5.1. Crear un nuevo proyecto

Para crear un nuevo proyecto, se debe presionar el botón “nuevo”, y completar los datos de la interfaz.

### **Algunas opciones importantes:**

Administrador del proyecto, es buscar un responsable del proyecto, este acceso puede ser otorgado a usuarios/equipos. En el campo buscar cuentas o equipos y habilitar el checkbox correspondiente, además al crear un nuevo proyecto es posible adicionar participantes, y existen dos categorías

1. Hay usuarios/equipos/grupos que tienen una cuenta en el programa OGo. Pueden ser buscados en el campo “Buscar Cuentas” y concederles derechos de acceso.
2. Hay personas/empresas externos listadas en las bases de datos de los contactos o de las empresas. Pueden ser asociadas solamente al proyecto; no pueden recibir ningún derecho de acceso, porque no tienen ninguna cuenta en programa OGo. Para buscar un asociado, se realiza en el campo “buscar asociados”.

### **- Derechos de acceso**

Los derechos de acceso pueden ser dados a cuentas de usuario o a equipos respectivos, para un proyecto específico, carpetas y archivos.

Cada derecho puede ser otorgado en forma separada habilitando el checkbox respectivo, los derechos de acceso no son heredados en forma automática, por ejemplo si se tiene derecho para una carpeta específica, no se tiene automáticamente los mismos derechos para cada uno de los archivos que este contiene. El creador del proyecto posee automáticamente todos los derechos.

## 5.2. Visor de proyectos

Para abrir el visor de proyectos hacer clic en el nombre del proyecto seleccionado.

Se visualizan los siguientes membretes

- *Membrete documentos:* Es posible ver carpetas, documentos asociados al proyecto, si el usuario tiene los permisos suficientes, este podrá, crear, renombrar, mover, insertar, borrar, etc. una carpeta o documento

La carpeta del proyecto raíz se crea automáticamente y no puede ser removida.

### Algunas opciones especiales

- **Crear un nuevo documento:** Para crear un nuevo archivo, presione el botón "*nuevo*" el formulario "*editar archivo en la ruta .....*" es abierto donde se debe especificar el nombre del archivo e incluso su extensión, el tener archivos sin extensión pueden no ser creados por el programa OGo. Para escribir el texto se realiza dentro del campo editor de texto, debajo del editor, hay dos botones para validación, código-HTML, y XML respectivamente se puede escribir código fuente directamente y revisarlo, esta particular característica ofrece una facilidad para crear archivos HTML/XML

- **Visor de archivo:** Para ver un archivo dentro del visor de proyectos, hacer clic en el nombre del archivo, el editor del archivo es abierto, este editor contiene 5 membretes: contenido, atributos, versiones, permisos y registros.
  - *Membrete Buscar:* Permite realizar búsquedas a través del proyecto completo, por las carpetas , archivos o documentos, especificando un nombre y la extensión o ambos y comenzar a buscar presionando el botón “buscar.”
  - *Membrete Atributos:* Se despliega diversa información relacionada al proyecto actualmente seleccionado, dentro de este membrete puedes editar el proyecto, modificar sus atributos.
  - *Membrete Trabajos:* Aquí proporciona una conexión a la aplicación trabajos, puedes seleccionar trabajos para el proyecto actual.
  - *Membrete Notas:* Para adicionar notas, algún comentario relacionado al proyecto actual.

## 6. CONTACTO Y EMPRESAS

Ambas aplicaciones son muy similares,

### Características comunes

Ambas aplicaciones pueden ser usadas para almacenar, buscar, ver y modificar entradas, también para el envío de correo.

Se visualizan los siguientes membretes

- *Membrete búsqueda:* Por nombres, apellidos, compañía y cuenta en el programa OGo. Y se recibirá una lista con todos los resultados del dato de entrada correspondiente.
- *Membrete búsqueda avanzada:* Búsqueda por una gran variedad de atributos (ciudad, nombre, profesión, correo electrónico etc.)
- *Membrete texto completo:* Usa este criterio para realizar una búsqueda por todos los campos de la base de datos de contactos y empresas, con solo escribir la palabra en el campo correspondiente, desplegará una lista con todos los datos que coincidan con la palabra de entrada.

### 6.1. Visor de personas

El visor de personas muestra los siguientes membretes

- *Membrete Proyectos:* Este muestra todos los proyectos en el cual el contacto está involucrado.
- *Membrete Empresas:* Este membrete es visible solo si la persona seleccionada ha sido asignada a una empresa.
- *Membrete Direcciones:* Muestra la dirección privada, de correo y la dirección de localización de la persona.
- *Membrete atributos:* Se despliega diversa información relacionada al contacto seleccionado.

- *Membrete Picture*: Es posible adicionar fotografías del contacto respectivo.
- *Membrete Citas*: Muestra todas las citas del contacto.
- *Membrete Log (registro)*: cualquier modificación de un contacto o empresa queda grabada aquí, con el dato del usuario y acción.

## 6.2. Visor de empresas

El visor de empresas muestra los siguientes membretes y además los membretes de igual función que los del visor de contactos

- *Membrete personas*: Aquí se muestran las personas involucrados a la empresa, ofrece una conexión a la aplicación contacto.
- *Membrete proyectos*: Aquí se muestran los proyectos involucrados de la empresa, ofrece una conexión a la aplicación proyectos.
- *Membrete overview*: Este membrete contiene un archivo de texto `index.txt`, el cual puede ser usado para escribir notas cortas.
- *Membrete direcciones*: Contiene direcciones de la empresa seleccionada

## 7. GESTOR DE USUARIO

El administrador, especifica los usuarios, equipos y recursos que serán utilizados en el programa.

- *Membrete cuentas:* Aquí es posible buscar una cuenta ya existente en el programa. Para crear un nuevo usuario hacer clic en el botón nuevo para abrir el editor de cuentas y completar los datos correspondientes.
- *Membrete equipos:* En este membrete es posible manejar equipos respectivos y crear nuevos equipos, es muy similar al de cuentas, para modificar un equipo hacer clic en el nombre del equipo para abrir el editor donde es posible asignar cuentas a un equipo y crear uno nuevo .
- *Membrete recursos:* Es posible crear recursos, buscar, modificar, es similar a la opción cuentas y equipos, el membrete recursos sirve para asignar recursos a una cita por ejemplo (pc, sala, etc.).

## **8. PREFERENCIAS**

Para personalizar la interfaz del programa, usar la opción de preferencias, es posible cambiar lenguaje, horario, contraseña y otras opciones, también personalizar el programa de acuerdo a sus requerimientos, para acceder a todas las aplicaciones se debe tener los permisos correspondientes.

*Cambiar password:* Para cambiar un password presione el botón "*modificar clave*" para abrir el editor de password y escriba el password correspondiente y presione el botón "grabar."

Mas abajo esta la opción preferencias de la aplicación es posible personalizar en forma independiente, para abrir cada una hacer clic en el nombre respectivo por ejemplo, correo, contactos, empresas, proyectos, trabajo, etc.

## **9. DESK (ESCRITORIO)**

Este enlace proporciona un acceso rápido a la lista de enlaces que contienen los bookmark, que es importante para la comunicación en la intranet en la empresa, esta lista es creada por el administrador del sistema y puede ser usada por los usuarios del programa OGo, si existe una lista esta puede ser accesada desde afuera con solo presionar el botón "*escritorio*"

## ANEXO C Firmar y Encriptar un mensaje con la herramienta WinPT

- *Encriptación de un mensaje:* Con el programa de correo o en el Bloc de Notas, se escribe un mensaje, se selecciona todo el texto. Con el botón derecho del ratón pulsar copiar. Ahora con el botón derecho del ratón pulsar sobre el icono que se encuentra en la esquina inferior derecha, hay un icono con una lupa del GPG. Al pulsar muestra un menú, se escoge *clipboard*, seguido de *“Encrypt”*. En la nueva ventana. Elegimos la clave (*si se tiene mas de una*). Pulsar OK. Al hacer esto, el contenido del portapapeles quedara encriptado y al volver al programa de correo o el bloc de notas (*donde seguirá el texto seleccionado*). Pulsar en el texto con el botón derecho otra vez y elegir pegar.

El resultado es un bloque de texto ininteligible de números y letras, precedido por un encabezado que muestra que es un bloque de datos cifrado con GPG.

El proceso inverso, si alguien ha enviado un correo cifrado, para verificar es copiar el texto al portapapeles, en el menú que esta en la esquina inferior derecha seleccionamos *clipboard* luego *“Decrypt/verify”*, en la nueva ventana se solicita ingresar la contraseña que protege la clave privada, si es correcta el contenido del portapapeles será descifrado



- *Firmar un mensaje:* Con el programa de correo escribimos un mensaje o en el bloc de notas. Seleccionar todo el texto. Con el botón derecho del ratón pulsar copiar. Ahora con el botón derecho del ratón pulsar sobre el icono que se encuentra en la esquina inferior derecha hay un icono con una lupa del GPG. Al pulsar muestra un menú, se escoge *Clipboard - Sign*. En la nueva ventana, elegir la clave con la que se va a firmar el mensaje (pedirá la clave secreta) si se tiene mas de una y pulsar OK. Volvemos al programa de correo o al Bloc de Notas(*donde seguirá el texto seleccionado*). Pulsar en el texto con el botón derecho otra vez y elegir pegar.

Para verificar un mensaje firmado con GPG, se realiza el proceso inverso, copiar el texto en el portapapeles, en el menú que esta en la esquina inferior derecha, seleccionamos *clipboard* luego *"Decrypt/verify"*, el contenido del portapapeles será verificado y en una nueva ventana nuestra si la firma es válida o no.