

UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PRIVACIDAD EN UN SISTEMA DE MEMORIA ORGANIZACIONAL.

YERKO MILTON MUÑOZ MALLANES

COMISIÓN EXAMINADORA	NOTA (nº)	CALIFICACIONES: (Letras)	FIRMA
PROFESOR GUÍA SR. JOSÉ PINO U.	:		
PROFESOR CO-GUÍA SR. LUIS GUERRERO	:		
PROFESOR INTEGRANTE SR. HUGO MORA	:		
NOTA FINAL EXAMEN DE TÍTULO	:		

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN COMPUTACIÓN

SANTIAGO DE CHILE
OCTUBRE DE 2003

Resumen

La presente memoria tuvo como objetivo definir un marco teórico y conceptual sobre la privacidad de información en un sistema de memoria organizacional.

Para ello se estudiaron dos casos reales de diseño e implementación de sistemas de manejo de información. Uno de memoria organizacional, y otro sistema diseñado para compartir bitácoras de navegación en la red. Se estudiaron las barreras culturales y técnicas que se enfrentaron en tales sistemas al momento de diseñarlos. Finalmente se evaluaron en su desempeño, mediante criterios definidos para sistemas de tales características.

Para completar el marco se estudió en forma teórica las consideraciones sobre la privacidad de las personas, las iniciativas legislativas de distintos países para enfrentar los desafíos tecnológicos de la era de la información en que vivimos y las soluciones que entrega la computación frente a las amenazas de la privacidad.

Se consideraron dos casos de manejo de información individual de las personas, tales como son la información personal médica y la información financiera, las iniciativas y normativas que poseen algunos países desarrollados sobre este tipo de información y su manipulación.

Finalmente, se hizo como propuesta de diseño de un modelo de memoria organizacional a **Priv-Control**. Esta es la capa final del modelo propuesto por Pino y Guerrero para un sistema de manejo de información. Se recopilaron de la literatura las estrategias de privacidad y se propusieron nuevas. Se definieron niveles de privacidad para realizar los aportes en el sistema, agrupando algunas de forma coherente.

Se tuvo como premisa para diseñar la interfaz de privacidad que el autor de los aportes deben tener control absoluto del acceso a dicha información. Se consideró también el apoyo a la colaboración entre los usuarios del sistema, dado el trade-off existente entre privacidad/colaboración.

Agradezco a mi madre Rosa, a mis abuelos, Inés y Héctor Mario y a mi hermana Cindy, por su apoyo incondicional durante todo este proceso. A todos mis amigos, antiguos y nuevos, que me acompañaron por estos largos años en la Escuela. Porque hicimos Universidad y la seguiremos haciendo.

Índice general

1. Introducción.	1
2. Motivación.	4
3. Objetivos.	6
3.1. Objetivos Generales.	6
3.2. Objetivos Específicos.	7
4. Revisión bibliográfica y material relacionado.	8
5. Casos de estudio.	11
5.1. Sistema de Memoria Organizacional basado en QuestMap TM.	12

5.1.1.	Introducción.	12
5.1.2.	Barreras frente al diseño.	12
5.1.3.	Diseño de la memoria organizacional.	14
5.1.4.	Implementación.	16
5.2.	COLLABCLIO.	19
5.2.1.	Introducción.	19
5.2.2.	Interfaces de privacidad en COLLABCLIO.	19
5.2.3.	Conclusiones.	23
6.	Tópicos en Privacidad.	25
6.1.	Computadores, bases de datos y la privacidad de la información.	25
6.1.1.	Consideraciones sobre privacidad.	26
6.1.2.	Amenazas tecnológicas contra la privacidad de la información.	29
6.1.3.	Legislación sobre privacidad.	29
6.2.	Privacidad y tecnología.	31

6.2.1. <i>Remailers</i>	32
6.2.2. Uso de criptografía.	34
6.3. Protección de la información de las personas.	36
6.3.1. Privacidad en la información médica.	36
6.3.2. Privacidad en la información financiera.	40
6.4. Privacidad de la información en Chile.	44
6.4.1. Ley 19.628	44
6.4.2. CONFIARe.cl	47
7. Modelo propuesto.	50
7.1. PrivControl.	57
8. Diseño de PrivControl	59
8.1. Casos de Uso.	59
8.1.1. Plan de acción antes de la reunión	60
8.1.2. Memoria de corto y largo plazo.	61

8.1.3.	Precisión en los niveles de autoría.	62
8.1.4.	Uso de seudónimos.	63
8.1.5.	Encriptación de la información.	64
8.1.6.	Perfiles de usuario.	65
8.1.7.	Marcas de tiempo relativas.	66
8.1.8.	Envejecimiento de la información.	67
8.1.9.	Modelo completo.	68
8.2.	Casos de uso para los niveles predefinidos.	70
8.2.1.	Nivel de privacidad "Aceptar todo".	70
8.2.2.	Nivel de privacidad Básico.	71
8.2.3.	Nivel de privacidad Medio.	72
8.2.4.	Nivel de privacidad Alto.	74
8.2.5.	Nivel de privacidad "Restringir todo".	75
8.3.	Interfaz del sistema.	76

8.3.1.	Interfaz principal.	76
8.3.2.	Interfaz "Aceptar todo".	77
8.3.3.	Interfaz Nivel Básico.	77
8.3.4.	Interfaz Nivel Medio.	78
8.3.5.	Interfaz Nivel Alto.	80
8.3.6.	Interfaz "Restringir Todo"	81
8.4.	Discusión del modelo.	82
9.	Conclusiones.	84
A.	QuestMap TM.	88

Índice de figuras

2.1. Diagrama de <i>OMUSISCO</i>	5
5.1. Modelo simple de la memoria humana.	15
5.2. Expresión genética del ADN.	15
5.3. Un ejemplo de despliegue en QuestMap TM.	17
5.4. Componentes principales del modelo.	18
5.5. Ventana de elección del tipo de privacidad.	21
5.6. Interfaz del editor de políticas de privacidad.	22
5.7. Ventana de monitoreo de la política de privacidad.	22
6.1. Encriptación asimétrica.	42

6.2. Cómo se firma digitalmente.	43
7.1. Componentes del sistema de manejo de información (KMS).	51
7.2. Interfaz de configuración de IE.	58
8.1. Estrategia aplicable antes de la reunión.	60
8.2. Registros de corto y largo plazo.	61
8.3. Niveles de precisión en la autoría.	62
8.4. Uso de seudónimos.	63
8.5. Encriptación.	64
8.6. Perfiles de usuario.	65
8.7. Marcas de tiempo difusas o relativas.	66
8.8. Información desechable.	67
8.9. Modelo completo - 8 estrategias.	68
8.10. Aceptar todo.	70
8.11. Nivel de privacidad Básico.	71

8.12. Nivel de privacidad Medio.	72
8.13. Nivel de privacidad alto	74
8.14. Restringir todo.	75
8.15. Interfaz principal del sistema.	76
8.16. Interfaz web de nivel de privacidad básico.	77
8.17. Interfaz web de nivel medio.	78
8.18. Nivel alto de privacidad.	80
8.19. Interfaz de configuración de privacidad.	81
8.20. Gráfico: nivel de privacidad versus nivel de colaboración.	83
A.1. Interfaz principal de QuestMap TM.	89

Capítulo 1

Introducción.

En las compañías nuevas y en aquellas que son exitosas, los directivos se concentran principalmente en administrar eficazmente las finanzas y los recursos tangibles de la organización, mejorar e implementar nuevos estándares de calidad, ofrecer mejor y más oportuno servicio a sus clientes, en capacitar a su personal, conocer a la competencia y las tendencias del mercado, y en general en lograr que su compañía reporte utilidades. Sin embargo, muy pocas se han preocupado por administrar y almacenar su conocimiento organizacional, de manera que después pueda ser utilizado, ahorrando tiempo, dinero y permitiendo conocer los errores y abstinencias del pasado para mejorar el presente sin repetir esos errores [6].

Teniendo en cuenta estas necesidades de almacenamiento en forma estructurada de este conocimiento inherente, perteneciente a cada organización, aparece el concepto de "memoria organizacional". La memoria organizacional va a ser, por lo tanto, todo el conocimiento formal e informal [5] presente en la organización. El primero aparece de los documentos, guías de buenas prácticas, manuales y libros que apoyan a los miembros de la organización a tener un buen desempeño. El conocimiento informal, en cambio, aparece en los resultados formales del proceso de creación de los miembros. Aquí se incluyen las ideas, hechos, significados, presunciones, preguntas, puntos de vista y decisiones. Se hace notar que este tipo de conocimiento es difícil de capturar y mantener estructurado, ya que se genera en los individuos pertenecientes a la organización y en la interacción de los mismos.

El problema del almacenamiento del conocimiento con estos propósitos, se hace medianamente

complicado. Se debe tener en cuenta el nivel de estructuramiento de los datos relevantes como también su procedencia. Se debe distinguir los conceptos de dato, información y conocimiento. Dato, definido como los hechos, los cuales no están ni analizados ni resumidos. Información como los datos procesados en alguna forma para darles significado y por último, el conocimiento se puede explicar como la habilidad de usar esta información.

Para automatizar este almacenamiento del conocimiento, se puede plantear el diseño de un sistema de manejo del conocimiento (Knowledge Management System - KMS). Un KMS es un sistema dinámico que provee la funcionalidad de apoyar la identificación, la adquisición, la retención, el mantenimiento, búsqueda y recuperación del conocimiento, visto como información más el contexto donde fue generado. Para que este conocimiento sea útil en una organización, el KMS debe incluir un sistema de recuperación del mismo de buena calidad. Con esto es posible apoyar la toma de decisiones dentro de la organización, con las experiencias pasadas almacenadas en el sistema, con el fin de no repetir errores anteriores. Una opción, por ejemplo, es usar técnicas modernas de recuperación de la información, para generar criterios de búsqueda inteligente en el repositorio de conocimiento [7].

Un sistema de estas características enfrenta problemas en la creación de las tres estructuras que lo componen: adquisición de la información, almacenamiento y recuperación de la misma.

En la primera, existen problemas debido a la naturaleza no estructurada de la información relevante. Es decir, la información más rica en conocimiento no posee una estructura pues nace de la interacción de grupos de trabajo, en reuniones resolutorias y en el mismo accionar diario de los individuos dentro de la organización. La interacción dentro de un grupo y la sinergia producida por sus miembros afines, genera más información rica en conocimiento que la que se pueden encontrar en documentos escritos como reportes y memorándums, la cual se hace imprescindible estructurar y almacenar.

El problema del almacenamiento, debe dar solución al diseño de una estructura coherente para este tipo de información. Se puede recurrir a modelos biológicos de estructuramiento de la memoria humana, como la característica distintiva de asociatividad de los conceptos almacenados. Es decir, una "búsqueda" en la memoria humana, en otras palabras, recordar, no retorna directamente un resultado, sino se asocian conceptos para llegar la solución. Otra característica es que la memoria humana es reorganizativa, esto es, la nueva información está siempre relacionada con el conocimiento previo, el cual es reestructurado a su vez.

El problema del acceso a la información hace latente el usar técnicas modernas de recuperación

de la información, con el fin de rescatar el conocimiento previamente almacenado en forma estructurada. Se deben definir criterios claros para el uso del sistema por parte de los usuarios y para la búsqueda de la información relevante.

Capítulo 2

Motivación.

La utilidad de un sistema de memoria organizacional aparece en la necesidad de tener a mano todo este conocimiento para su posterior utilización en los procesos de la organización, como repositorio de experiencias y metodologías donde recuperar la información necesaria al momento de tomar decisiones. Una fuente de conocimiento, antes mencionada, son las reuniones de decisión o resolutivas. Al existir sistemas de apoyo a reuniones como SISCO [3], que apoya la preparación de las reuniones. Este modelo ayuda a generar una pre-reunión estructurada con el fin de que todos los participantes del grupo se enteren de los temas concernientes a la reunión, se discutan y generen pre-soluciones, para disminuir la equivocabilidad e incerteza de la reunión correspondiente. También posee roles que diferencian a los participantes y sus obligaciones en el sistema, tomando en cuenta las tareas generadas a partir de los temas tratados en la pre-reunión. Además, posee opcionalmente un repositorio de las discusiones, argumentos e ideas generadas en el sistema. Este repositorio es usado en otra implementación, como fuente de conocimiento en un sistema de memoria organizacional (OMUSISCO) [12]. (Ver figura 2.1)

Un tópico no muy desarrollado, que surge al momento de diseñar un sistema de estas características, es el de la privacidad de los participantes del sistema al mantener una relación entre las opiniones y el autor de las mismas. Este factor tiene connotaciones éticas pues las opiniones pueden ser utilizadas fuera del contexto de las discusiones, perjudicando al autor de alguna manera. El modelo de datos SISCO no incluye esta característica, aunque algunas implementaciones lo agregan a su funcionalidad interna. Existen varios paradigmas para su implementación. Uno que surge naturalmente es el de *anonimato*, es decir, el autor de las opiniones está completamente desligado de relación, al ser su aporte anónimo. Con relación a esto, es deseable, de alguna manera,

medir el nivel de participación de los miembros del grupo, por lo que este paradigma no sirve para este fin, pues se pierde el vínculo de la autoría del aporte. Esto conlleva al problema de *free-riding*. Esto es, algún usuario se puede aprovechar de la situación de anonimato, al considerar que si el grupo está contribuyendo en forma eficiente, no existen incentivos para que él lo haga.

Otro paradigma, es romper el vínculo eventualmente de la autoría al introducir la funcionalidad de "olvido del nombre". Esto es una metáfora de la realidad, ya que cuando se recuerda una conversación hecha hace algún tiempo, típicamente se recuerda lo dicho, pero no el autor. Interesante sería incluir en el modelo de datos SISCO, la característica de privacidad mezclando los paradigmas existentes e ideando nuevos, con el propósito de incluirlos.

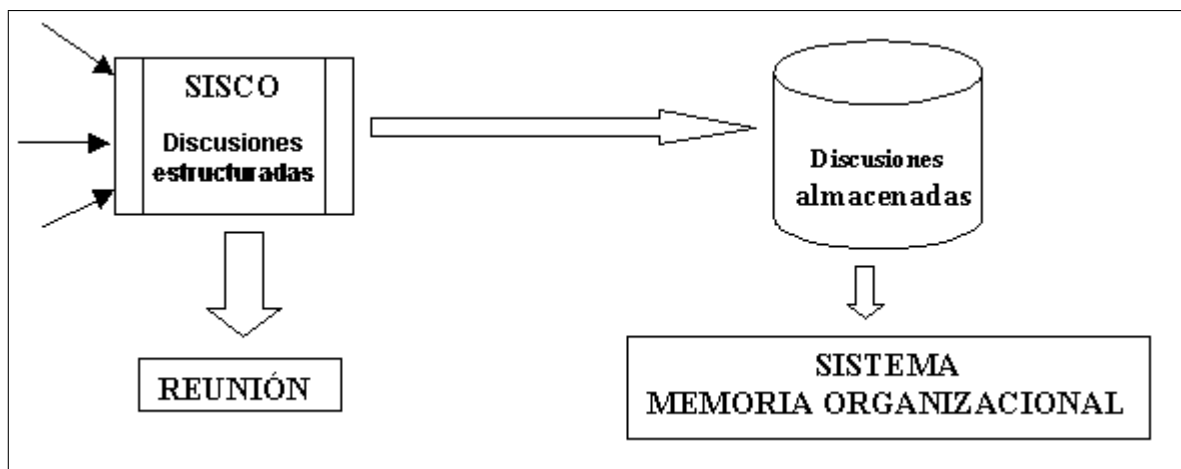


Figura 2.1: Diagrama de *OMUSISCO*.

Capítulo 3

Objetivos.

3.1. Objetivos Generales.

- Definir el marco conceptual y teórico para la inclusión de privacidad en el diseño del modelo de datos SISCO.
- Presentar variados casos de estudio de sistemas ya implementados, como base de conocimientos para proponer un nuevo modelo.
- Proponer un nuevo modelo de datos, que incluya la característica de privacidad en el sistema de memoria organizacional.
- Justificación del modelo propuesto.

3.2. Objetivos Específicos.

- Replantear el modelo SISCO más orientado a un sistema de memoria organizacional.
- Incluir en el modelamiento del diseño, la característica de privacidad.
- Validar el modelo de datos nuevo con el marco conceptual ya existente.
- Comparar el modelo del sistema con las implementaciones conocidas de memoria organizacional.
- Implementar un sistema de memoria organizacional, con las características deseadas de privacidad.

Capítulo 4

Revisión bibliográfica y material relacionado.

El material bibliográfico investigado, al momento de definir el marco teórico necesario para una introducción al tema de memoria organizacional fue muy variado, con la única meta de lograr tener distintos puntos de vista sobre el mismo tema. Esto denotó las concordancias y diferencias entre los autores, lo cual permitió sacar en limpio lo aportes más importantes de sus trabajos.

Comenzando, en el artículo "*Diaries at Work*" [8] se presenta el caso de un sistema de memoria organizacional dentro de una industria papelera. En ésta se utiliza una maquinaria con muchos procesos de producción complejos, por lo tanto, se hace necesario mantener un repositorio de información compartida entre todos los operarios, pertenecientes a cada etapa de la línea de producción. La primera solución dada es de carácter primitivo, como lo puede ser una libreta con anotaciones a mano, perteneciente a los distintos niveles del proceso de producción y a los distintos turnos de trabajo de los operarios. Se propone un sistema electrónico de anotaciones, con la característica de ser distribuido y asíncrono. Se separan por niveles jerárquicos y de turnos, dentro de las jornadas de trabajo.

El autor Jeffrey E. Conklin da como ejemplo una serie de casos de empresas que no implementan un sistema de memoria organizacional en su proceso de gestión. Él utiliza estos casos como fundamento para la incorporación de este tipo de sistemas dentro de una organización. Presenta las etapas del proceso de memoria organizacional, problemas inherentes a cada etapa y una revisión

de la herramientas a utilizar para la creación del sistema, del punto de vista de las habilidades de liderazgo del nivel gerencial de la empresa [6]. En el artículo *"Capturing Organizational Memory"* [4], el mismo autor define los conceptos de Memoria Organizacional (MO), como también los pasos a seguir para diseñar la estructura de un sistema de recolección de datos para una MO. Se basa en un paradigma orientado a los procesos de la organización, más que uno orientado a los componentes (artefactos de información) como documentos, memos, libros, manuales, etc., integrando tres tecnologías: hipertexto, como la representación más apropiada para un sistema de estas características; groupware, como un sistema de ayuda a la cooperación entre los miembros y vía para compartir información y un modelo retórico, como es IBIS, que le agrega la estructura a esta información. Continuando con Conklin, en el artículo *"Designing Organizational Memory: Preserving Intellectual Assets in Knowledge Economy"* [5] desarrolla el proceso de diseño de un sistema de memoria organizacional (MO) desde el punto de vista de un modelo biológico de la memoria (3 componentes). Se enumeran en principio los problemas inherentes al crear un sistema de MO como también las consideraciones a tomar en cuenta al momento de diseñar. Los tipos de información, las barreras culturales y técnicas dentro de la organización misma, el error de no considerar el contexto al almacenar la información son algunos de estos problemas. Se hace una comparación de los modelos biológicos existentes con la creación de un sistema de MO y se propone, finalmente, una solución al diseño, considerando todo lo antes descrito.

En este sentido, en el artículo *"An IBIS – based model to support group discussions"*, los autores Bellasai, Borges, Fuller, Pino y Salgado, a su vez, muestran un ejemplo concreto de una organización y un sistema de apoyo a las pre - reuniones denominado SISCO, basado también en el modelo retórico de discusión IBIS (*Issue Based Information System*). Se presenta un modelo que lo sustenta, incluyendo las funcionalidades inherentes a un sistema de estas características y adecuándose al sistema en funcionamiento [3]. Dos casos nuevos de implementación del sistema SISCO se presentan en los artículos *"Organizational Memories as Electronic Discussion By – Products"* y *"Understanding Organizational Memory"*. En el primero se muestra un estudio sobre un alcance de desarrollo de un sistema de memoria organizacional, basado en el reuso de discusiones apoyadas por computador obtenidas de preparaciones a reuniones o pre - reuniones. Se presenta un sistema denominado OMUSISCO, que posee la característica de tener como fuente de información un sistema SISCO de apoyo a pre - reuniones, como un sistema Thesaurus para permitir al usuario la recuperación de la información almacenada en el sistema. El sistema se testeó con discusiones simples previamente almacenadas, fácilmente escalable a casos de situaciones reales [12]. En el segundo artículo, se presenta una nueva implementación de memoria organizacional, denominada WSISCO, que considera a un sistema como SISCO como fuente de información para el sistema de Memoria Organizacional. Se hace una revisión de previas implementaciones y de sistemas de manejo de información (KMS). Se propone un nuevo sistema, considerando características de privacidad de la información introducida al sistema [7].

Otro estudio interesante hacen los autores Mark Ackerman y Christine Halverson (Véase [1]), en el cual abordan el tema de memoria organizacional considerando el caso puntual de un centro de llamados. Se analizan las actividades dentro de la organización, luego del requerimiento de una llamada telefónica y la "memoria" utilizada en estas actividades. Se hace el análisis desde el punto de vista de la teoría cognoscitiva, dentro de un grupo de personas.

Todo el material antes descrito hasta este momento, falla en una inclusión seria de una característica importante, al diseñar un modelo de memoria organizacional, como lo es la característica de privacidad. En *"Forgetful or Bad Memory?"*, el autor John Landry hace una crítica al modelo ideal de memoria organizacional (MO), que no posee la característica de "olvido" de la información no relevante. Se explora el rol que posee el olvido individual y colectivo dentro de una organización. Se muestra, además, que el olvido permite agrandar la visión de la información dentro de la organización y puede ser la característica más importante al diseñar una MO para proveer el apoyo adecuado a los gerentes y a la organización en sí [9]. En un siguiente artículo (Véase [10]), se desarrolla una manera de cómo facilitar el compartir información dentro de una organización, utilizando las redes de comunicación modernas, dando las capacidades al usuario de decidir qué compartir, qué no y a quién. Se introducen los conceptos de políticas de privacidad intensionales y extensionales. Se estudian tres casos de sistemas que implementan políticas con este criterio y se concluye, para cada caso, que se deben diseñar este tipo de políticas como componentes explícitos del sistema, de primera clase.

Por otro lado, Mark Ackerman y Lorrie Cranor, en su trabajo *"Privacy Critics: UI Components to Safeguard User's Privacy"*; introducen el concepto de "críticos de privacidad" (*Privacy Critics*) como agentes semiautónomos, que tienen como función principal proteger a los usuarios de Internet de compartir información en línea no deseada, basados en un sistema de sugerencias y advertencias. Se aborda el tema de privacidad como un problema de interfaz, el cual carece de políticas de privacidad claras, no permitiéndole al usuario tomar decisiones informadas, al entregar información personal [2].

Capítulo 5

Casos de estudio.

A continuación se presentarán casos de estudio, tomados como base de conocimientos para definir y proponer un diseño que agregue la característica de privacidad a los modelos existentes.

1. Sistema de memoria organizacional basado en QuestMap TM. [5]
2. Interfaces de privacidad para el manejo de la información. [10]

5.1. Sistema de Memoria Organizacional basado en QuestMap TM.

Una organización basada en conocimiento es aquella en la cual el recurso clave es el conocimiento. Su ventaja competitiva proviene de poseer y usar efectivamente dicho conocimiento. Ejemplos de organizaciones pueden ser una oficina de leyes, una firma de contabilidad o marketing, una compañía de software, la mayoría de las agencias de gobierno, universidades, el ejército y partes significativas de la mayoría de las compañías manufactureras. Organizaciones basadas en conocimiento son el contenedor para obreros del conocimiento, el vehículo por el cual ellos aplican tal conocimiento [5].

5.1.1. Introducción.

Como se ha dicho ya, el conocimiento es el recurso clave de la organización basada en conocimiento. Es aquí que la memoria organizacional se extiende y amplifica este recurso al capturar, organizar, diseminar y reusar este conocimiento generado y creado por los mismos trabajadores. Para crear y diseñar este sistema de memoria organizacional se enfrentaron cuatro grandes barreras: capturar y estructurar la información relevante dentro de la organización; la segunda, la falencia al preservar el contexto que da a los documentos significado, lo más importante que les permite ser útiles en el futuro; en tercer lugar es que el conocimiento tiende a perder su relevancia, con el paso del tiempo; y finalmente, las políticas de "amnesia organizacional", es decir, la destrucción sistemática de todas las notas y documentos personales innecesarios, en forma periódica.

5.1.2. Barreras frente al diseño.

La primera barrera enfrentada hace relación a los tipos de conocimiento inherente a una organización. Los autores muestran que la dificultad al capturar el conocimiento, es que existen dos tipos: formal e informal. Las organizaciones fácilmente y rutinariamente capturan conocimiento formal, en formato de libros, manuales, documentos y cursos de capacitación. En cambio, el conocimiento informal surge y es utilizado en el proceso de creación de los resultados formales. En éstos se incluyen las ideas, hechos, presunciones, significados, preguntas, decisiones, suposiciones, historias

y puntos de vista del equipo de trabajo. Este tipo de conocimiento es obviamente más difícil de capturar, ya que para el trabajador mismo se refleja más efímero y transitorio. A su vez, es un recurso organizacional de inmenso valor, pues mucho de lo que es creado y compartido entre compañeros de trabajo nunca llega a estar en documentos formales. Esto último es una de las causas que llevan a los equipos de trabajo a enfrentar problemas conocidos y repitiendo los mismos errores pasados.

Una de las razones que da el autor para que se produzca esta falencia al capturar el conocimiento informal, es que en la cultura occidental se valoriza más el resultado final - la entrega final del proceso de trabajo - por sobre el proceso en sí mismo, enfatizando de sobremanera las cosas (producto final) sobre las relaciones (proceso en sí).

La segunda barrera que se enfrenta al diseñar un sistema de estas características proviene de la falta de tangibilidad de este tipo de conocimiento es el uso de las herramientas modernas de comunicación y computacionales, ya que éstas pobremente reconocen o apoyan el proceso de trabajo del conocimiento. Estas herramientas entregan la falsa idea de que al entregar un producto limpio y finalizado está todo el proceso completo, pero sistemáticamente se ignora el trabajo de razonamiento y aprendizaje que conllevó el realizar este producto final.

Por lo tanto, dados los factores descritos anteriormente, si sólo se considera un repositorio del conocimiento formal de la organización, éste carecerá de contexto y será ignorado como recurso. Por otra parte, si la organización toma en cuenta también el conocimiento informal subyacente, el razonamiento detrás de las decisiones y documentos se convierte en las relaciones que sustentan el conocimiento formal, dándole el significado que hasta este momento carecían. Por consiguiente, se afirma que ese trabajo de conocimiento requiere herramientas y los procesos que conserven el contexto del trabajo tal como él evoluciona, y esta conservación no puede ser llevada a cabo meramente por los artefactos del trabajo (documentos formales). El contexto al conservarlo se plasma en una trama de información que incluye hechos, suposiciones, restricciones, decisiones y su justificación, los significados de condiciones cruciales, y por supuesto, los documentos formales mismos.

La tercera barrera que se enfrenta al diseñar un sistema de memoria organizacional es que el conocimiento tiende a perder relevancia, y así su valor. El conocimiento informal, siendo más contextual, es aún más dinámico de esta forma. Un sistema de memoria organizacional debe por consiguiente, justo como la memoria humana, tener la capacidad de recordar todo lo relevante y sobresaliente hasta ese momento.

De cierta forma se retorna al problema de la estructuración del conocimiento, ya que si se utiliza

como símil la memoria humana, ésta tiene la extraordinaria capacidad de significación y, de esta manera, de relevancia. Ésto queda en evidencia que al ingresar un "trozo" dado de conocimiento, éste no es almacenado en un sólo compartimento ni campo de datos de la memoria, sino que es distribuido por toda ella. Además se tiene que, a diferencia de los computadores, la memoria humana es asociativa por naturaleza: para acceder este "trozo" de conocimiento, se llega a él a través de una red rica en asociaciones semánticas.

La última y cuarta barrera a enfrentar es lo que algunas organizaciones han adoptado como política de seguridad de la empresa, la llamada "amnesia organizacional", es decir, la destrucción sistemática de todas las notas personales y documentos innecesarios, en intervalos de tiempo regulares. El razonamiento detrás de esta política es que, en el evento de una litigación o juicio criminal, es peligroso mantener documentos escritos que puedan ser usados en contra de la corporación. El riesgo de juicios onerosos contra la organización ha creado un incentivo económico para esta amnesia. Este razonamiento, mientras exista, será el mayor obstáculo para la creación de una memoria organizacional.

Resumiendo, las barreras para la creación de un sistema de memoria organizacional caen en dos grandes categorías: barreras culturales y barreras técnicas. Las barreras culturales incluyen, por ejemplo, la gran importancia y énfasis que se les da a los resultados finales de un proceso y no al proceso en sí; la resistencia a utilizar el proceso de captura del conocimiento, dado el esfuerzo que requiere; el temor a la pérdida de privacidad, debido a las investigaciones que conlleva algún caso judicial. Entre las barreras técnicas se pueden nombrar el cómo lograr un fácil proceso de captura del conocimiento, cómo hacer que la recuperación de dicho conocimiento sea transparente, y a la vez, fácil; y, por último, cómo asegurar que el conocimiento recuperado del sistema tenga la suficiente relevancia y inteligibilidad, dependiendo de su contexto.

5.1.3. Diseño de la memoria organizacional.

Luego de enumerar los problemas que se presentan al diseñar un sistema de memoria organizacional, se dan las soluciones a ellos, junto a una adecuada justificación. Estas capas identificables de un sistema de memoria organizacional provienen de los modelos biológicos que se pueden encontrar en la naturaleza. Como muestra, se puede considerar uno de los modelos más aceptados de la memoria humana (Ver figura 5.1).

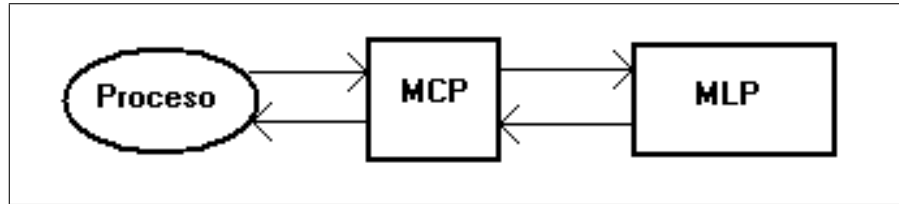


Figura 5.1: Modelo simple de la memoria humana.

Las teorías actuales sobre el funcionamiento de la memoria humana dicen que consta de dos componentes principales: una memoria de corto plazo (MCP) y una memoria de largo plazo (MLP). El tercer componente que aparece en la figura, es el encargado del procesamiento cognoscitivo del cerebro, que correspondería al procesador de un computador. La MCP o memoria de corto plazo, participa directamente en el proceso de cognoscitivo, aunque su tamaño es pequeño. La MLP o memoria de largo plazo, es usada para el almacenamiento permanente de la información y las experiencias. Por ende, la MCP está en el medio de la memoria, ya que para guardar algo en la memoria se debe enfocar el procesamiento sobre la MCP con las suficientes repeticiones, para que se produzca una marca permanente en la MLP. En el otro sentido, si se desea recuperar algo desde la MLP, se debe traer y pasar por la MCP. Nada sale o entra desde la MLP, sino pasa antes a través de la MCP (Memoria de corto plazo, ver figura 5.1).

Existen variados ejemplos de este mismo fenómeno en procesos presentes en la naturaleza. Un ejemplo claro es el almacenamiento de la información genética en el núcleo de las células. Aquí también existe una memoria intermedia presente en el proceso: las moléculas de ARN (Ácido Ribonucleico) media entre las proteínas, que son las encargadas de ejecutar todas las funciones metabólicas de las células; y el ADN (Ácido Desoxi – Ribonucleico), que da el esquema para la estructura de cada proteína, a través de sus secuencias de aminoácidos.

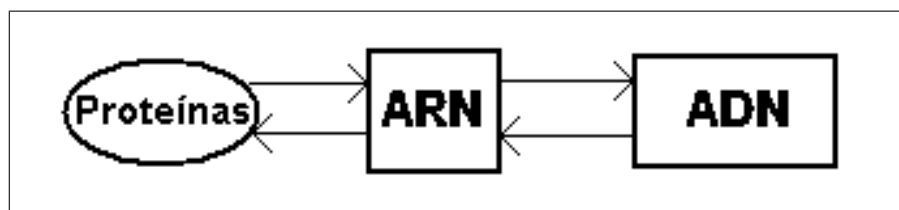


Figura 5.2: Expresión genética del ADN.

Al igual que antes, nada sale ni entra del ADN sino pasa a través del ARN. El ADN es transcrito a una molécula complementaria de ARN, la cual es usada como plantilla para que las proteínas sean fabricadas. (Ver figura 5.2)

Si se hace una aproximación de estos modelos hacia un modelo básico de memoria organizacional, se deben identificar también los tres componentes, antes ya descritos. Para agregar las funcionalidades requeridas de este componente intermedio, entre el proceso de trabajo en sí y el almacenamiento real de la información, de largo plazo, tales como son un almacenamiento rápido del conocimiento, el estructuramiento indexado y, obviamente, la recuperación de este conocimiento. El autor propone como solución para esta estructura, un sistema de despliegue compartido entre los participantes del proceso de trabajo. Los tres grandes tópicos a enfrentar, por ende, son la captura del conocimiento, una arquitectura que soporte esta información y un sistema de recuperación y despliegue de la misma.

El propósito principal de este sistema de despliegue para los equipos de trabajo, es facilitar el razonamiento y aprendizaje de sus miembros tanto como se reúnan para discutir y resolver problemas complejos. Un propósito secundario de este sistema es servir como interfaz para la memoria organizacional, para la captura del conocimiento formal e informal, tanto como para recuperar, de forma transparente, el conocimiento previamente capturado.

5.1.4. Implementación.

La solución elegida posee los siguientes componentes:

- Captura del conocimiento: una persona con el rol de facilitador del sistema, que ingrese la información necesaria;
- Arquitectura: Se elige el modelo conversacional IBIS (Issue Based Information System);
- Despliegue de la información: un sistema de hipertexto que soporte las estructura anterior, en conjunto con el despliegue adecuado. La herramienta utilizada será QuestMap TM. Ver figura 5.3.

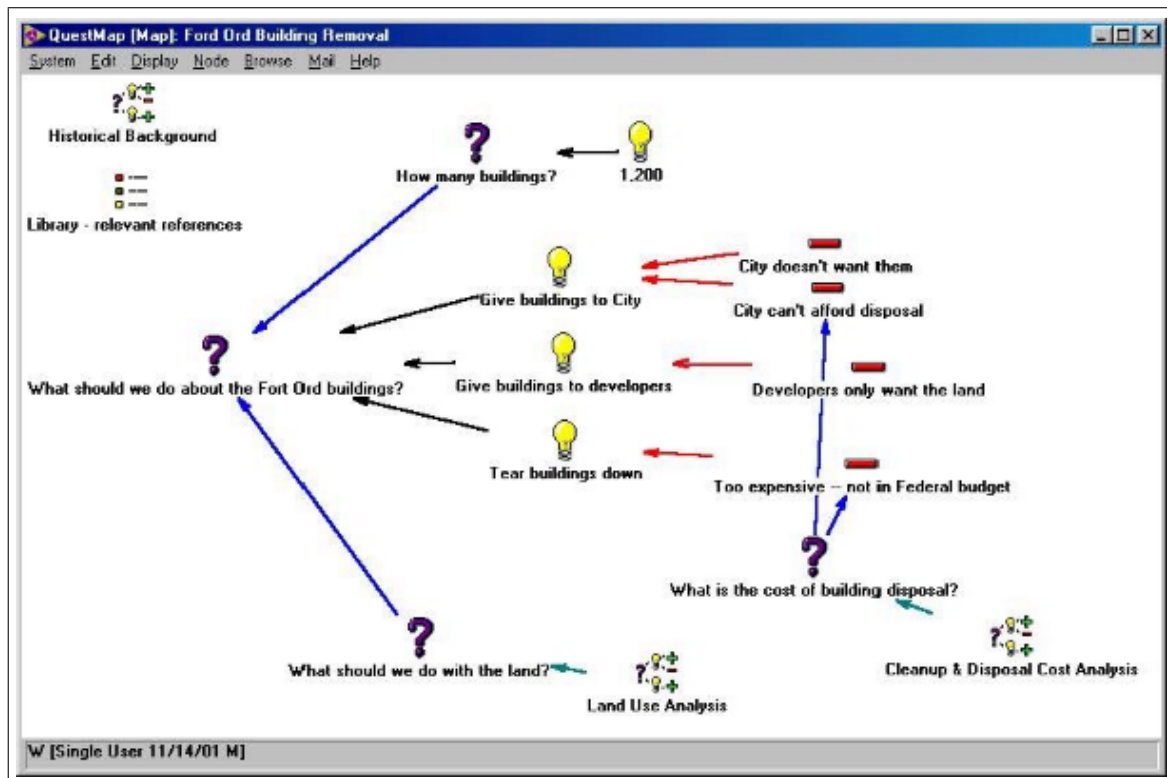


Figura 5.3: Un ejemplo de despliegue en QuestMap TM.

Los pasos a seguir para llegar a implementar un sistema de despliegue, que cumpla con las características descritas son los siguientes:

1. Dar a los miembros del equipo de trabajo el sistema de despliegue, que aumente en forma inmediata la calidad del proceso que involucra conocimiento y eliminar las típicas frustraciones presentes en las reuniones, como la falta de claridad y rigurosidad en la toma de decisiones, reapertura de discusiones ya dadas por cerradas, falta de resultados claros, basarse en las mismas ideas de solución, etc.
2. Conectar el sistema de despliegue a la red computacional de la organización, con el fin de lograr mostrar los resultados en forma distribuida para todos los miembros de la misma.
3. Desarrollar tecnologías y prácticas avanzadas que permitan indexar y almacenar, en una forma transparente, el conocimiento informal en el sistema de despliegue; llegar a recuperar los trozos relevantes de conocimiento informal, al momento de ser necesitados por un usuario del sistema de despliegue.

4. Finalmente, se hace necesario desarrollar mecanismos efectivos de recuperación y captura, que conecten la red organizacional con el sistema de almacenamiento de corto plazo (ACP), presente como componente intermedio del modelo (Ver figura 5.3).

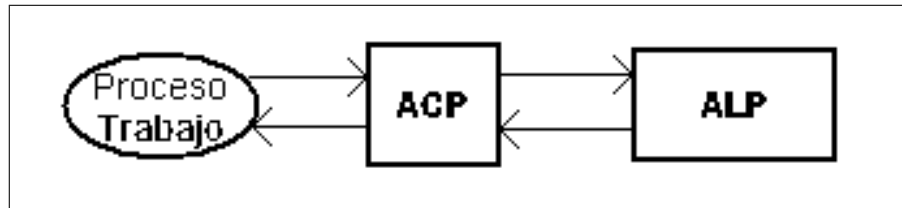


Figura 5.4: Componentes principales del modelo.

Resumiendo, el uso de un sistema de despliegue para el conocimiento informal en reuniones de equipos de trabajo hace este conocimiento explícito y aumenta la calidad del entendimiento mutuo dentro del equipo. El sistema de despliegue funciona como componente intermedio de almacenaje de corto plazo (ACP), y se convierte en una pieza fundamental al momento de diseñar un sistema de memoria organizacional efectivo.

5.2. COLLABCLIO.

Para facilitar el proceso de compartir información usando las redes de comunicaciones modernas, los usuarios deben ser capaces de decidir su propia política de privacidad, es decir qué información proteger, cuál revelar y a quién. [13]

5.2.1. Introducción.

Los autores presentan COLLABCLIO, un sistema diseñado para compartir historias de navegación en la Web, de un usuario determinado. El sistema proporciona políticas claras de privacidad sobre la información, con el fin de hacer expédita los mecanismos de colaboración. Esto dado que lo que se observa hoy en interfaces de privacidad es inadecuado. Un usuario que posea una política de privacidad en mente, a menudo enfrenta medios no muy convenientes para llevarla a cabo. Un ejemplo de ello, es que no hay manera que uno le diga a un teléfono que suene, sólo y si la llamada es de un familiar o amigo cercano, las demás llamadas, por ejemplo, que las envíe a la máquina contestadora. De forma similar, para compartir archivos en sistemas operativos como *Microsoft Windows NT* o *UNIX*, el usuario debe manipular cada archivo o directorio en forma individual. Las interfaces de privacidad descritas están claramente basadas en las propiedades de los objetos individuales, que se ven afectados con la restricción general, sólo si están configurados individualmente. Esto es un inconveniente, si se trata de un gran número de objetos.

Por lo tanto, se necesario definir políticas de privacidad intensionales, como nombran los autores, es decir, que deben apoyar la directa manipulación de los objetos.

5.2.2. Interfaces de privacidad en COLLABCLIO.

Los autores Lau, Etzioni y Weld, en su artículo "*Privacy Interfaces for Information Management*"[13] recopilan la evolución de las interfaces de manejo de información en COLLABCLIO, como un sistema que permite automáticamente compartir las bitácoras de navegación por la Web, con otros usuarios. COLLABCLIO almacena la información de la bitácora, ordenándolas según una palabra clave ("*keyword*") y otros atributos anexos. Con esto, los demás usuarios pueden hacer con-

sultas a la bitácora de navegación de otros usuarios, surgiendo claras amenazas de privacidad. Para solucionar esto, proponen manejar políticas de privacidad como objetos de primera clase, que sean fáciles de crear, inspeccionar, modificar y monitorear. Deben tener una representación compacta y ser aplicados proactivamente a los objetos que aún no han sido creados.

COLLABCLIO proviene de CLIO, un sistema desarrollado por los autores, que captura e indexa el contenido de las páginas Web que el usuario visita. Éste permitía al usuario hacer búsquedas dentro de las páginas ya visitadas e indexadas previamente, en términos de sus atributos como la palabra clave de la página, URL ¹, título, etc. Además de tener la posibilidad de recuperar los URL's para uso personal, a menudo es necesario compartirlos con los demás compañeros de trabajo. Para agregar esta funcionalidad es necesario que el usuario registre su CLIO en un servidor centralizado, perteneciente a la red de la organización. La solución a esto es COLLABCLIO. Con esto, cualquier usuario puede conectarse y revisar el contenido de la bitácora de URLs de otro. Esto, obviamente, conlleva una gran falta a la privacidad de los usuarios y su información. La solución más simple es que los registros sean separados en dos clases: públicos y privados. Para permitir que los usuarios clasifiquen las páginas entre públicas y privadas, los autores diseñaron las interfaces de privacidad para COLLABCLIO.

La primera interfaz diseñada consiste en dos mecanismos: una luz de grabación y una herramienta de *"Buscar & Marcar"*. La pequeña ventana de la luz de grabación (Ver figura 5.5) fue diseñada para estar posicionada cerca de la ventana del navegador Web del usuario. Está basado en la idea de la luz roja en una cámara de video. Cuando la luz está encendida, las acciones – las visitas a las páginas Web, en este caso – se registran como públicas. En cambio, cuando la luz se encuentra apagada, las páginas Web se registran como privadas. Los usuarios pueden cambiar el estado de la luz en cualquier momento y ésta no cambia hasta que el usuario lo desee. Por ende, el uso de esta luz de grabación permite a los usuarios clasificar cada página Web inmediatamente como públicas o privadas.

El segundo mecanismo, la herramienta del *"Buscar & Marcar"*, fue pensado para ser utilizado conjuntamente con la luz de grabación, como método de revisar y de enmendar decisiones anteriores. Una vez que las páginas Web se han ingresado en un índice del sistema COLLABCLIO, el usuario puede utilizar este mecanismo para cambiar las clasificaciones de las páginas Web visitada.

Un inconveniente que surgió, al encuestar a un pequeño número de usuarios, es que el sistema no permite hacer políticas generales de privacidad, esto es, por ejemplo, implementar la política de hacer privadas *"todas las páginas Web del dominio .com"*. Para hacer esto, el usuario debería

¹Uniform Resource Locator.



Figura 5.5: Ventana de elección del tipo de privacidad.

cambiar la luz de grabación a privado, cada vez que visite una página perteneciente al dominio .COM, o periódicamente buscar y marcar los sitios .COM ya visitados, como privados. Obviamente va a existir una ventana de tiempo entre que el usuario visita la página y realmente la marca como privada, quedando la probabilidad no nula de que una consulta remota revele información sensible para éste. Otro problema notado, es que la luz de grabación no se comporta en forma proactiva, esto es, si un sitio fue marcado privado en el pasado, futuras visitas no serán marcadas como privadas, sino como esté seteada la luz de grabación en ese momento.

Teniendo en cuenta estos problemas, los autores notaron que el origen de éstos era la falta del uso de las políticas de privacidad como un objeto. En este caso, una política de privacidad es tratada como un atributo y no como un objeto en sí.

Para solucionar esto, introdujeron los conceptos de representación intensional y extensional de las políticas de privacidad. La primera representación describe una clase de objetos, caracterizando estos objetos, es decir, como en el ejemplo de cómo marcar privadas todas las páginas Web del dominio .COM. En contraste, la representación extensional describe una clase de objetos, enumerando los objetos pertenecientes a esa clase, como el listado de todas las páginas públicas. La luz de grabación crea una política del tipo extensional.

Queda, por consiguiente, la representación intensional que implementar. para esto, los autores crearon un editor de políticas de privacidad (Ver figura 5.6), que posee las funciones de crear,

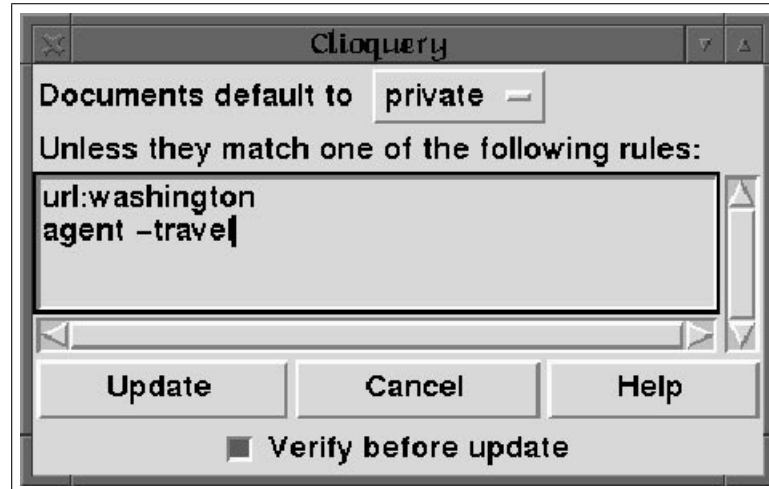


Figura 5.6: Interfaz del editor de políticas de privacidad.

revisar y modificar las políticas creadas por el usuario. Una política de privacidad consiste en la especificación de la protección por omisión y una lista anexa de reglas de excepción a esa restricción. Cada línea en la política representa una regla. Para hacer más fácil el manejo de las reglas generadas por el usuario, se creó una interfaz que despliega y monitorea el título de cada página Web y su clasificación. En la figura 5.7 se muestran los títulos recientemente visitados. Los que poseen el signo (+) son públicas y con (-), los privados. El ícono de la parte inferior denota el estado de la página actual.

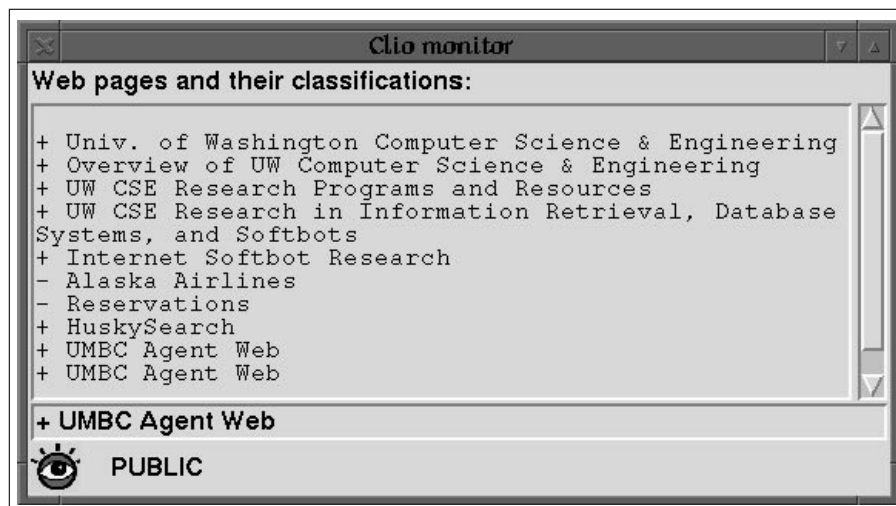


Figura 5.7: Ventana de monitoreo de la política de privacidad.

5.2.3. Conclusiones.

La evaluación final del sistema, con todas las características antes descritas, fue hecha midiendo los criterios definidos por Belloti:²

- *Flexibilidad: lo que cuenta como privado varía de acuerdo al contexto y las relaciones interpersonales. Los mecanismos de control sobre el usuario y los comportamientos del sistema, deben ser tolerables a que los usuarios puedan extender según sus necesidades.*

Las políticas de privacidad son configurables, no fijas; el sistema no impone ningún tipo de privacidad particular a nadie. Una medida de flexibilidad de COLLABCLIO es la expresividad del lenguaje disponible para especificar las políticas de privacidad. La interfaz de privacidad es completamente expresiva con respecto a que cualquier política puede ser especificada sólo con cambiar el estado de la luz de grabación entre público o privado, o posteriormente con el mecanismo de *buscar y marcar*.

- *Confiabilidad: los sistemas deben ser técnicamente confiables e inculcar confianza en sus usuarios. Para hacer esto, deben ser perfectamente comprensibles por sus usuarios. Las soluciones propuestas de la muestra del diseño no deben requerir un modelo mental complejo de cómo el sistema trabaja.*

Como el concepto de interfaz extensional de privacidad parece conceptualmente simple, algunos usuarios malentienden su uso. La interfaz implementa un modelo en el cual cada visita a una página Web puede ser pública o privada, dependiendo del estado de la luz de grabación. Un posterior uso de la herramienta de *Buscar y Marcar* cambiará la calificación de los documentos ya presentes en el sistema, pero esta acción no se aplicará proactivamente a las futuras visitas a dichas páginas Web. Dos usuarios, por ejemplo, erróneamente creyeron que usando esta herramienta de búsqueda y marcado, para especificar una política de privacidad, esta política sería aplicada a páginas Web visitadas en el futuro.

- *Bajo esfuerzo: las soluciones de diseño deben ser livianas de utilizar, requiriendo pocas acciones y poco esfuerzo, de parte del usuario, como sea posible.*

La luz de grabación requiere un pequeño y constante esfuerzo para clasificar cada página web. Aunque en el criterio anterior, algunos usuarios encontraron que el uso del sistema conlleva mucho esfuerzo. Al usar las políticas en forma extensional existe un esfuerzo requerido para crear, inspeccionar y modificar las políticas de privacidad. En cambio, al usarlas en forma intensional, la interfaz basada en reglas, en primer lugar soporta una manera compacta de manejar las políticas de privacidad, al representarla como una lista de reglas y excepciones

²Victoria Belloti, *Design for Privacy in Multimedia Computing and Communications Environments* – 1996

a las mismas. En segundo lugar, la interfaz es proactiva al permitir definir reglas aplicables proactivamente a las páginas Web visitadas o por visitar.

- Sincronización apropiada: *la retroalimentación y el control deben ser provistos en el momento en que son más probable ser requeridos y eficaces.*

Ambas interfaces despliegan inmediatamente la información sobre la operación de la política de privacidad del usuario.

- Perceptibilidad: *la retroalimentación y los medios de ejercer control deben ser perceptibles.*

La retroalimentación y el control están provistos por la luz de grabación, la interfaz de monitoreo y las ventanas de consulta.

- Molestia nula: *la retroalimentación no debe distraer o molestar al usuario.*

Al ver las interfaces se denota que este criterio se cumple. Ver figuras 5.5, 5.6, 5.7.

- Mínima intrusividad: *la retroalimentación no debe implicar la información que compromete la privacidad de otros.*

Se adoptó el principio de que la privacidad del usuario debe permanecer privada, a pesar de las múltiples consultas que se hagan frente a ese usuario.

- Seguridad ante fallas: *en casos donde los usuarios omiten tomar acciones explícitas de protección de su privacidad, el sistema debe minimizar la captura de información tanto como la construcción y el acceso.*

En ambas interfaces, la política de privacidad por omisión es clasificar a las páginas Web privadas, así reduciendo al mínimo la cantidad de información compartida con otros usuarios.

- Significación: *la retroalimentación y el control deben incorporar representaciones significativas de la información capturada y acciones significativas para controlarlas, no sólo información en bruto y acciones desconocidas.*

La luz de grabación es similar a la luz roja usada en una cámara de video. El lenguaje de reglas es similar al lenguaje usado en la mayoría de los motores de búsqueda de la red.

- Bajo costo: *naturalmente se busca que los costos de las soluciones de diseño permanezcan bajos.*

La implementación de COLLABCLIO es un prototipo, por lo que la implementación final deberá reflejar el bajo costo del desarrollo de éste.

Capítulo 6

Tópicos en Privacidad.

6.1. Computadores, bases de datos y la privacidad de la información.

La era de la informática ha aumentado la preocupación con respecto a la protección de la privacidad¹. Esto se denota en los siguientes aspectos:

- La vida de las personas está increíblemente relacionada y atada a los computadores y bases de datos públicas, tales como de registros gubernamentales, de transacciones financieras, comunicaciones personales, etc. En estos tiempos todos prácticamente dejamos una huella de datos, sea lo que sea que hagamos.
- Grandes cantidades de información sobre una persona puede ser capturada, almacenada, procesada y recuperada a un relativo bajo costo. De hecho, las tecnologías de información se han difundido y desarrollado en el mundo pues se mantienen siendo rentables y efectivas. Han creado vastas oportunidades de recoger y de utilizar datos personales de las maneras que habrían sido impracticables y prohibitivamente costosas previamente.

¹Ethics and Technology: Readings for PHIL 236.3. Version 1.1, Ed. Will Buschert y Sarah Hoffman

La información personal se ha convertido literalmente en un *commodity*, algo que se compra, se vende y se negocia en forma natural. En efecto, como colección de datos y que la minería de datos ("*data mining*") cada vez es más barata, la privacidad de los datos personales ha llegado a ser más costosa.

- La gente no puede tener en cuenta las protecciones por omisión que poseen las limitaciones de la memoria humana, las ineficiencias en mantener los registros y las limitaciones de las prácticas de reunir información, usadas en las eras pre – computador.
- Tomando en cuenta todos estos factores, fuertemente se sugiere que los computadores en general y las tecnologías de bases de datos en particular, presentan una seria amenaza contra la privacidad personal.

6.1.1. Consideraciones sobre privacidad.

1. Privacidad como un derecho natural.²

- Entre los derechos básicos e inalienables, es un derecho a la propiedad.
- El derecho a privar la propiedad es una consecuencia de nuestro derecho natural de pertenencia de nuestros cuerpos. Se ve una conexión entre la propiedad intelectual, Locke sostiene que se adquieren los derechos de propiedad cuando mezclamos nuestro trabajo, es decir, la actividad de nuestros cuerpos, con lo material. Nuestra propiedad es una extensión natural de nuestros cuerpos.
- El derecho a privar la pertenencia sobre nuestros cuerpos puede ser extendida a nuestros pensamientos y acciones. Según el punto de vista de Locke y el punto de vista liberal de los derechos en general, el derecho a privar la propiedad es un derecho por negación, un derecho a no interferencia. Como el cuerpo pertenece a cada uno, nadie más tiene el derecho a interferir con él sin el consentimiento del dueño. A su vez, con una propiedad privada, como un terreno, nadie tiene el derecho de traspasarlo, sin consentimiento.
- Una extensión a este derecho de privacidad, debe funcionar de la misma manera: el espacio de los pensamientos y acciones constituye un espacio personal, y , justo como las propiedades inmobiliarias, nadie tiene el derecho de ingresar, cambiar o usar este espacio personal de los pensamientos y acciones, sin el consentimiento del propietario.

²John Locke - Segundo Tratado de Gobierno Civil, 1690 - EE.UU.

2. Privacidad como un componente de libertad y autonomía.

Si es o no es un derecho fundamental e inalienable, la privacidad puede también ser una condición necesaria para otros derechos importantes tales como el ejercicio de la libertad o de la autonomía.

- Para Kant la libertad y racionalidad es lo que distingue al ser humano del resto de la naturaleza. Nuestra capacidad para la autodeterminación normativa es qué nos hace merecer respeto y qué nos obliga a respetar la autodeterminación de los otros: el ser humano merece respeto, ya que puede libremente determinar su futuro y su destino. Sería lógicamente inconsistente con sí mismo no respetar esta misma capacidad de autodeterminación en otros (El imperativo categórico.³). De esta manera, en una visión Kantiana, respetar a alguien como persona es respetar su libertad, teniendo en cuenta que al hacerlo se debe considerar de cómo las acciones y decisiones propias pueden afectar las libertades de otros.
- Si alguien abiertamente observa las acciones de otro, entonces se cambia el contexto de tales acciones y quizás se alteren sus comportamientos. Se hacen concientes de sus actos y se puede llegar a alterar el comportamiento, con el fin de lograr un objetivo y/o aprobación.
- Si, en forma cubierta, se observan las acciones de algún individuo, tal vez no se cause efecto alguno en su autonomía, directamente, pero, no obstante, deliberadamente se engaña a esa persona sobre su propio espacio. Esto es, la persona cree que su espacio propio está inalterado, pero al ser secretamente observado, se alteran las condiciones por razones que no son las propias.

Se hace notar, de alguna manera, que el deber respeto a la privacidad de otra persona es presumiblemente sólo un deber primario (*Prima Facie*). Organismos gubernamentales de seguridad de E.E.U.U., como el FBI, por ejemplo, regularmente violan el presunto derecho a la privacidad, basándose en un deber supremo de preservar la ley y el orden o proteger la vida y propiedad de los ciudadanos.

3. Supervivencia mental.

- Cualquiera situación con respecto a los derechos y a los deberes, parece que la gente tiene cierta clase de necesidad natural de un grado de privacidad.
- Mantenerse como un personaje público requiere esfuerzo y tributos. La salud mental parece requerir poder tener cierta hora y espacio privados, en los cuales hacer y pensar como plazca.

Alguna objeción posible dice relación a que algunos historiadores y antropólogos han discutido que la distinción entre público y privado, por lo menos en un cierto grado, en sí misma

³Emanuel Kant - "Crítica de la Razón Práctica"

es un artefacto tecnológico. Algunos mantenían la idea que la distinción pública – privada se origina con los griegos y que tales delineaciones no se podrían haber hecho en las teocracias del Oriente Cercano antiguo, pues en tales culturas, Dios, como el ente que pone las reglas, permea todo lo existente y no hay cabida posible para la privacidad. Otros argumentan que, entrado el siglo XVI, la privacidad no era ni posible ni deseada, lo cual surgió hace unos pocos cientos de años atrás, en el momento que las viviendas comenzaron a ser más pequeñas y comenzaron a ser construidas con pasillos y espacios secretos.

De cualquier manera, probablemente ninguno de los dos puntos de vista muestran toda la verdad sobre la privacidad, pero vale la pena tener en mente que aún ahora existen distintas culturas, con distintos conceptos de privacidad.

4. Consideraciones utilitaristas.

Varias consideraciones utilitaristas parecen ser relevantes para comprender el porqué se aprecia la privacidad.

- Si las consideraciones de "supervivencia mental" están bien fundadas, entonces al fallar en proveer algún grado de privacidad, se puede preocupar a la gente, sólo por esta razón.
- La información personal sobre una persona, recuperada por otra puede ser inexacta. Esto es que, hasta el punto que se llegue extender, puede llegar a ser una información inútil.
- Además, en algunas clases de información, si son divulgadas a otras personas, difícilmente pueden llegar a ser útiles, debido precisamente a que son exactas.

Este principio puede ser generalizado fácilmente: al poseer derechos de privacidad se pueden incrementar mejores resultados para los individuos, como también incrementar una mayor cohesión social y mejorar los resultados para todos.

6.1.2. Amenazas tecnológicas contra la privacidad de la información.

Ya se hizo notar antes que el derecho a la privacidad de la información es presumiblemente un derecho primario (*Prima Facie*). Los organismos de seguridad gubernamentales regularmente violan este presunto derecho a la privacidad, con el fin de velar por un bien común superior. Este concepto puede ser generalizado diciendo que quizás cualquier teoría sobre cómo la privacidad de la información se justifica, ésta tiene que conceder que si las personas optan por vivir en una sociedad moderna y tecnológica, la información sobre ellas se necesita para un funcionamiento eficaz del gobierno y para los contratos personales normales.

El tipo y el grado de la información que puede ser justificablemente requerida de las personas, sigue estando en tela de juicio sin embargo. Y, finalmente, lo más importante de todo que es a quién le pertenece la información personal y, de esta manera, tiene el derecho de controlarla, está lejos de ser colocada como una cuestión práctica.

6.1.3. Legislación sobre privacidad.

Estados Unidos : Acta de Protección de Privacidad (1974).

- Prohíbe al gobierno mantener bases de datos centralizadas, bases de datos secretas, y bases de datos cuya función no se indica y no se justifica explícitamente.
- No se aplica al sector privado, aunque lo hace la otra legislación, como lo es el *Acta de Reportes de Crédito* (1999).

Organización para la cooperación económica y desarrollo (OECD) : Lineamientos sobre Protección de Privacidad y Flujos de Información (1982).

- Establece principios básicos de privacidad y provee para la restricción de flujo de información entre países que no cumplan con los mismos principios de protección de la privacidad.
- Sirve como base para la estandarización de la Unión Europea de las regulaciones de privacidad (1990), la Directiva de Privacidad de la Unión Europea (1998), la legislación de varios países pertenecientes a la Unión Europea, etc.

Canadá : Acta de Información Personal y Documentos Electrónicos (2000).

- Se aplica a todas las organizaciones en Canadá que capturen, utilicen o divulguen información personal. Con excepción de individuos que utilicen tal información con propósitos periodísticos o artísticos.
- Contiene pautas bastante específicas en el consentimiento, identificando los propósitos para los cuales la información será utilizada, la responsabilidad sobre el uso y la seguridad de las bases de datos de información personal.

Chile : *Ver sección 4 del presente capítulo.*

- Ley N° 19.628, *"Sobre Protección De La Vida Privada"*
- Ley N° 19.799, *"Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma."*
- CONFIARE.cl: conjunto de normas autorregulatorias que buscan proteger el derecho básico de las personas a resguardar su privacidad.

6.2. Privacidad y tecnología.

Como se ha dejado claro ya, la privacidad es un tópico muy importante que concierne a todos. Con las nuevas tecnologías globales de comunicación, como lo es la Internet, han aparecido nuevas amenazas a la privacidad. Existen en este campo potencialidades de desarrollo de las mismas tecnologías, con el fin de solucionar estas constantes amenazas.

En los últimos años la Internet ha visto un enorme crecimiento, con miles de nuevos usuarios que aumentan a razones siempre crecientes. Esta expansión ha catapultado a Internet, desde el campo de la investigación académica hacia una novedosa aceptación general y un aumento de importancia social para el individuo común. Sin embargo, toda esta creciente confianza repentina en la Internet tiene un potencial de amenazar las privacidades personales, que alguna vez se dieron por aceptadas. Esto queda claro al notar que los nuevos usuarios de la Internet, generalmente, no se dan cuenta que cada publicación que hacen en un *newsgroup*, cada email que envían, cada página web al cual tienen acceso y cada producto que compran en línea, se podría monitorear o registrar por terceras personas. Dado esto, el impacto en la privacidad es enorme. Las bases de datos con este tipo de información, ya son una realidad, la existencia del comercio de colecciones de datos personales hacen que esta práctica se haga más común, mientras la demanda por esta información aumenta.

La amenaza de un almacenamiento de largo plazo (bases de datos) y la mala utilización de la información personal se acentúa en Internet. Es técnicamente muy fácil recopilar información y almacenarla por un período de tiempo determinado. Por ejemplo, si se recopilarán todas las publicaciones hechas por un usuario en *USENET*; eventualmente no sería deseable que un futuro empleador viera lo publicado, pasado un tiempo y fuera de su contexto. Una base de datos, a largo plazo, amenaza la posibilidad de elegir que descartar del pasado de cada individuo.

Una de las soluciones más frecuentemente usadas, para contrarrestar esta amenaza es el "ANONIMATO".

Se observa a menudo la utilización de algún tipo de anonimato, con el fin de alcanzar un grado de desvinculación de la identidad física y los datos personales reales correspondientes. En general, en un sentido mucho más amplio, la interacción social anónima es común y culturalmente aceptada. El uso de seudónimos en la literatura, llamados telefónicos anónimos a centros de ayuda y orientación, el secreto profesional del periodismo, que protege la identidad de los informantes, son algunos ejemplos de la aceptación y reconocimiento de esta práctica.

Al igual de cómo se trata fuera de la Internet, se debe asegurar la protección del anonimato dentro de la Internet. Existen varios usos legítimos de anonimato en la red, los cuales son una extensión de los usos normales. Por otra parte, un uso ilícito del anonimato también está presente en Internet. Como la mayoría de las tecnologías, el buen o mal uso del anonimato en la red, va a depender del usuario finalmente. Un uso poco favorable de esta herramienta puede ser la distribución de software protegido, sin los correspondientes permisos; los "spammers", es decir, personas que envían correo electrónico no deseado a miles de otros usuarios, con la finalidad de distribuir sus avisos de marketing, etc. Los proveedores del servicio de anonimato necesitan aprender a prevenir los abusos más efectivamente.

A continuación se mostrarán ejemplos de herramientas que permiten salvaguardar la privacidad de los usuarios en la red.

6.2.1. *Remailers.*

El sistema de remailer⁴ se refiere a un servicio que permite hacer privado el correo electrónico. Un remailer de alta calidad contrasta mucho con el estándar de un Proveedor de Servicio de Internet (ISP), que puede llegar a monitorear, almacenar y compartir información personal de sus usuarios con muchas personas no autorizadas. Hasta hace pocos años, los remailers permitían enviar mensajes electrónicos a grupos de USENET, o a una persona, sin revelar el nombre verdadero o dirección electrónica del remitente. Más recientemente, la aparición de remailers basados en la Web le permiten al usuario enviar correos electrónicos usando el nombre real, pero protegiendo el eventual registro del correo por parte de los ISP's u otras personas.

Hay básicamente tres estilos de remailers, se clasifican en tipos, los cuales indican el nivel de sofisticación y seguridad del mismo. El más famoso remailer del tipo 0 fue `anon.penet.fi`. Proveía la característica de ocultar el remitente del correo, mediante el borrado de los encabezados que podían identificarle. También proveía el anonimato del destinatario: al usuario se le daba un seudónimo al azar en `anon.penet.fi`, el sistema mantenía la privacidad de la relación con la identidad, al tener en secreto la tabla de correspondencia entre la dirección de correo real con su seudónimo. A su vez, el sistema retransmite el correo al usuario y en su dirección real. Dada su facilidad de uso, de este sistema de remailer en particular, fue el sistema más ampliamente usado, aunque se hizo desaparecer como servicio, por presiones legales. La desventaja de este tipo de remailer es que provee un sistema bastante débil de seguridad. Los usuarios del sistema deben

⁴No se encontró una traducción adecuada para el término.

confiar en él, al revelar su identidad al enviar un mensaje a través del sistema. Aún peor, los usuarios anónimos deben confiar en la confidencialidad de la tabla de correspondencia de los datos reales; el anonimato estaría comprometido, si llegara a ser revelada.

El segundo tipo de remailer es el denominado "*Cypherpunk*" (tipo I), que fueron diseñados para solucionar las falencias del tipo anterior. El uso de seudónimos se retiró, por lo tanto, la tabla de correspondencia de las identidades secretas fue descartada. Otra nueva característica es que los servidores pueden aceptar mensajes cifrados, descifrarlos y enviarlos al destinatario. Esto evita la amenaza de que alguien esté escuchando los mensajes, eliminando la relación entre el mensaje de entrada y el de salida. Por último, para alcanzar una más robusta seguridad, se utiliza la ventaja del encadenamiento de los servidores de remailers. Esto es, enviar los mensajes a través de una serie de servidores remailers anónimos, típicamente combinada con encriptación para perder el rastro hacia atrás del mensaje.

El tercer tipo de remailer es el llamado "*Mixmaster*" (tipo II), que rescata y extiende las buenas características del remailer tipo I. Se mantiene el encadenamiento y encriptación entre cada enlace de la cadena, pero además, se utiliza un largo constante de mensaje, con el fin de prevenir el ataque de correlacionar el tamaño del mensaje de entrada, con el de salida.

Todas estas características descritas de este tipo de sistemas, permiten asegurar a los usuarios su privacidad y contrarrestar los ataques maliciosos hacia esta seguridad de la información, suficiente razón para utilizar este tipo de sistemas.

6.2.2. Uso de criptografía.

Información "encriptada", en los términos más simples, son datos hechos inentilgibles al tergiversarlos con procesos de permutaciones matemáticas, controladas por una clave especial. El desciframiento invierte esta acción y hace la información legible de nuevo. Esto es fácil si se tiene la clave disponible. Si ésta, el acceso a la información encriptada es extremadamente difícil en principio, y a menudo imposible en la práctica. Durante los últimos 50 años, la encriptación ha sido en gran parte usada por los gobiernos para esconder la información militar y diplomática, pero está siendo ahora cada vez más usado comercialmente para aparatos como cajeros automáticos, televisión satelital y alarmas antirrobo inalámbricas.

Esta tecnología puede ser utilizada, por ende, como medio para proteger la privacidad de la información, enviada a través de vías poco seguras, como lo puede llegar a ser el correo electrónico o la mensajería instantánea. Además módulos de criptografía pueden ser implementados en aplicaciones tales como navegadores de Internet, con el fin de mantener cierto nivel de confidencialidad en transacciones de comercio electrónico, incluyendo la Capa de Paquetes Seguros (SSL)⁵ para encriptar sesiones entre usuarios y servidores.

Existen variadas herramientas que permiten enviar en forma segura, anónimamente y encriptada a su vez, correos electrónicos. Un ejemplo de esto es la herramienta llamada *SafeMessage TM* ⁶. Es un sistema de comunicaciones seguras, que provee un control y seguridad integrales sobre la información confidencial y sensible, perteneciente al usuario. *SafeMessage* entrega privacidad total al prevenir la duplicación de sus mensajes encriptados. El remitente del correo tiene la posibilidad de configurar restricciones sobre si el destinatario puede copiar, reenviar, guardar o imprimir el mensaje. El software permite solucionar los típicos problemas de privacidad que poseen los sistemas de correo electrónico, tales como:

- El contenido del correo es virtualmente público. Muchas otras personas pueden leer el correo electrónico corporativo, ya se desde dentro o fuera de la organización.
- Los mensajes pueden ser reenviados a participantes involuntarios, sin que el remitente tenga el control.
- Los datos pueden ser almacenados por siempre. Copias de correo electrónico pueden ser archivados a través de todo el mundo.

⁵Secure Sockets Layer.

⁶<http://www.safemessage.com>

- El estado de entrega del correo es incierto. El remitente no está seguro del cuándo y cómo el mensaje llegó.

El sistema resuelve estos problemas entregando un sistema de mensajería encriptada y con estado de entrega del mensaje asegurado. Al hacer una búsqueda por la *World Wide Web*, aparecen un gran número de herramientas de correo electrónico seguro, basados en los mismos paradigmas. Se pueden nombrar *Ensuredmail TM*⁷, *SoftClan e-cryptor TM*⁸, *Zendit by Authora*⁹, etcétera.

⁷<http://www.ensuredmail.com>

⁸<http://www.e-cryptor.com>

⁹<http://www.authora.com>

6.3. Protección de la información de las personas.

A continuación se mostraran dos ejemplos de información sensible para las personas que se transmite por la Internet, y por ende, sujeta a amenazas de privacidad. El primer ejemplo es qué sucede con la información de salud de los usuarios de sitios que manejan las fichas médicas en línea, cómo se regulan y qué restricciones de seguridad poseen para solucionar estas amenazas. La segunda, es el tratamiento de la información comercial y financiera de las personas, por parte de las personas que tienen acceso a ella.

6.3.1. Privacidad en la información médica.

El problema de la privacidad de la información clínica es muy complejo y balancear las necesidades de protección continuarán siendo extremadamente difíciles. Idealmente, las organizaciones podrían considerar políticas de la privacidad conjuntamente con pautas de seguridad. La carencia de la integración durante el desarrollo de los proyectos afines darán lugar seguramente a la duplicación de esfuerzos y de volver a trabajar en políticas y procedimientos.

Los esfuerzos apuntan a crear y afinar códigos éticos de comportamiento, más que crear nuevas soluciones tecnológicas. Un ejemplo de ello es la creación de organismos reguladores de la privacidad de la información médica de los pacientes de diversas instituciones de salud. El caso de Estados Unidos es interesante, existe el organismo llamado "Comisión Federal de Comercio" – (FTC)¹⁰, el cual mediante pruebas a los sistemas de información de éstas instituciones, encontró los siguientes problemas a la privacidad:

1. Los visitantes no son anónimos, incluso si piensan que lo son.
2. Las políticas de privacidad faltan a la verdad en salvaguardar a sus consumidores.
3. Una inconsistencia entre las políticas y las prácticas está presente.
4. La seguridad no es suficientemente alta para proteger la información de la salud.

¹⁰*Federal Trade Commission.*

5. Pocos sitios, que niegan la responsabilidad por terceros involucrados, pueden garantizar que esas entidades están protegiendo la información de la salud de los visitantes.

La amenaza más grande para los consumidores en línea fue identificado como guardar los registros médicos en línea. Por otra parte, la encuesta de la FTC arrojó que el 17 % de los usuarios en línea no buscarían información de salud, debido a las preocupaciones por la privacidad. Esta preocupación puede abrir o cerrar la puerta a un mundo de comercio en línea y de los recursos informativos de gran importancia a los sistemas de cuidado de la Salud. Esta demanda de los consumidores ha conducido a muchos sitios a trabajar juntos y proactivamente a autoregularse.

H.I.P.A.A. : Privacidad Médica – Estándares para proteger la privacidad de la información personal de salud.

Una de las iniciativas más recientes, con respecto a esta autorregulación, es la última regla de seguridad del Acta de Portabilidad y de Responsabilidad del Seguro Médico (HIPAA)¹¹, propuesta por la Secretaría del Departamento de Salud y Servicios Humanos (HHS)¹² y publicada en el Registro Federal de Estados Unidos.

El Congreso hizo un llamado al HHS para publicar las protecciones de la privacidad de los pacientes HIPAA, el año 1996. El acta del HIPAA incluyó los suministros diseñados para enfrentar las transacciones electrónicas y también requirió nuevas precauciones para proteger la seguridad y el secreto de la información de salud. La regulación final cubre planes de la salud, cámaras de compensación de cuidado médico y a los proveedores de cuidado médico que llevan a cabo transacciones financieras y administrativas, por ejemplo, inscripción, facturación y verificación de la información, en forma electrónica. Requirieron a la mayoría de las aseguradoras de salud, las farmacias, a los doctores y a otros proveedores de cuidado médico a cumplir con estos estándares federales, que comenzaron a funcionar en Abril de 2003.

HHS ha dirigido y ha provisto la dirección y la ayuda técnica a los proveedores y negocios de este rubro, para hacer tan fácil como sea posible el poner las nuevas protecciones de privacidad en ejecución. Estos esfuerzos incluyen respuestas a los centenares de preguntas sobre las reglas, así como explicaciones y descripciones sobre los conceptos claves de dicha regla.

¹¹*Health Insurance Portability and Accountability Act – 1996.*

¹²*Department of Health and Human Services.*

Algunos conceptos que estandariza las reglas del HIPAA, frente a las protecciones que se deben tener en cuenta con la privacidad de la información de los pacientes, han fijado una base sobre cómo los planes de salud, las farmacias, los hospitales y otras entidades relacionadas a la Salud pueden utilizar la información médica personal de los pacientes. Estas regulaciones protegen los expedientes médicos y cualquier otra información identificable de los pacientes, si está impresa en papel, en computadores o comunicada por vía oral.

Algunos de los lineamientos claves, presentes en el HIPAA, para estos nuevos estándares son:

Acceso a los registros médicos : Los pacientes generalmente deberían ser capaces de ver y obtener copias de sus fichas médicas y requerir, cuando corresponda, correcciones a la información. Los planes de salud, los doctores, hospitales, clínicas, casas de reposo y otras entidades relacionadas generalmente deberían proveer el acceso a dicha información dentro de 30 días y poder cobrar a los pacientes por el costo de la copia y envío de los registros.

Notificación de las prácticas de privacidad : Los planes de salud, los doctores y otros proveedores de cuidado médico deben entregar una notificación a sus pacientes de cómo pueden usar su información personal y los derechos que los benefician, bajo la nueva regulación de privacidad. Los doctores, los hospitales y otros proveedores directos de salud generalmente proveerán la notificación en la primera visita del paciente, a partir de 14 de abril del 2003, previo requerimiento del mismo. A los pacientes se les pedirá firmar su conocimiento frente a esta notificación. Además, éstos podrán pedir a las entidades que restrinjan el uso o el acceso a su información más allá de las prácticas incluidas en la notificación, con la salvedad de que las entidades pueden no estar de acuerdo con estos cambios.

Límites en el uso de la información médica personal : La regla de privacidad pone límites en cómo los planes de salud y los proveedores pueden usar la información de salud individual de cada paciente. Para promover el mejor cuidado de la calidad para los pacientes, la regla no restringe la capacidad de doctores, de enfermeras y de otros abastecedores de compartir la información necesitada para tratar a sus pacientes.

En otras situaciones, sin embargo, la información personal médica generalmente no puede ser usada para propósitos no relacionados con el cuidado de la salud y las entidades relacionadas pueden usar o compartir sólo una mínima cantidad de información protegida, necesaria por un propósito en particular. Como extensión a esto, el paciente deberá firmar una autorización expresa antes de que algún organismo de salud pueda entregar su información médica a empresas de seguros, bancos alguna firma de *marketing* u otro negocio externo, para propósitos no relacionados con su cuidado médico.

Prohibición de comercialización : La regla final de privacidad fija nuevas restricciones y límites en el uso de la información los pacientes, para propósitos de comercialización. Las farmacias,

los planes de salud y otras entidades de salud deben primero obtener la autorización específica del cliente, antes de divulgar su información médica para fines de *marketing*. Al mismo tiempo, la regla permite a los doctores y a las demás entidades a comunicarse libremente con los pacientes sobre las opciones de tratamiento y otra información relacionada con salud, incluyendo programas de manejo de enfermedades.

Leyes estatales potenciadas : Los nuevos estándares federales de privacidad no afectan las leyes estatales que entregan protecciones adicionales a la privacidad de los pacientes. Las protecciones a la confidencialidad son acumulativas, la regla de privacidad de la HIPAA provee una base a nivel nacional de estándares de privacidad que protegen a todos los ciudadanos, independiente del estado donde estén.

Comunicaciones confidenciales : Bajo la regla de privacidad, los pacientes pueden pedir que sus doctores, sus planes de salud o las entidades relacionadas tomen las medidas razonables que aseguren que las comunicaciones con los pacientes son confidenciales. Por ejemplo, un paciente puede pedir que su doctor llame a su oficina en vez de su hogar, y la oficina del doctor debe adecuarse con esta petición, si es razonablemente fácil de seguir.

Derecho a quejas : Los clientes pueden hacer quejas formales en relación con las prácticas de privacidad de un plan o de una entidad de salud. Tales quejas pueden ser hechas directamente al organismo involucrado del plan de salud o a la Oficina de Derechos Civiles del HHS, el cual se encargará de investigar las quejas y de hacer cumplir la regulación de sobre privacidad. La información sobre el registro de las quejas se debe incluir en el aviso de prácticas de privacidad de cada entidad de salud.

6.3.2. Privacidad en la información financiera.

Al igual que en la sección anterior, la privacidad de la información financiera de las personas se basa en reglas de comportamiento y procesos que regulan el acceso y el uso de dicha información. La literatura carece de aplicaciones específicas que resguarden la privacidad de la información de este tipo. Sólo existen las mismas herramientas que permiten restringir el acceso a información de cualquier tipo, tales como la encriptación de datos, acceso restringido en las bases de datos, uso de la firmas electrónicas, etc.

Una regla adoptada por entidades relacionadas con el manejo de información financiera y comercial de sus clientes, centra las bases de la protección de la información y requieren que ésta debe ser:

- Obtenida legalmente.
- Usada sólo para el propósito especificado originalmente.
- Adecuada, relevante y no excesiva en su propósito.
- Exacta y actualizada.
- Accesible al tema.
- Mantenido segura.
- Destruída, luego que su propósito está completo.

Uso de firma electrónica.

La herramienta más usada para proteger la información financiera y comercial de un individuo es la firma electrónica. Ésta permite identificar unívocamente a un cliente en transacciones en línea, que comprometan traspaso de fondos como, por ejemplo, en compras en línea, en despliegue de información contable de cuentas bancarias o en pagos de cuentas. Debe cumplir las siguientes características, qué hace a una firma electrónica:

1. Debe estar únicamente relacionada a la persona que firma.
2. Debe ser capaz de identificar a la persona que firma.
3. Debe ser creado usando medios, tales que la persona que firman los mantenga bajo su control.
4. Debe estar relacionada a los datos, de tal manera que cualquier cambio en ellos sea perfectamente detectable.

La firma electrónica o digital se basa en el concepto de criptografía de clave pública o "asimétrica", el cual fue introducido por W. Diffie y M. Hellman en el año 1976 [14]. En este tipo de sistemas existen dos claves distintas: una para encriptar y otra para desencriptar. La clave para encriptar es públicamente conocida y, por consiguiente, se denomina "*clave pública*". La clave para desencriptar sólo es conocida por el destinatario del mensaje, por lo que se denomina "*clave privada*". La ventaja de estos sistemas de encriptación es que la denominada clave pública puede ser usada por cualquier persona para encriptar mensajes – transformarlos a texto ininteligible –, bajo la premisa que sólo quien posea la clave privada, podrá desencriptar – ver en forma legible – tales mensajes. (Ver figura 6.1)

La idea básica de un sistema de clave pública radica en que es infactible determinar la clave privada a partir de la clave pública, aunque se utilice el computador más potente para ello. Además, una vez encriptado un mensaje, para cualquier persona que no sea el remitente o el receptor, es computacionalmente infactible encontrar el mensaje original.

Este método es el que permite disponer de esta herramienta análoga a las firmas convencionales: las "firmas electrónicas o digitales". Por consiguiente, de la forma que una firma manuscrita convencional puede ser utilizada en cartas o cheques, para especificar la persona responsable por el documento, una firma digital permite relacionar unívocamente a un documento almacenado digitalmente, con una persona específica y verificar la autenticidad del contenido del documento.

En particular, un sistema de firmas electrónicas establece un esquema por el cual un individuo firmante, puede acompañar un documento por cierta información adicional (una "firma digital"), generada a partir del contenido del documento y de la clave privada del mismo, tal que permita al receptor comprobar que el autor del documento es quién dice ser y que el documento no ha sido alterado. (Ver figura 6.2)

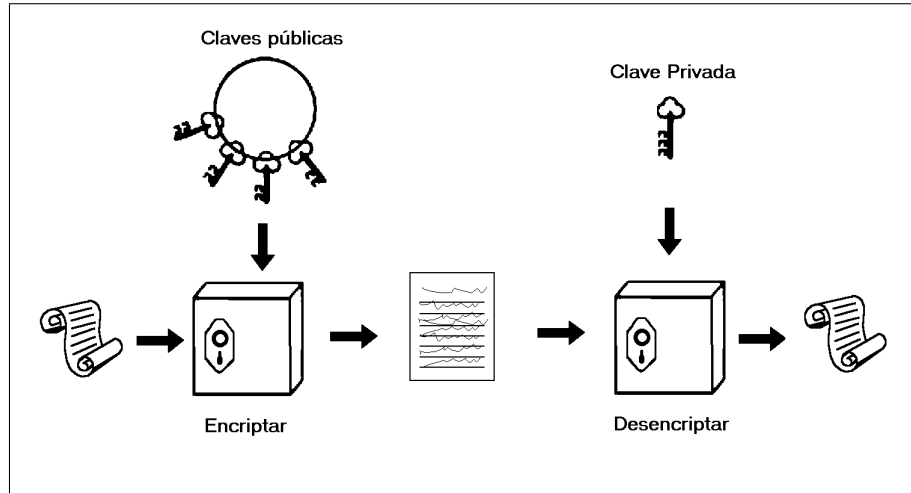


Figura 6.1: Encriptación asimétrica.

Las connotaciones que conlleva la identificación digital de las personas en la red, obviamente hacen surgir evidentes amenazas a la privacidad de las personas. Una legislación clara al respecto es necesaria. En este sentido, el caso de Estados Unidos es interesante. A través de la Comisión de Comercio Federal (FTC)¹³ y en conjunto con la Administración de Información y Telecomunicaciones del Ministerio de Comercio (NTIA)¹⁴ lanzaron un informe que prepararon en común, a petición del Congreso, con respecto a las ventajas y desventajas del requisito de la "demostración razonable", de la entrega del consentimiento de los consumidores presentes en las firmas electrónicas, decretadas en el Acta Global y Nacional de Comercio (ESIGN).

ESIGN asegura que los contratos comprometidos electrónicamente sean legalmente eficaces y válidos. Además que los consumidores que adquieren contratos electrónicamente tienen las mismas protecciones que los que puedan contraer en el mundo real. Para preservar estas protecciones al consumidor, E-SIGN asigna que por mandato la información legalmente requerida para estar por escrito, se puede poner a disposición electrónicamente a un consumidor solamente si éste consiente afirmativamente el deseo de recibir la información en forma electrónica. A su vez, el negocio divulga la información especificada al consumidor antes de obtener su consentimiento y tal consentimiento del consumidor será enviado de una manera que "razonablemente demuestre" que el cliente puede tener acceso a la información en la forma electrónica que será utilizada para proporcionar dicha información.

¹³Federal Trade Commission.

¹⁴National Telecommunications and Information Administration – NTIA

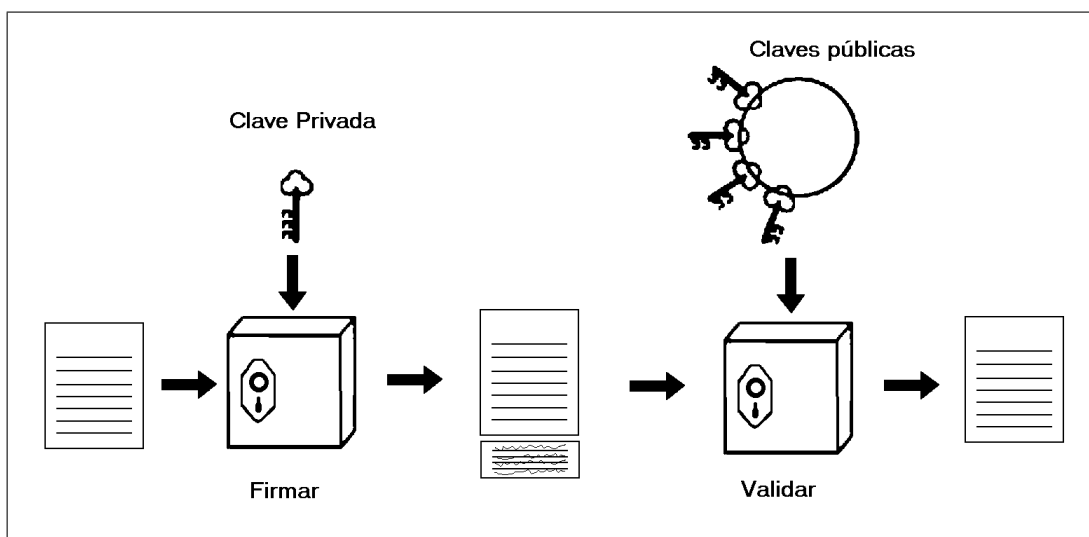


Figura 6.2: Cómo se firma digitalmente.

6.4. Privacidad de la información en Chile.

En Chile existen variados marcos regulatorios sobre el manejo de la información privada de los individuos. Además existen nuevas leyes que regulan las nuevas tecnologías de recolección de datos y la privacidad que deben tener dicha información. Las dos leyes principales que están relacionadas con la privacidad de la información de las personas es la ley N° 19.628, llamada *"Sobre Protección De La Vida Privada"*. La segunda ley es la denominada *"Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma."*, N° 19.799.

6.4.1. Ley 19.628

A continuación se entregará un extracto de la ley 19.628 (*"Sobre Protección De La Vida Privada"*) que regula en Chile la privacidad de la información de las personas.

Artículo 2° Para los efectos de esta ley se entenderá por:

- a. Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.
- b. Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.
- c. Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.
- d. Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.
- e. Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
- f. Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- g. Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas,

las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

- h. Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
- i. Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.
- j. Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.
- k. Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- l. Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.
- m. Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.
- n. Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.
- ñ. Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.
- o. Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Artículo 3° En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas. El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

Artículo 4° De la utilización de datos personales.

El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Esta ley define las bases de qué se debe hacer en materia del manejo de la privacidad de todos los tipos de información personal de un individuo. En general, todos los casos legislativos revisados convergen hacia un punto: la información pertenece al individuo y éste debe ser capaz de restringir el acceso a ella, en los niveles que estime conveniente. Los medios electrónicos de almacenamiento de la información deben lograr brindar este tipo de restricciones y su manejo debe ser confiable, para las partes interesadas. La información que no queda afectada a las restricciones de privacidad es la de libre acceso, ya sea en publicaciones electrónicas y/o escritas, que sean de interés de instituciones afines a tal tipo de información.

6.4.2. CONFIARe.cl

CONFIARe es un conjunto de normas autorregulatorias que buscan proteger el derecho básico de las personas a resguardar su privacidad. Uno de sus objetivos principales es educar a los usuarios de Internet e incentivarlos a exigir que su privacidad sea respetada en el mundo virtual. CONFIARe ha sido creado por la Cámara Nacional de Comercio, Servicios y Turismo de Chile (CNC). Es un programa independiente sin fines de lucro que busca crear un ambiente de confianza en Internet para que sus usuarios se sientan seguros y cómodos, al entregar y compartir información de carácter privado. A través de extensas investigaciones de sitios web, el respaldo de importantes compañías nacionales, internacionales y multinacionales, así como también el apoyo del sector público, CONFIARe ha ganado su reputación de líder promotor de la protección a la privacidad de los usuarios de Internet. Esto lo ha realizado a través de una adecuada entrega de información y permanentes campañas de educación a usuarios y sitios web para que éstos tomen decisiones en la red con pleno consentimiento personal.¹⁵

La idea de esta iniciativa es permitir a los sitios Web asociarse, y con ésto, se adhieren al cumplimiento de siete políticas mínimas de privacidad, a las cuales se asocian todos aquellos portales Web que están preocupados por proteger la información personal de sus usuarios y visitantes.

Un sitio adherido a CONFIARe desplegará un sello en forma clara en su página de inicio, o bien, dejará expresamente claro estar adherido a las Políticas de Privacidad de CONFIARe, en aquella sección destinada a publicar sus propias políticas de privacidad, las que deberán estar en estricta concordancia con las normas definidas por CONFIARe.

Los sitios Web afiliados a CONFIARe garantizan el cumplimiento de las siguientes políticas mínimas de privacidad sobre la información personal de los usuarios o visitantes del sitio:

1. **Recolección:**

El sitio Web afiliado que recolecta o archiva con sistemas propios la información personal vinculada a los usuarios o visitantes lo indicará claramente antes de obtenerla. Si quien recolecta o archiva la información personal de los usuarios del sitio es una empresa distinta a la que administra el sitio web afiliado, esta tercera empresa será identificada claramente, con datos tales como el nombre, dirección, teléfono, número de fax y correo electrónico.

¹⁵www.conficare.cl

2. Uso de la información:

El sitio Web afiliado indicará claramente cómo será utilizada la información personal vinculada con los usuarios del sitio web.

3. Seguridad:

El sitio Web afiliado tendrá implementados y dará a conocer los procedimientos razonables para proteger la información personal vinculada a los usuarios del sitio, teniendo control sobre las posibles pérdidas, mal uso, alteración o entrega no autorizada de dicha información.

4. Calidad:

El sitio Web afiliado tendrá especial cuidado al recolectar, mantener, usar, publicar o distribuir la información personal vinculada a los usuarios y visitantes, verificando que los datos sean correctos, completos y adecuados para cumplir con los fines para los que serán utilizados.

5. Modificación:

El sitio Web afiliado tendrá implementados procesos o mecanismos apropiados para que los usuarios que hayan entregado información personal propia o de terceros puedan modificarla o corregirla. Este proceso de modificación o corrección deberá ser simple y fácil de cumplir. Además contará con un mecanismo de confirmación a los usuarios, en cuanto a la modificación o corrección practicada. Para cumplir con esta exigencia los afiliados cuentan, al menos, con servicio de contacto telefónico o vía correo electrónico con los usuarios.

6. Publicación e intercambio:

El sitio Web afiliado no podrá hacer accesible al público general o compartir con terceros la información personal vinculada a los usuarios o visitantes del sitio, salvo que exista consentimiento de quién entregó dicha información, expresado a través de un documento escrito en soporte papel o electrónico.

No queda incluida por esta restricción:

- a) Aquella información que está disponible por encontrarse contenida en guías telefónicas públicas, reportajes de prensa, publicaciones, zonas de chateo o boletines u otras similares.
- b) Aquella información que sea requerida por la ley, una orden judicial u otro procedimiento legalmente válido que así lo exija.

7. Uso de información personal vinculada a terceros:

El sitio Web afiliado deberá utilizar la información personal vinculada a terceros sólo para los efectos de poder completar y ejecutar la transacción que motivó la entrega o recolección de dicha información.

Las iniciativas de normas autoregulatorias sobre el comportamiento frente al manejo de la privacidad de la información, hacen que los usuarios de Internet conozcan los derechos y obligaciones sobre su propia información personal. Ésto crea la conciencia, por parte de los administradores de los sitios Web, sobre las restricciones de privacidad que posee la información personal de sus usuarios. Por otra parte, del punto de vista de los usuarios, clarifica las convenciones existentes en la red y ayuda a la navegación por la misma, al hacer más fácil identificar los sitios asociados con el compromiso de cumplimiento de las reglas de CONFIARe.

Capítulo 7

Modelo propuesto.

Luego de los casos de estudio revisados en los capítulos anteriores, y de la base de conocimiento en privacidad y las buenas prácticas, generadas a partir de las legislaciones de los distintos países, en el presente capítulo se presentará una propuesta de solución a los evidentes problemas de privacidad en un sistema de memoria organizacional.

Las característica esencial que debe poseer toda política de privacidad, en cualquier tipo de sistema o ámbito, es el **control absoluto sobre el acceso a la información personal**, por parte del dueño de ésta, ya sean datos personales de cualquier índole, o, en este caso, contribuciones a un sistema colaborativo de apoyo a reuniones.

Para agregar a una nueva capa de privacidad de la información potenciada, al modelo del sistema de manejo de la información (KMS)¹, como se muestra en la figura 7.1, se requiere reunir las características importantes que la literatura entrega sobre privacidad de información. Esto conlleva a enfrentar el problema de los diferentes niveles de privacidad que entregan las distintas soluciones. Además, se debe tomar en cuenta el nivel de confianza que se le entregue al usuario y la conciencia que él mismo posea al momento de decidir entre una política de privacidad de otra.

¹Knowledge Management System.

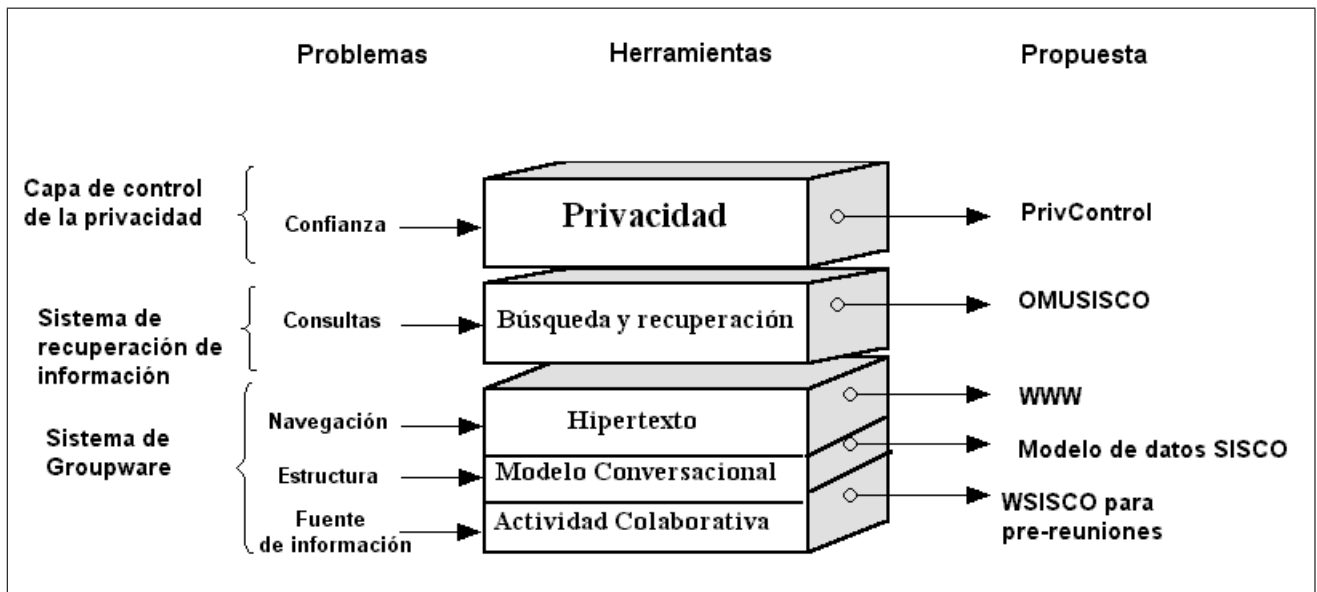


Figura 7.1: Componentes del sistema de manejo de información (KMS).

Las distintas soluciones propuestas, que definen un nivel independiente de privacidad para cada uno, se pueden clasificar dependiendo del momento en que expresen su mayor utilidad, es decir, antes, durante o después de la reunión, en la cual aparecen los aportes de los participantes de la misma.

Estas son:

◇ *Antes de la reunión:*

- Antes de la reunión misma, se puede tener un plan de acción con respecto a la privacidad. El facilitador puede planear para cada ítem de la minuta de la reunión si los aportes a la discusión de los mismos, se hacen en forma anónima, semi-anónima o abiertamente. Al comienzo de la reunión, el facilitador da a conocer a los participantes las capacidades que posee el sistema, en materia de privacidad.

◇ *Durante la reunión:*

- Implementar los paradigmas de memoria de corto plazo y de largo plazo:
En una reunión típica hay contribuciones que son explícitamente hechas para los registros y otras que no. No debería haber ningún registro de tal información, ya que el autor no desea estar comprometido a ella. La memoria de largo plazo contiene toda la información que será archivada. En cambio, en la memoria de corto plazo, la información será borrada al momento de terminar la reunión. La decisión si una contribución pertenece a la memoria de corto o largo plazo, puede ser hecha en cualquier momento de la reunión, por parte del participante.
- Niveles de autoría, con distinta precisión:
Para proteger la privacidad en la memoria de la reunión, es importante poder controlar la autoría de los aportes. Para conciliar la necesidad de entender la información guardada, fuera de su contexto, y la necesidad de proteger la privacidad, la introducción del concepto de niveles de autoría es útil. El autor del aporte puede decidir si su contribución será almacenada bajo su autoría individual (por ejemplo, Juan Pérez), la autoría de un subgrupo a cual pertenece (por ejemplo, campaña publicitaria de jabones), la autoría del grupo a cual pertenece (por ejemplo, departamento de marketing), la autoría de la organización completa (por ejemplo, Compañía de Perfumería); o absolutamente anónimo. Esto permite al participante decidir el nivel de autoría de su contribución. A la vez, puede usar un nivel por omisión, que puede cambiar cuando desee, dependiendo de las circunstancias.

- Uso de seudónimos:

Cualquier participante que quiera mantener su participación confidencial, puede ingresar al sistema bajo un seudónimo. Las contribuciones hechas de esta manera, pertenecerán al grupo de trabajo.

- Uso de encriptación asimétrica, al guardar la información:

Para agregar un nivel más alto de confidencialidad se puede utilizar la seguridad que brinda la criptografía. La idea es mantener un sistema de claves públicas para cada uno de los usuarios del sistema, con la finalidad de asegurar la confidencialidad posterior de la información. Si el autor de la contribución lo desea, es posible encriptar los aportes con su clave pública, por lo que sólo él podrá ver el contenido de las contribuciones, pues él solamente posee acceso a su clave privada. (Ver figura 6.1), evitando el posterior mal uso de la información al estar disponible a cualquier persona.

◇ *Después de la reunión:*

- Derechos de acceso a la información:

Los DBMS ²y los sistemas operativos entregan protección a los datos, dando distintos privilegios de acceso a usuarios seleccionados. La idea es proteger la información de un posterior mal uso. Esto es similar a lo propuesto por Pino y Guerrero en su trabajo "*Understanding Organizational Memory*"[7], denominado perfiles de usuario.

- Marcas de tiempo relativas o difusas:

La información de las marcas de tiempo pueden amenazar otras medidas de privacidad, al permitir reconstruir la información de la reunión a partir de éstas. Almacenar la hora exacta de la contribución hace posible rearmar la reunión y las personas que participaron en ellas. Una manera de desvincular y perder el rastro de las contribuciones con el autor, es guardar sólo la hora o fecha de cuando fue creada. Otra manera, es utilizar una hora relativa con respecto a la reunión en sí, es decir, comenzar un contador en 00:00 al comienzo de la reunión, permitiendo proteger la contribución de ser identificada con cierta reunión.

- "Envejecimiento" de la información:

Hacer que la memoria organizacional, en la medida que pasa el tiempo, vaya siendo más selectiva con lo que "recuerda". Esto es, inicialmente almacenar toda la información de la contribución, pero al pasar el tiempo, la información se va haciendo más general. Por ejemplo, en los aportes almacenados se puede quitar el autor, dejándolos anónimos. Luego, hacer un resumen de los mismos, dejando sólo los encabezados de las contribuciones, etc. Esta idea es una metáfora de la memoria humana, ya que, en general, al recordar una conversación sólo logramos recordar lo dicho en ésta, pero no el autor. Y mientras más lejana en el tiempo esté, sólo se recordará los tópicos más importantes y en una forma cada vez más sintética. Esto es similar a lo propuesto por

²Database Management System.

Pino y Guerrero en su trabajo "Understanding Organizational Memory"[7], denominado olvido programado.³

Cada una de estas estrategias definen un nivel propio de privacidad, inherente a las fortalezas y debilidades que posean. Además algunas al favorecer la confidencialidad de la información, pueden atender a la colaboración entre los integrantes, que busca el sistema de memoria organizacional. En la siguiente tabla, se hará una comparación de las estrategias por separado.

Política de privacidad.	Nivel de Privacidad	Apoyo a la colaboración.
Plan de acción antes de la reunión.	Medio	Medio
Memoria de corto y largo plazo.	Medio–bajo	Alto
Precisión en los niveles de autoría.	Medio	Medio
Uso de seudónimos.	Medio–alto	Bajo
Encriptación de la información.	Alto	Bajo
Perfiles de usuario.	Bajo	Alto.
Marcas de tiempo relativas.	Alto	Bajo
Envejecimiento de la información.	Medio	Alto

Al situarse antes de la reunión misma y que la persona que tome el rol de facilitador le permita a los usuarios elegir un plan de privacidad para cada ítem de la minuta de la reunión, es decir, si la discusión se hará en forma anónima, semi-anónima o abiertamente para tal ítem, hace que el nivel de privacidad dependa del plan elegido. En un extremo, si los ítemes se discuten completamente en forma anónima, se reduce el caso de uso de *anonimato* en las contribuciones, con lo que el nivel de privacidad de dicho caso es alto, pero el nivel de apoyo a la colaboración entre los participantes es muy bajo[7]. En cambio, en el otro extremo, si se elige hacer los aportes al sistema en forma abierta, el nivel de privacidad baja y a su vez, el apoyo a la colaboración aumenta a un nivel muy alto. En el caso promedio, esto es, si se elige usar anónimo o contribuciones abiertas, indistintamente en forma uniforme, los niveles también se estabilizan en los casos promedio, es decir, el nivel de privacidad es medio y el nivel de apoyo a la colaboración es medio. Lo mismo sucede si se utiliza el plan de semi-anonimato en las contribuciones.

En el momento de la reunión se pueden dar varios escenarios. El empleo del paradigma de memoria de corto y largo plazo da la posibilidad de tener "contribuciones sin rastro". La decisión si una contribución pertenece a la memoria de corto o largo plazo, puede ser hecha en cualquier momento de la reunión. Esta estrategia no es capaz de proteger a los participantes dentro de la

³*Scheduled forgetting.*

reunión, de otro participante, pues este último puede hacer fácilmente una copia de la memoria de corto plazo. Aunque el sistema, de esta manera, protege de los usuarios externos a la reunión, por lo que el nivel de privacidad es medio bajo. El nivel de apoyo a la colaboración es alto, ya que los participantes sólo mantienen en el tiempo las contribuciones más importantes después de la reunión, y sólo pueden ser vistas por los integrantes de la reunión. Por otra parte, el uso de niveles con distinta precisión en la autoría, el nivel de privacidad queda determinado a un promedio, ya que como el usuario tiene la posibilidad de controlar la precisión de la autoría de los aportes, éste puede elegir uniformemente entre autoría individual hasta el anonimato, para cada uno de los ítemes de la agenda de la reunión.

Equivalentemente al caso de antes de la reunión, el apoyo a la colaboración de esta estrategia será medio, pues dependerá de la elección del nivel de precisión que escoja el usuario. El uso de seudónimos hace que el nivel de privacidad sea medio-alto, pues podría no ser posible probar que cierta persona corresponde a cierto seudónimo. En materia de colaboración, se le permite al usuario saber el número de participantes en la discusión, pero no sus identidades, lo que conlleva a que el nivel sea bajo. Si se utiliza encriptación al momento de almacenar la información, el nivel de protección que entrega esta tecnología se traduce a un nivel de privacidad alto, considerando que nadie más que el autor de las contribuciones podrá ver el contenido de ellas. Por lo tanto, el nivel de colaboración de esta estrategia será bajo, ya que la información no estará disponible para ningún usuario que no sea el autor.

Después que los aportes están almacenados en el sistema, es decir, luego de la reunión, las estrategias de privacidad definen distintos niveles de privacidad y de colaboración. Al emplear la política de generar derechos de acceso a la información, es decir, poseer distintos perfiles de usuario con distintos privilegios, hace que el nivel de privacidad presentado para esta estrategia sea bajo, pues cualquier persona con los privilegios suficientes puede hacer mal uso de la información almacenada. Además, no daña un nivel básico de colaboración entre los integrantes, por ende el nivel es alto de apoyo a la misma. En el caso siguiente, de uso de marcas de tiempo relativas o difusas, al anular el vínculo del tiempo de creación de la contribución, hace, a su vez, que los aportes pierdan la relación con el participante, al sólo almacenar, por ejemplo, la hora o el día de la contribución. De esta manera, el nivel de protección de la privacidad del usuario es alto. Para fines de colaboración, si se pierde este vínculo, el nivel de apoyo es bajo, al igual que en los casos anteriores. Al lograr que la información registrada envejezca, es decir, que con el paso del tiempo se haga más resumida, el soporte entregado por esta estrategia a la colaboración es alto, pues la información de los integrantes está presente en el momento de la interacción, pero sólo se va perdiendo en la medida que pasa el tiempo. Por otro lado, en materia de privacidad el nivel se puede considerar dependiente del tiempo que haya transcurrido desde la creación del aporte. Esto quiere decir, que cómo la información va perdiendo exactitud y ganando generalidad mientras pasa el tiempo, va a depender de en qué momento la información es accesada. Por lo que se puede considerar un nivel de privacidad medio.

Luego de detallar los distintos niveles de privacidad y de apoyo a la colaboración de las diferentes estrategias, anteriormente nombradas, se hace necesario crear nuevas estrategias mixtas, que unan las fortalezas de las individuales. Una forma de lograrlo es utilizar más de una estrategia individual, con el fin de potenciar las fortalezas de cada una y disminuir las debilidades.

La manera propuesta de utilización de las estrategias y teniendo en cuenta que el usuario debe tener el control absoluto de sus contribuciones al sistema de memoria organizacional, en el nivel de que éste desee, es entregarle la posibilidad de elegir entre niveles crecientes de privacidad. Cada nivel de privacidad tendrá una batería de estrategias predefinidas, que perfilaran el nivel de confidencialidad deseado por el usuario. Se plantea, por lo tanto, el uso de una interfaz que permita al usuario escoger cada nivel de privacidad predefinido. En cada uno de los niveles, se implementarán una o más estrategias de las estrategias anteriormente nombradas. El nombre del sistema se eligió tal que denotara el control sobre la información de parte del usuario. Éste es **PrivControl**.

7.1. PrivControl.

Se pueden especificar los distintos niveles de privacidad, definidos por la elección que de el usuario. En la siguiente tabla se encuentran ordenados ascendentemente en nivel de privacidad.

Nivel de privacidad.	Estrategias a utilizar.
1. Aceptar todo.	▪ No se utiliza ninguna estrategia de privacidad.
2. Bajo o básico.	▪ Registros de corto y largo plazo. (Medio–bajo) ▪ Uso de perfiles de usuario. (Bajo)
3. Medio	▪ Registros de corto y largo plazo. (Medio–bajo) ▪ Niveles de precisión en la autoría. (Medio) ▪ Uso de seudónimos. (Medio–alto) ▪ Envejecimiento de la información. (Medio)
4. Alto	▪ Uso de seudónimos. (Medio–alto) ▪ Encriptación de la información. (Alto) ▪ Marcas de tiempo relativas o difusas. (Alto)
5. Restringir todo	▪ Niveles de precisión en la autoría. (Medio) ▪ Uso de seudónimos. (Medio–alto) ▪ Encriptación de la información. (Alto) ▪ Marcas de tiempo relativas o difusas. (Alto) ▪ Envejecimiento de la información. (Medio)

La elección de las estrategias de cada nivel de privacidad se hizo ordenando de manera ascen-

dente cada una de las estrategias individuales. Se agregó al lado de cada una, su nivel individual de privacidad. No se consideró el nivel de colaboración de cada estrategia, pues la interfaz contempla solamente como más, importante, el nivel de privacidad que le puede agregar a este tipo de sistemas y, por consiguiente, el nivel de confianza que pueda tener el usuario.

La elección de estos niveles de privacidad se asemeja a la interfaz que entrega el navegador *Internet Explorer* de Microsoft, que permite elegir al usuario, la configuración del nivel de privacidad al visitar ciertas páginas Web. (Ver figura 7.2)

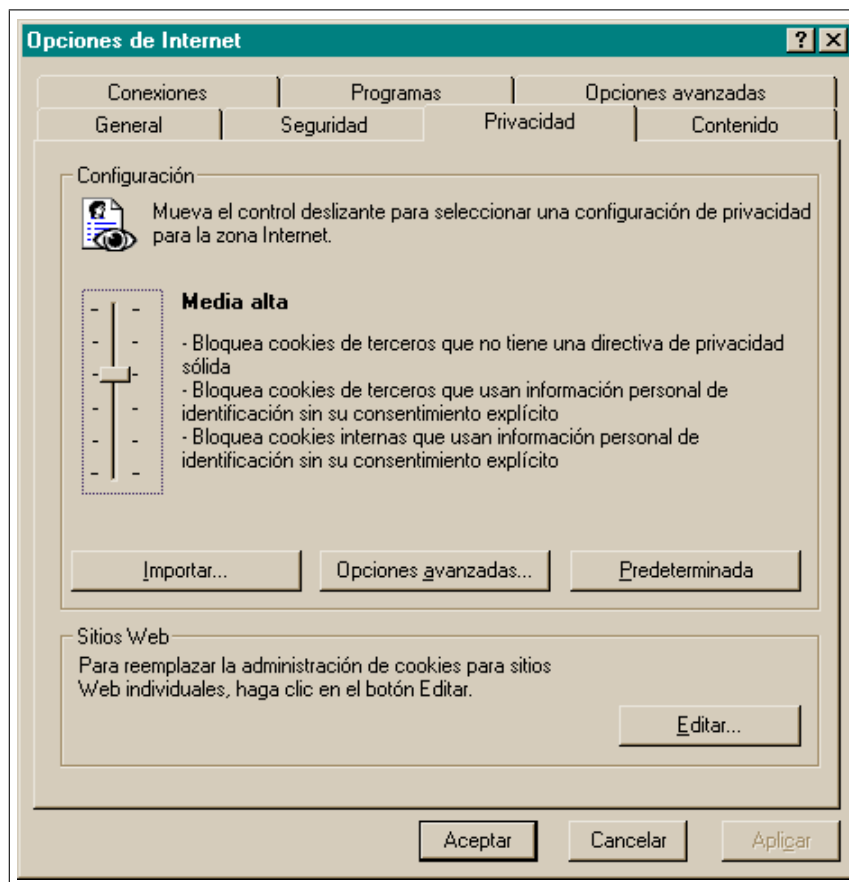


Figura 7.2: Interfaz de configuración de IE.

Capítulo 8

Diseño de PrivControl

8.1. Casos de Uso.

A continuación se detallarán los casos de uso de las estrategias de privacidad, individualmente.

8.1.1. Plan de acción antes de la reunión

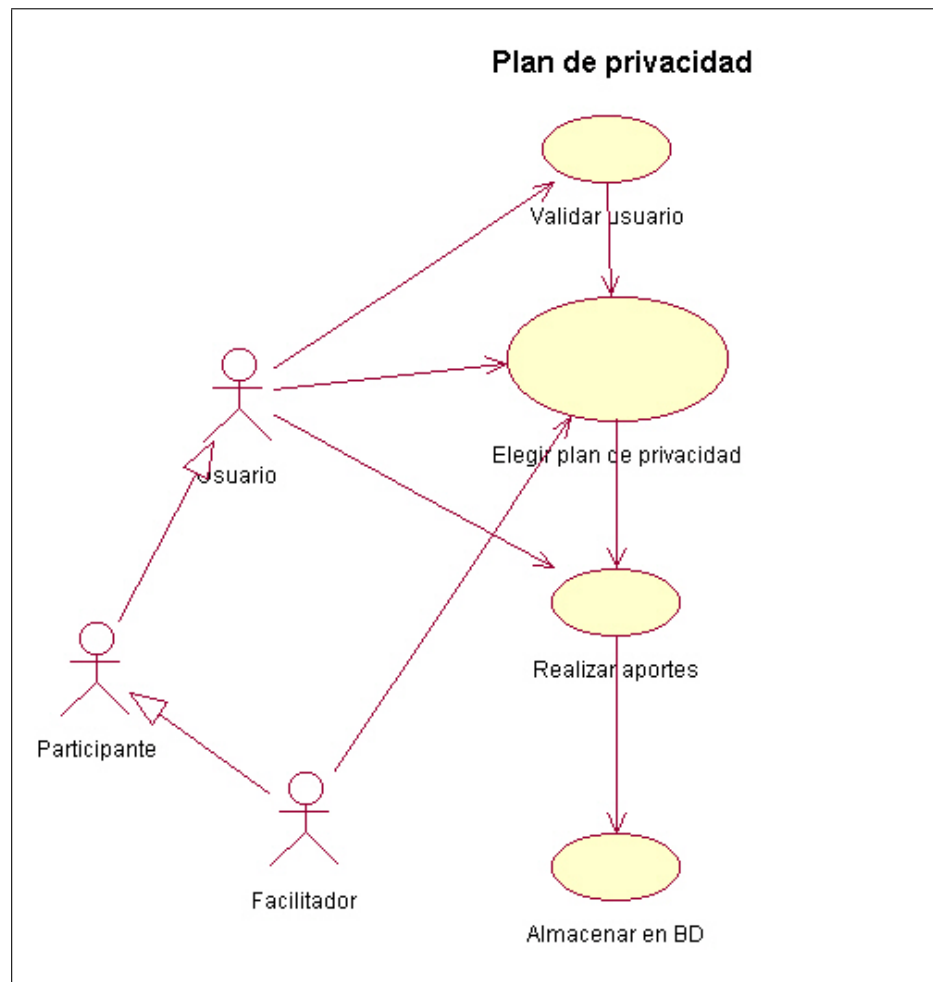


Figura 8.1: Estrategia aplicable antes de la reunión.

CASO DE USO: Plan de privacidad antes de la reunión.

ACTORES: Facilitador, participante.

TIPO: Opcional.

DESCRIPCION: Al ingresar al sistema, el usuario participante puede elegir el plan de privacidad que desee, previamente definidos por el facilitador. Luego puede realizar los aportes.

8.1.2. Memoria de corto y largo plazo.

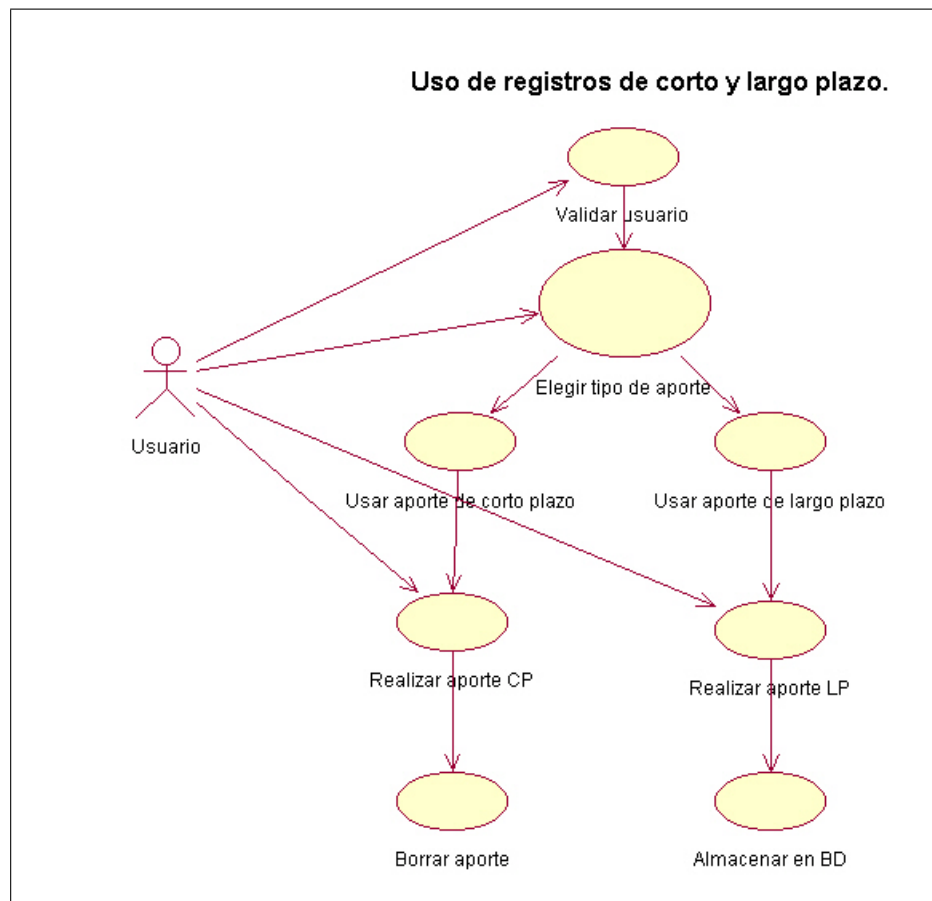


Figura 8.2: Registros de corto y largo plazo.

CASO DE USO: Uso de registros de corto y largo plazo.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: El usuario elige el tipo de registro que desea utilizar, de corto o largo plazo. Luego puede realizar los aportes, que serán guardados dependiendo de la elección inicial.

8.1.3. Precisión en los niveles de autoría.

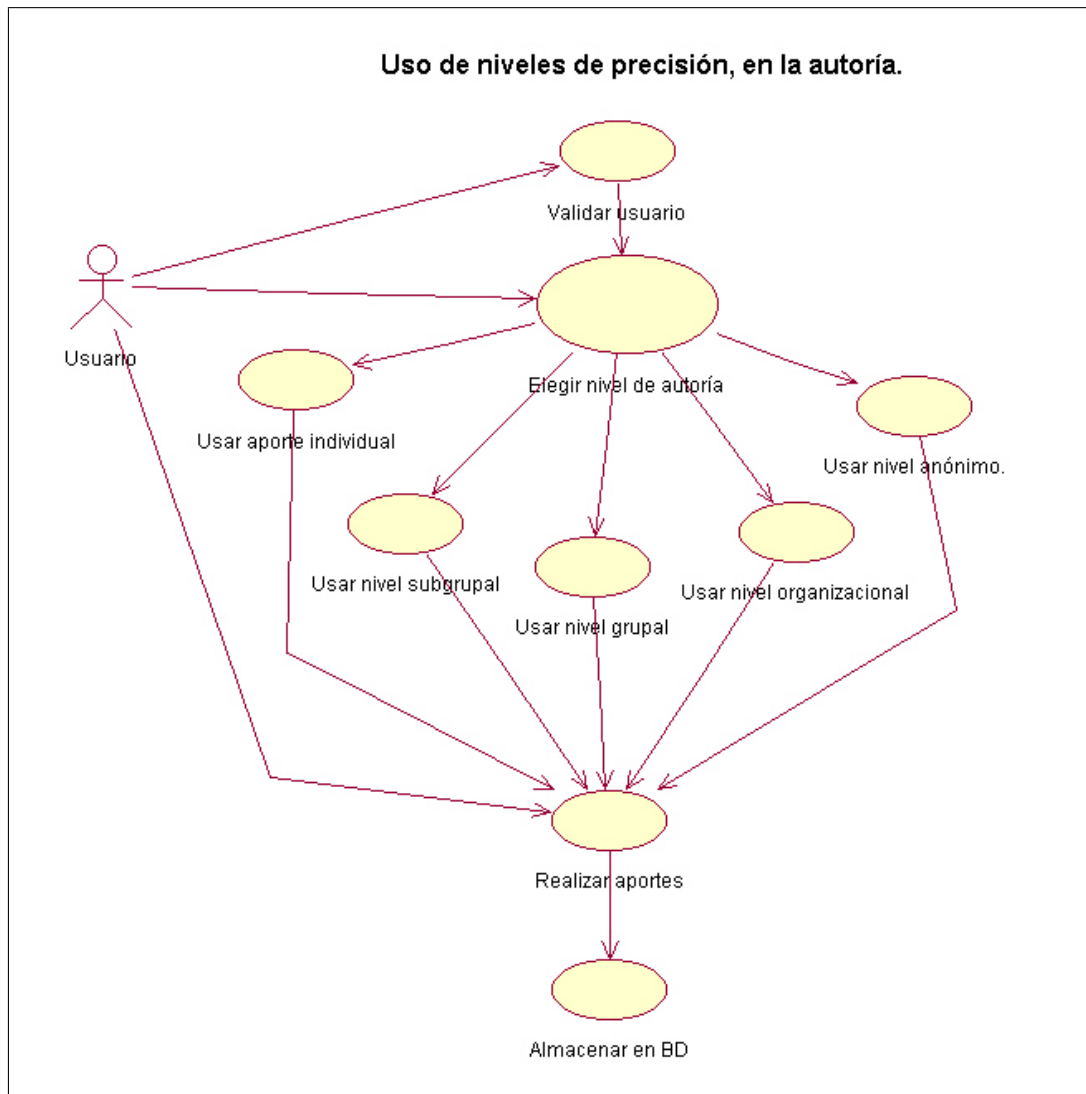


Figura 8.3: Niveles de precisión en la autoría.

CASO DE USO: Uso de niveles de precisión.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Para cada aporte individual al sistema, el usuario es capaz de elegir el nivel de autoría, desde un nivel individual hasta un aporte anónimo.

8.1.4. Uso de seudónimos.

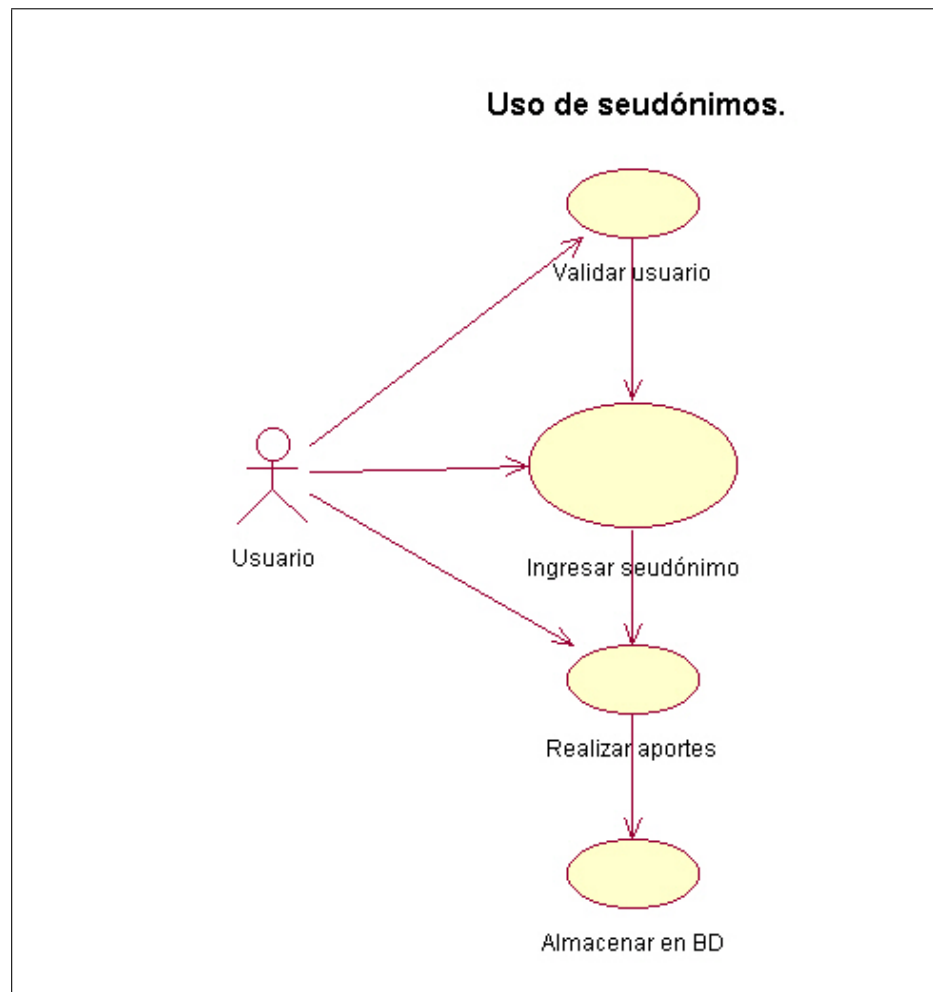


Figura 8.4: Uso de seudónimos.

CASO DE USO: Uso de seudónimos.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Al ingresar al sistema el usuario elige el seudónimo por el cual será conocido en el sistema. Luego puede realizar los aportes.

8.1.5. Encriptación de la información.

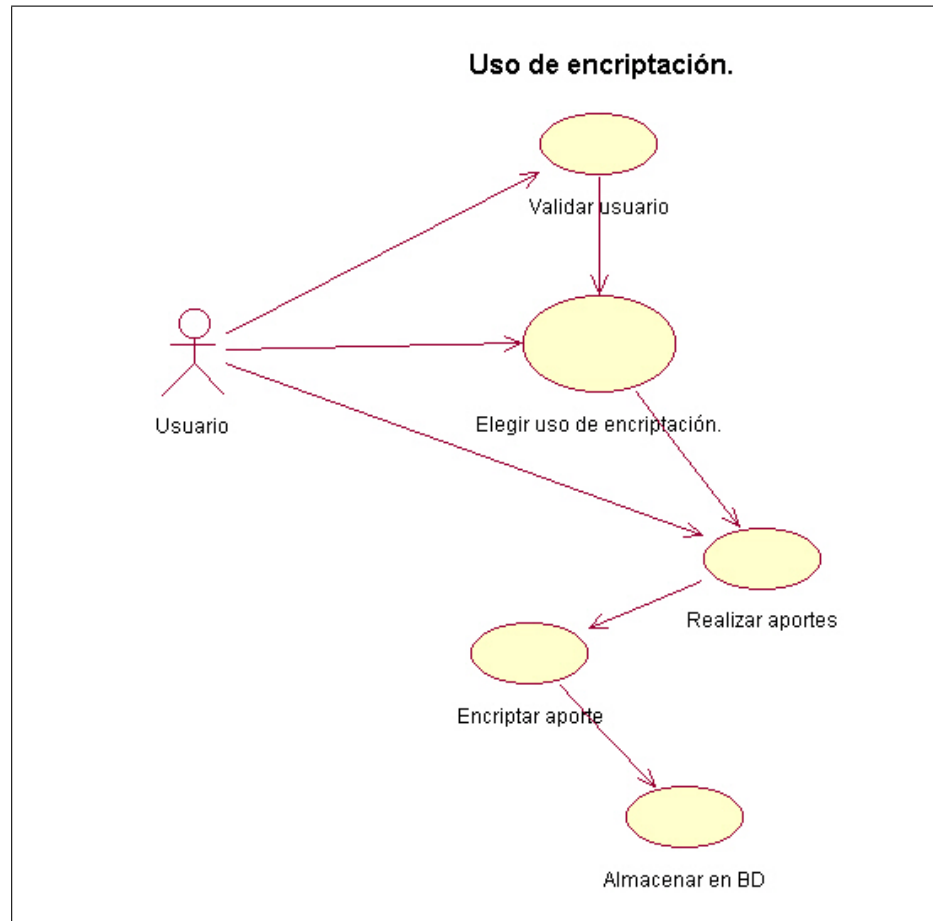


Figura 8.5: Encriptación.

CASO DE USO: Uso de encriptación.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Al elegir usar encriptación, el usuario debe proporcionar al sistema su llave pública para encriptar los aportes. Con la cual, éstos serán almacenados encriptados en el sistema.

8.1.6. Perfiles de usuario.

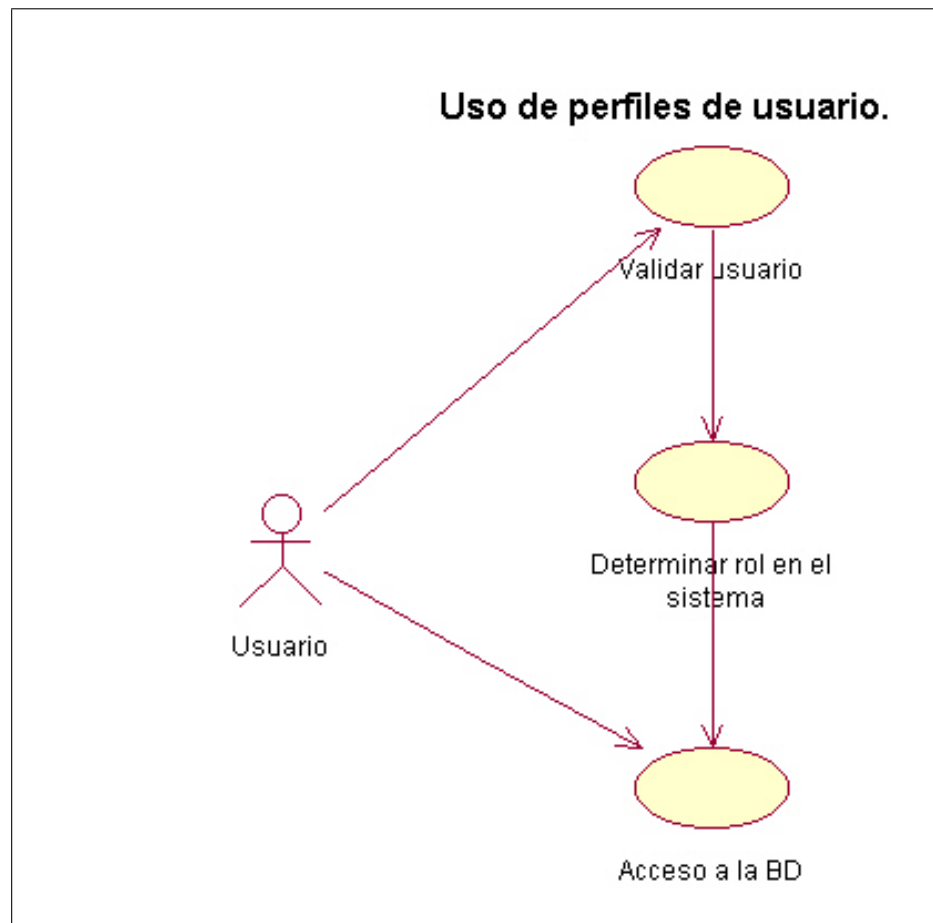


Figura 8.6: Perfiles de usuario.

CASO DE USO: Uso de perfiles de usuario.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Al ingresar al sistema y estar definida la pre-reunión, el sistema es capaz de identificar al usuario dependiendo del rol que posea en ella.

8.1.7. Marcas de tiempo relativas.

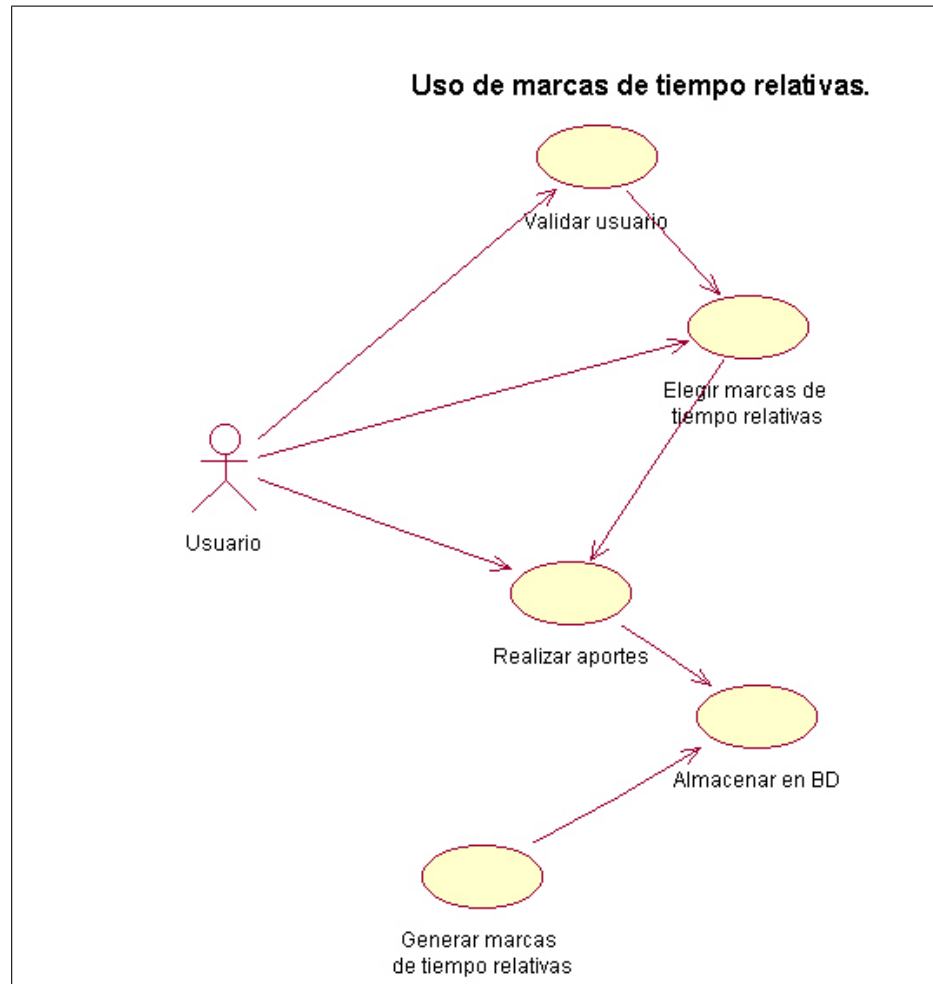


Figura 8.7: Marcas de tiempo difusas o relativas.

CASO DE USO: Uso de marcas de tiempo relativas.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Al ingresar al sistema, el usuario elige usar marcas de tiempo relativas, por lo que el sistema almacena los aportes con fechas de creación relativas a la pre-reunión misma.

8.1.8. Envejecimiento de la información.

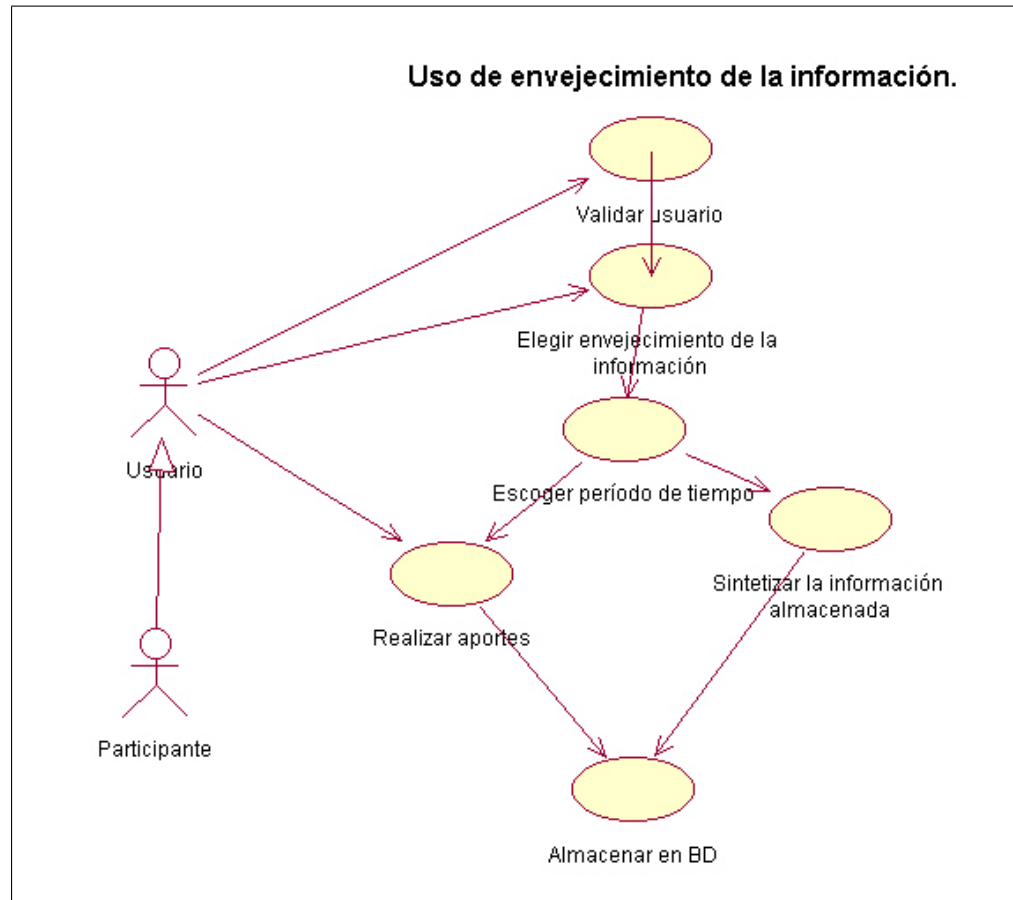


Figura 8.8: Información desechable.

CASO DE USO: Uso de envejecimiento de la información.

ACTORES: Usuario participante.

TIPO: Opcional.

DESCRIPCION: Al elegir el usuario el uso de envejecimiento de la información, debe entregar al sistema el periodo de tiempo

8.1.9. Modelo completo.

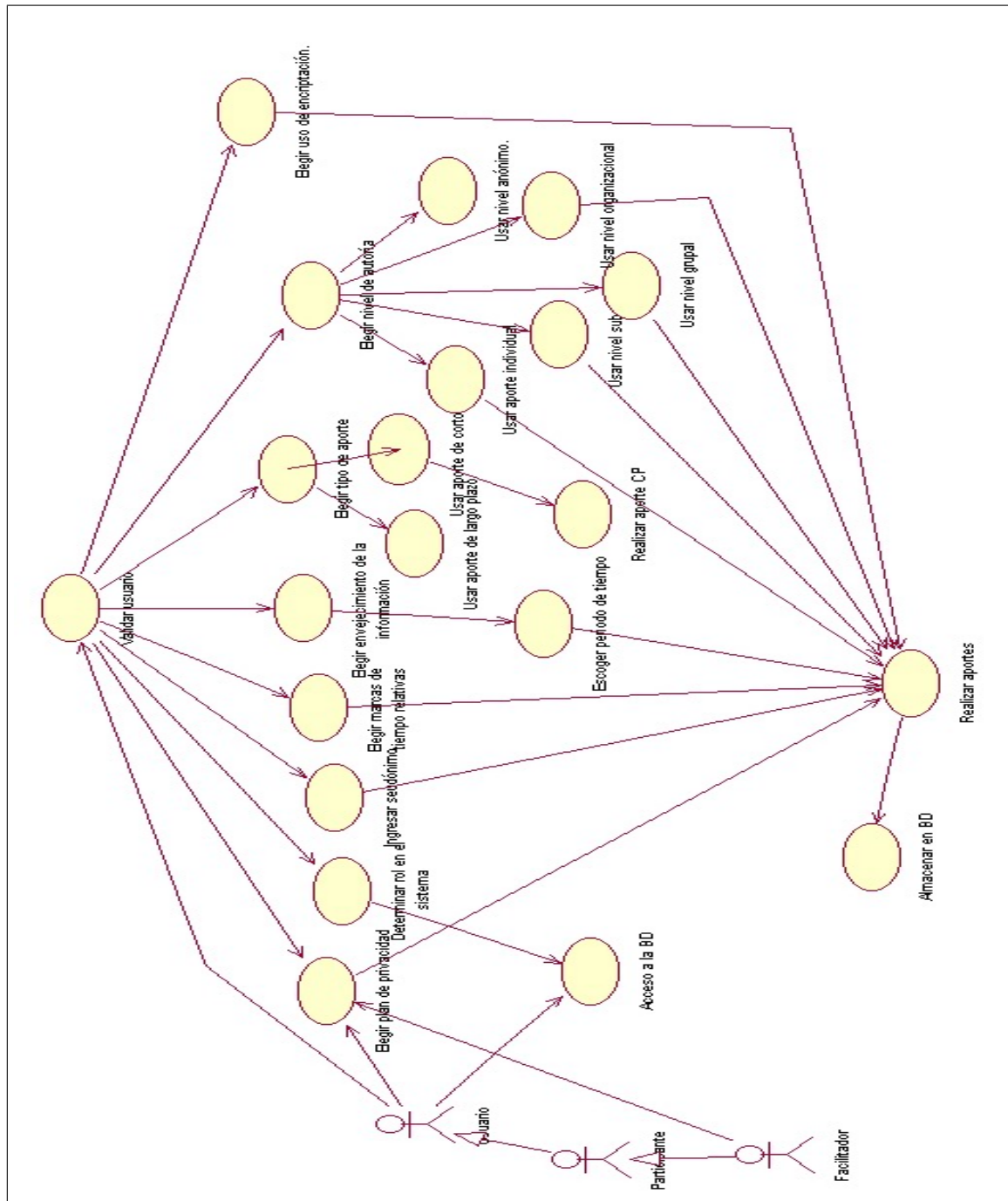


Figura 8.9: Modelo completo - 8 estratégias.

CASO DE USO: Todas las políticas.

ACTORES: Usuario participante, usuario facilitador.

TIPO: Real.

DESCRIPCION: Es la agregación de todas las políticas de privacidad anteriores.

8.2. Casos de uso para los niveles predefinidos.

En la presente sección se mostrarán los modelos de casos de uso de los distintos niveles de privacidad, predefinidos por el usuario, como también configurados.

8.2.1. Nivel de privacidad "Aceptar todo".

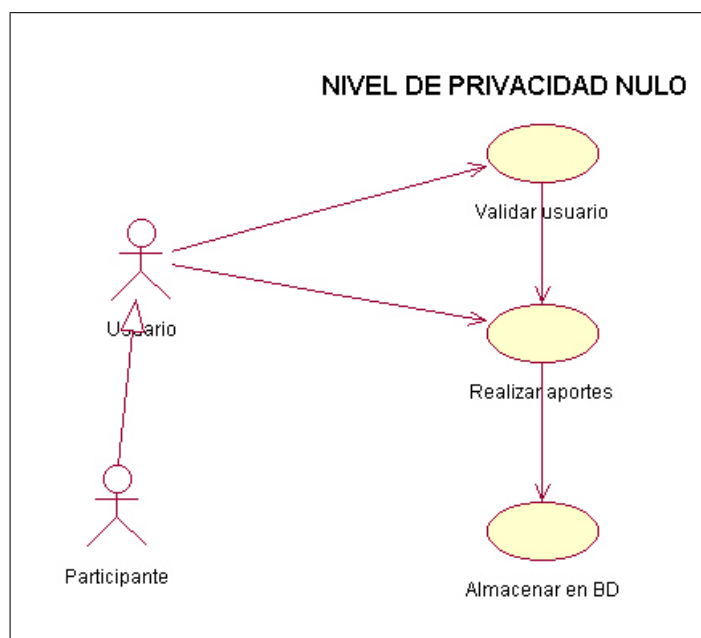


Figura 8.10: Aceptar todo.

CASO DE USO: Nivel "Aceptar todo".

ACTORES: Usuario participante.

TIPO: Primario.

DESCRIPCION: En este nivel no se utiliza ninguna estrategia de privacidad. El usuario ingresa al sistema y realiza aportes solamente.

8.2.2. Nivel de privacidad Básico.

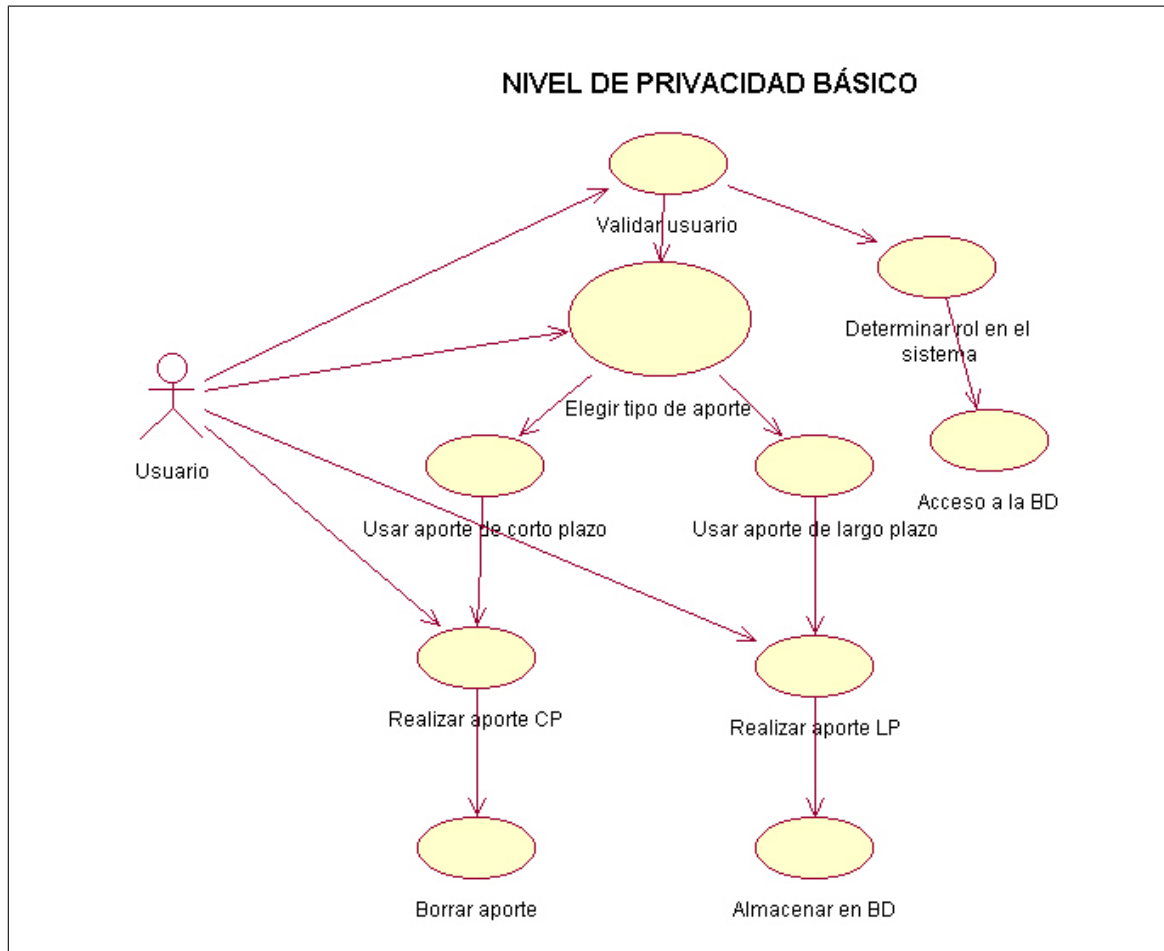


Figura 8.11: Nivel de privacidad Básico.

CASO DE USO: Nivel básico.

ACTORES: Usuario participante.

TIPO: Primario.

DESCRIPCION: Luego de ingresar al sistema, el usuario es identificado según su rol en la pre-reunión y las restricciones que éste tenga. Además el usuario marca los aportes como de corto o largo plazo.

8.2.3. Nivel de privacidad Medio.

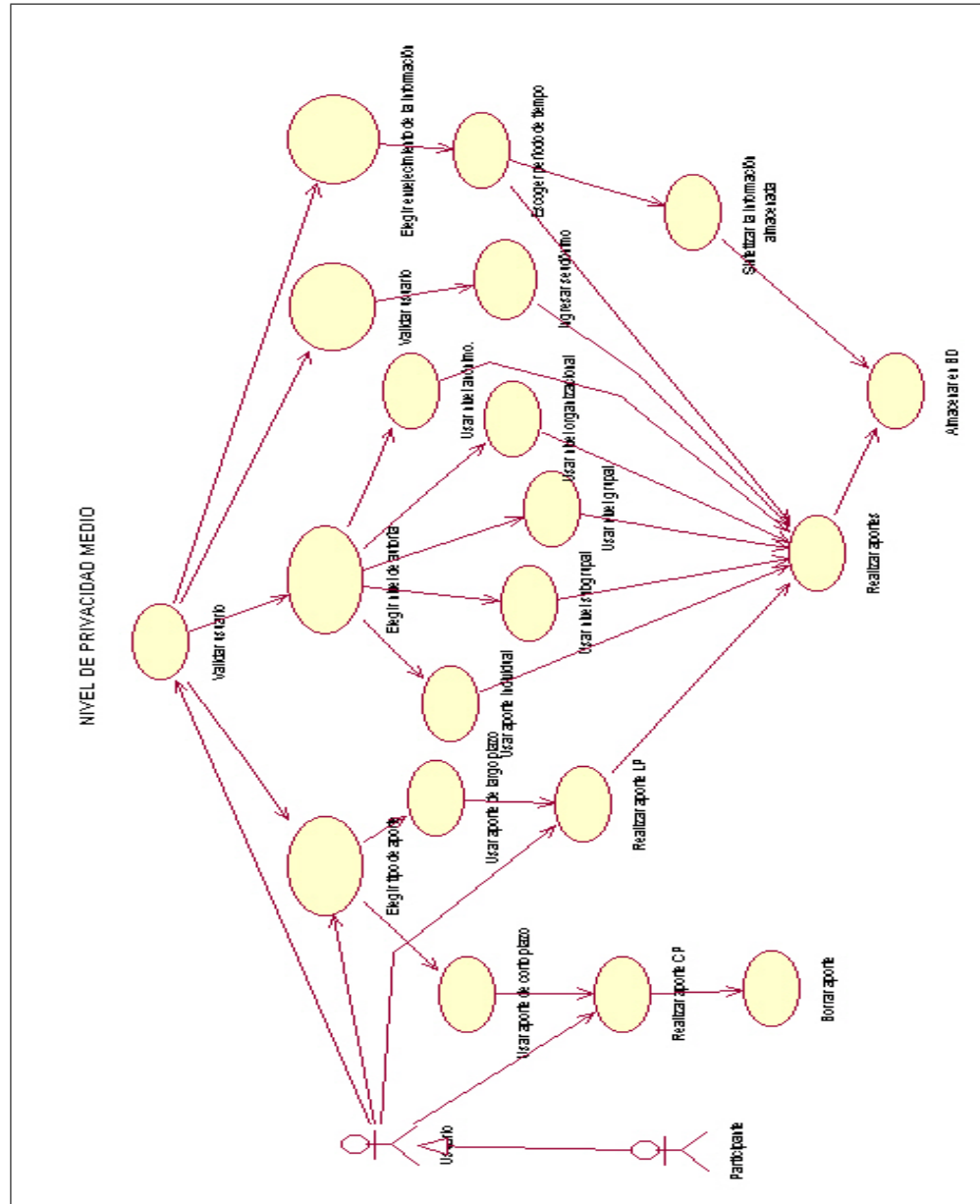


Figura 8.12: Nivel de privacidad Medio.

CASO DE USO: Nivel Medio.

ACTORES: Usuario participante.

TIPO: Primario.

DESCRIPCION: El usuario al ingresar al sistema debe ingresar el seudónimo con el cual será conocido. Luego, al realizar los aportes correspondientes deberá marcarlos como de corto o largo plazo, su nivel de autoría y el periodo de tiempo de envejecimiento de la información ingresada.

8.2.4. Nivel de privacidad Alto.

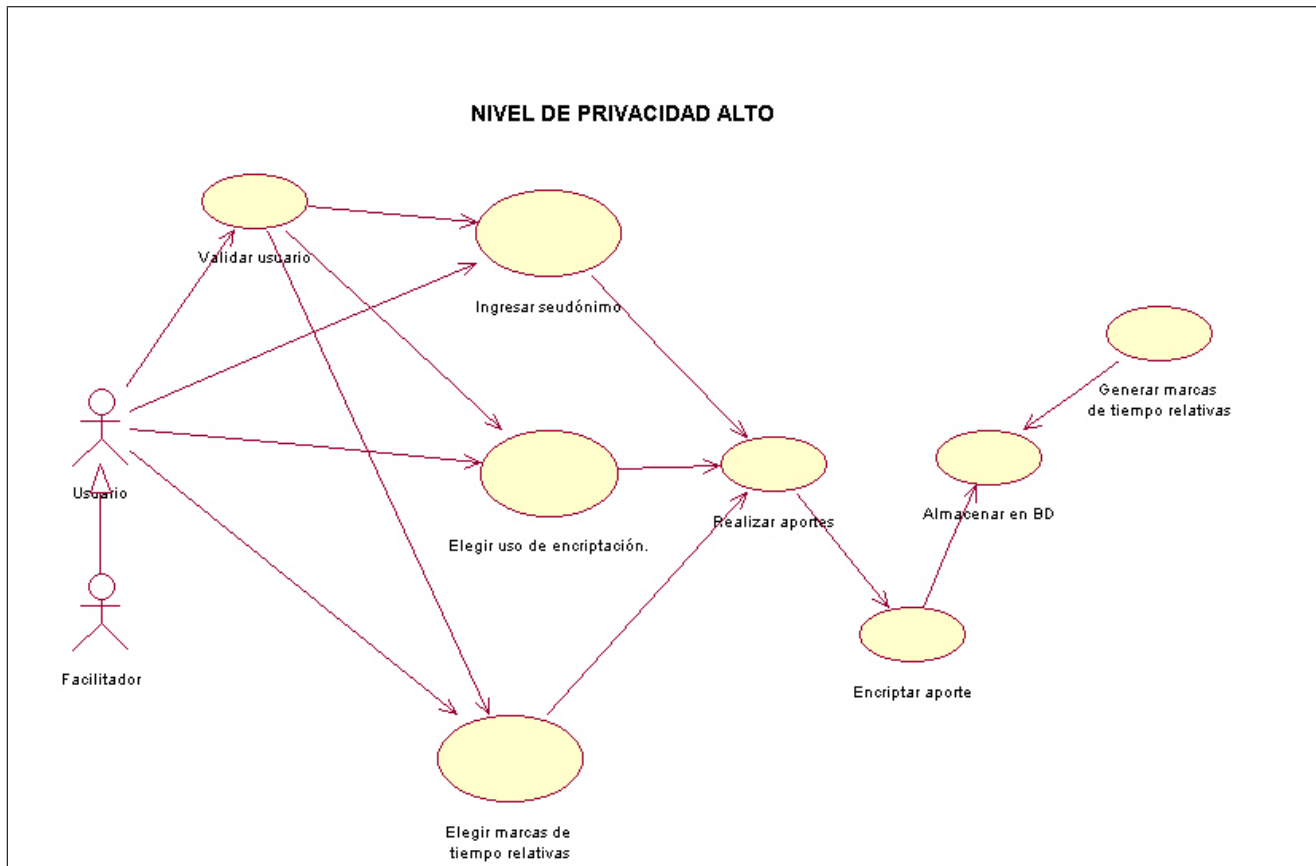


Figura 8.13: Nivel de privacidad alto

CASO DE USO: Nivel Alto.

ACTORES: Usuario participante.

TIPO: Primario.

DESCRIPCION: Al ingresar al sistema el usuario ingresa el seudónimo, por el cual será conocido. Luego al hacer aportes, éstos quedarán encriptados en el sistema y, además, la fecha de creación de los aportes puede ser configurada como difusa.

8.2.5. Nivel de privacidad "Restringir todo".

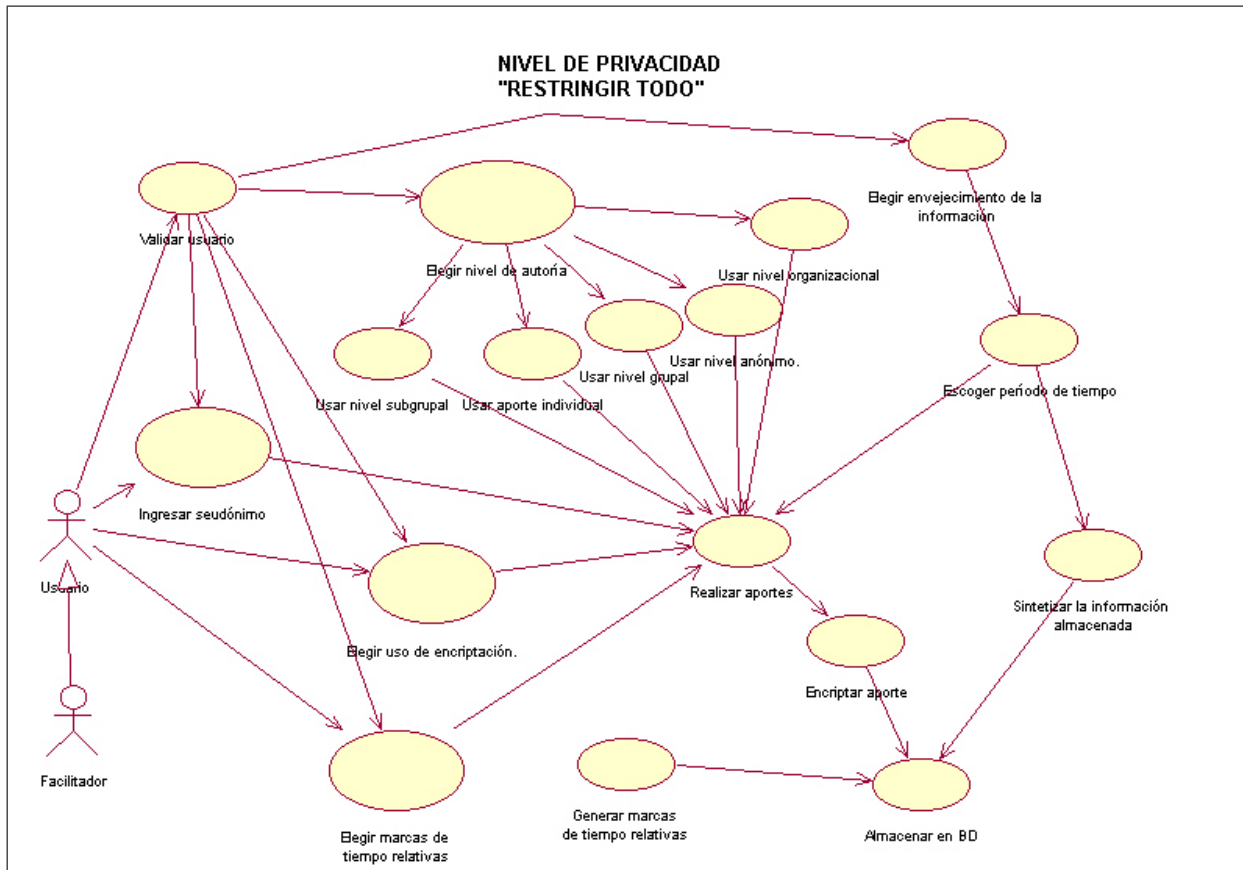


Figura 8.14: Restringir todo.

CASO DE USO: Nivel "Restringir todo".

ACTORES: Usuario participante.

TIPO: Primario.

DESCRIPCION: En este nivel de privacidad se utilizan el mayor número de estrategias, por consiguiente, el usuario debe configurarlas por separado. El nivel de precisión de la autoría es configurado para cada aporte, deberá ingresar un seudónimo, la información ingresada será encriptada con la clave que el mismo usuario proporciona. Por otra parte, el usuario puede definir el periodo de tiempo para la estrategia de envejecimiento de la información, como también, la fecha de creación del aporte en forma relativa a la pre-reunión.

8.3. Interfaz del sistema.

8.3.1. Interfaz principal.



Figura 8.15: Interfaz principal del sistema.

La interfaz principal del sistema presenta las opciones que puede tomar el usuario, para elegir el nivel de privacidad del cual desea hacer uso. Luego de hacer la elección y enviar el requerimiento, el sistema desplegará la interfaz de configuración adecuada, para el nivel de privacidad escogido. (Ver figura 8.3.1)

8.3.2. Interfaz "Aceptar todo".

En este nivel de privacidad no procede tener una interfaz de configuración de las estrategias individuales, pues no existe ninguna definida.

8.3.3. Interfaz Nivel Básico.



Figura 8.16: Interfaz web de nivel de privacidad básico.

Para el nivel básico de privacidad están presentes las estrategias de registros de memoria de corto y largo plazo, como además el uso de perfiles de usuario, para el acceso posterior de la información.

8.3.4. Interfaz Nivel Medio.

PrivControl
(Nivel Medio)

Su aporte actual será marcado como:

☒ CORTO PLAZO
☐ LARGO PLAZO

El aporte se hará a nombre de:

Anónimo

Su seudónimo en el sistema es:

"Facilitador"

Período de tiempo de duración de la información:

☐ 15 días
☐ 1 mes
☐ 3 meses
☒ 6 meses

Figura 8.17: Interfaz web de nivel medio.

Para este nivel de privacidad, las estrategias individuales presentes son:

1. Registros de corto y largo plazo.

2. Niveles de precisión en la autoría.
3. Uso de seudónimos.
4. Envejecimiento de la información.

Para cada una de ellas se deben configurar los parámetros adecuados para su correcto funcionamiento. Como por ejemplo, en la estrategia N° 2, se debe especificar el nivel de precisión de la autoría. Por otro lado, en la estrategia de envejecimiento de la información, se debe elegir el período de tiempo antes de que se comience a modificar el contenido de la información almacenada. (Los valores son referenciales.)

8.3.5. Interfaz Nivel Alto.

Pagina nueva 1 - Microsoft Internet E...

Archivo Edición Ver Favoritos Herram >>

PrivControl

(Nivel alto)

Su seudónimo en el sistema es:

"Facilitador"

Ingrese la clave para encriptar la información ingresada al sistema:

Enviar

La función de marcas de tiempo relativas a la reunión, está:

☒ Activada

☐ No activada

List Mi PC

Figura 8.18: Nivel alto de privacidad.

En este nivel de privacidad, el uso de seudónimos, más el uso de encriptación y el marcado del tiempo de creación de los aportes, según un tiempo relativo al inicio de la reunión, hacen que la seguridad que entrega el sistema al usuario sea alto. Los parámetros que se deben ingresar son dos: una clave secreta, con la cual encriptar la información ingresada y el seudónimo con que será conocido el usuario, al momento de la reunión. Además se da la opción de desactivar el uso de la tercera estrategia de marcas de tiempo relativas.

8.3.6. Interfaz "Restringir Todo"

The screenshot shows a web browser window with the title "D:\Memoria\Interfaces\restringir_todo.htm - Microso...". The browser's menu bar includes "Archivo", "Edición", "Ver", "Favoritos", "Herramientas", and "Ayuda". The main content area has a light blue background and is titled "PrivControl" with the subtitle "(Restringir Todo)".

The interface is divided into several sections:

- El aporte se hará a nombre de:** A dropdown menu showing "Anónimo".
- Su seudónimo en el sistema es:** The text "Facilitador".
- Período de tiempo de duración de la información:** A group of radio buttons with labels: "15 días" (selected), "1 mes", "3 meses", and "6 meses".
- La función de marcas de tiempo relativas a la reunión, está:** A group of radio buttons with labels: "Activada" (selected) and "No activada".
- Ingrese la clave para encriptar la información ingresada al sistema:** A text input field with a masked password "XXXXXXXXXX" and an "Enviar" button.

The bottom status bar shows "Listo" on the left and "Mi PC" on the right.

Figura 8.19: Interfaz de configuración de privacidad.

El más alto nivel de privacidad se encuentra en esta elección del usuario. Se acumulan las estrategias anteriores, dando ésto como resultado. Los parámetros ingresados ya fueron descritos anteriormente.

8.4. Discusión del modelo.

El modelo presentado en este trabajo funciona como una capa potenciada de estrategias de privacidad sobre el sistema de recuperación de la información, en un sistema de manejo de información (KMS).¹ (Ver figura 7.1).

El usuario es capaz de elegir de un conjunto de cinco niveles de privacidad ascendentes:

1. Nivel de privacidad nula: "Aceptar todo".
2. Nivel de privacidad baja o básica.
3. Nivel de privacidad media.
4. Nivel de privacidad alta.
5. Nivel de privacidad extrema: "Restringir todo".

Estos niveles fueron diseñados de tal manera de que sean capaces de entregar el nivel de privacidad que prometen. Para cada uno se consideró el nivel individual de privacidad que entregaban. Fueron agrupados por niveles y aplicados consecuentemente en subconjuntos, con la finalidad de aprovechar las fortalezas que podían entregar. Teniendo en cuenta esto, lo que sucede con el nivel de apoyo a la colaboración de cada estrategias es interesante. Cuando se encuentran en conjunto con las demás que componen el nivel de privacidad definido, mientras la privacidad aumenta, el nivel de colaboración disminuye.

La siguiente tabla muestra el fenómeno que sucede con la colaboración.

Privacidad	Niveles de Colaboración	Estrategias usadas.
Nula	Alto	—
Baja	Alto–Alto	2, 6
Media	Alto–Medio–Bajo–Alto	2, 3, 4, 8
Alta	Bajo–Bajo–Bajo	4, 5, 7
Muy alta	Medio–Bajo–Bajo–Bajo–Alto	3, 4, 5, 7, 8

¹Knowledge Management System.

Este fenómeno se puede deber a que mientras más alto es el nivel de confidencialidad que desee el usuario, mayor son el número de restricciones que se le entregan al sistema. Por consiguiente, el apoyo a la colaboración sufre las consecuencias de estas restricciones, disminuyendo paulatinamente el nivel al mismo que aumenta la privacidad. En un gráfico privacidad versus colaboración, de cada estrategia individual de privacidad aparece el mismo suceso demostrado.

Se nota del gráfico 8.20 que el sector con mayor índice de colaboración y privacidad, no existe. Esto es, si se desea aumentar el nivel de privacidad, se debe sacrificar el nivel de colaboración, y viceversa. Queda como trabajo posterior, encontrar estrategias nuevas de privacidad que estén situados en el área de mayor colaboración, como también de nivel de privacidad.

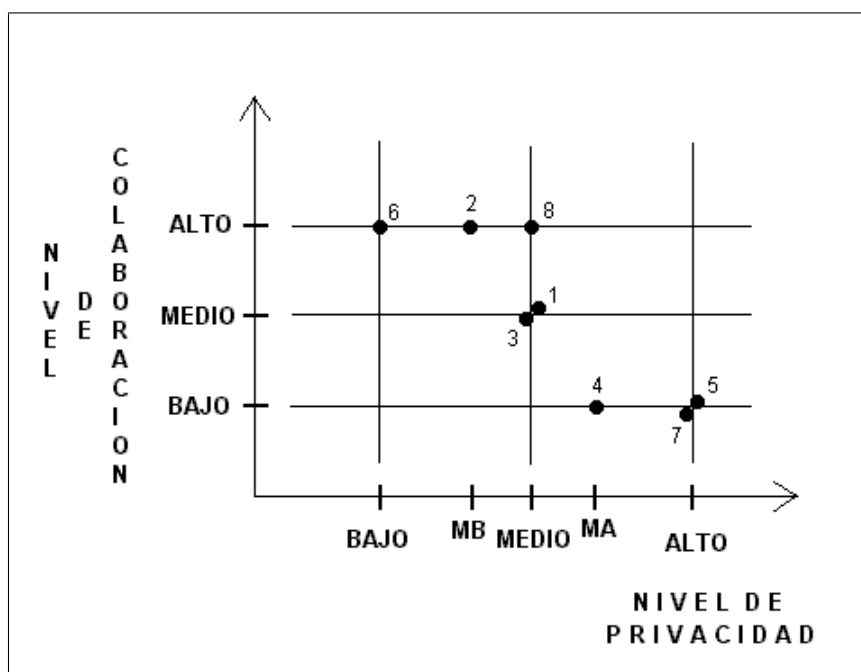


Figura 8.20: Gráfico: nivel de privacidad versus nivel de colaboración.

Por otra parte, el control que posee el usuario sobre los niveles de privacidad está, a simple vista, predefinido. Si se revisan las interfaces del sistema, en cada uno de los niveles, éstas le dan la libertad de desactivar las políticas de privacidad presentes en tal nivel. Esto denota que la representación extensional de la interfaz PrivControl, es decir, le permite al usuario marcar todas las contribuciones como el nivel le permite o subutilizarlo, con el fin de darle más control sobre sus propias políticas de privacidad al usuario.

Capítulo 9

Conclusiones.

Luego de elegir los casos de estudio de sistemas colaborativos, además de detallar los problemas que conllevan las amenazas que poseen los sistemas informáticos en materia de privacidad; lo que dicen las leyes de países desarrollados sobre este tópico, la legislación que hace 4 años ya rige en Chile sobre privacidad de la información de los individuos, se crea una base en la cual proponer una solución al problemas del manejo confidencial de la información, que considera unas soluciones ya descritas en trabajos anteriores, como otras nuevas propuestas por el autor de esta memoria, para fortalecer las potencialidades y sinergia de las tales soluciones.

El caso revisado de sistema de memoria organizacional, como es el basado en QuestMap y las interfaces de privacidad, para un sistema simple de colaboración entre usuarios, COLLABCLIO, dieron las pistas de cómo engendrar una solución a este problema de privacidad.

La premisa inicial de que el autor de las contribuciones debe tener el **control absoluto del acceso de la información** se ha tratado de cumplir. Al permitirle al usuario elegir el nivel de privacidad con el cual desea enfrentar un sistema colaborativo, que le permita satisfacer sus necesidades de confidencialidad de su información personal, el sistema hace lo necesario para que se cumpla esta premisa.

En lo propuesto por Pino y Guerrero en su trabajo "*Understanding Organizational Memory*"[7], exactamente en el modelo de sistema de manejo de información, la capa superior del modelo de 5 componentes (ver figura 7.1) es la privacidad, la propuesta de este trabajo es apoyar las potencialidades de estrategias individuales sobre privacidad. De esta manera, la última componente crece y llega a ser uno de los más importantes al momento de diseñar un nuevo sistema de memoria organizacional. En general, las soluciones de diseño de los otros cuatro componentes no presentan mayores problemas, pues son los subsistemas más desarrollados e investigados en el área de Trabajo Colaborativo Apoyado por Computador (CSCW).¹ Por lo que se dio mayor hincapié en el componente que poseía menor desarrollo, y por lo tanto, se eligió como tema de esta memoria.

Un sistema actual de manejo de información y de apoyo a pre-reuniones es PRIME. Éste no posee estrategias claras sobre privacidad, pues es posible, por ejemplo, acceder a toda la información registrada en el sistema, lo que puede dar lugar a situaciones complicadas, como el despedido de un empleado por algún comentario hecho anteriormente en alguna sesión de trabajo. Esto sucede cuando los aportes son tomados fuera de contexto y por consiguiente, con un significado erróneo.[13] PrivControl puede llegar a ser la interfaz que solucione este tipo de problemas, obviamente definiendo el balance preciso entre privacidad y colaboración. Para ésto se debe educar al usuario sobre la importancia que tiene un nivel adecuado de privacidad, como, a su vez, una consiguiente calidad en la colaboración entre los usuarios.

Claramente el problema de la privacidad de la información no es un tema fácil de manipular, se deben tomar en cuenta una serie de factores sociales y técnicos, para implantar un sistema que contenga las características deseables de privacidad y apoyo a la colaboración, al mismo tiempo. Se deben enfrentar distintos tipos de usuarios, organizaciones y códigos sociales inherentes a las mismas.

¹Computer Supported Collaborative Work.

Bibliografía

- [1] Ackerman, Mark S., Halverson, Christine **"Organizational Memory: Processes, Boundary Objects, and Trajectories"**.
<http://computer.org/proceedings/hicss/0001/00011/00011067.PDF>.
- [2] Ackerman, Mark S. y Cranor, Lorrie. **"Privacy Critics: UI Components to Safeguard User's Privacy"**.
<http://www.eecs.umich.edu/ackerm/pub/99b27/privacy-critics.pdf>.
- [3] Bellasai, G., Borges, M., Fuller, D.A., Pino, J. A. y Salgado, A. C. **"An IBIS-based model to support group discussions"**, volumen *"Information Systems and Technology in the International Office of the Future"* de Glasson, B., Vogel, D., Bots, P., Nunamaker, J.F. (Eds.), páginas 49–62. Chapman and Hall, London, 1996.
- [4] Conklin, E. Jeffrey. **"Capturing Organizational Memory"**.
<http://www.touchstone.com/tr/wp/CapOrgMem.html>.
- [5] Conklin, E. Jeffrey. **"Designing Organizational Memory: Preserving Intellectual Assets in Knowledge Economy"**.
<http://www.touchstone.com/tr/wp/DOM.html>.
- [6] Conklin, E. Jeffrey. **"La memoria organizacional"**.
<http://www.cibernetica.org.mx/A0020.html> (1/2)
<http://www.cibernetica.org.mx/A0021.html> (2/2).
- [7] Guerrero, Luis A., Pino, José A.. **"Understanding Organizational Memory"**. *Proceedings Of The XXI International Conference of the Chilean Computer Science Society*, páginas 124–132, 7-9 Nov. 2001, Punta Arenas, Chile. IEEE Computer Society Press, Los Alamitos, CA, USA.
- [8] Kovalainen, Mikko, Robinson, Mike y Auramäki, Esa. **"Diaries at Work"**.
- [9] Landry, John R.. **"Forgetful or Bad Memory?"**. *Proceedings Of The 32nd Hawaii International Conference on System Sciences*, 1999, Hawaii, USA.
<http://computer.org/proceedings/hicss/0001/00011/00011069.PDF>.

- [10] Lau, Tessa, Etzioni, Oren, Weld, Daniel S.. **"Privacy Interfaces for Information Management"**.
<http://citeseer.nj.nec.com/lau99privacy.html>.
- [11] Morrison, Jolie, Olfman, Lorne. **"Organizational Memory and Knowledge"**. *Proceedings Of The 32nd Hawaii International Conference on System Sciences*, 1999, Hawaii, USA.
<http://computer.org/proceedings/hicss/0001/00011/00011066.PDF>.
- [12] Romero, Natalia A., Pino, J.A., Guerrero, Luis A. **"Organizational Memories as Electronic Discussion By-products"**. *Proceedings Of The VIth International Workshop on Groupware (CRIWG '2000)*, páginas 11–18, Oct. 18-20 2000, Madeira, Portugal. IEEE Computer Society Press, Los Alamitos, CA, USA.
- [13] Moreno Beaupuits, J. M. C.. **"Awareness en Prime"**. Facultad de Ciencias Físicas y Matemáticas. Universidad de Chile, Julio 2003, Santiago, Chile. Memoria para optar al título de Ingeniero Civil en Computación.
- [14] Acepta.com – Autoridad certificadora. **"Criptografía y firma digital"**.
http://www.acepta.com/Doc/Firma_Digital.pdf.

Apéndice A

QuestMap TM.

QuestMap es una herramienta comercial para la captura de las justificaciones, creada por The SoftBicycle Company. Se enfoca en proveer soporte para registrar las decisiones conceptuales dentro de los procesos. QuestMap trata de modelar secuencias de procesos de pensamiento ofreciendo plantillas, que pueden usarse para estructurar ideas. Estas ideas proveen una manera y organización conveniente en la cual se registran las decisiones y la justificaciones correspondientes.

La figura (ver figura A.1) muestra un ejemplo del uso de QuestMap para capturar los procesos de decisión referente al marketing de un producto nuevo. QuestMap ofrece una serie de iconos y relaciones (las flechas codificadas en colores) para organizar ideas. Con estos iconos se pretende representar los conceptos y las flechas corresponden a las relaciones entre los conceptos. QuestMap también provee mapas jerárquicos que son conectados conjuntamente para habilitar las diferentes capas de captura de las ideas.

QuestMap no ofrece estructuras formales algunas, en las cuales organizar las ideas. En lugar de eso, ofrece elementos básicos que están supuestos a representar componentes fundamentales de procesos conceptuales de decisión. El usuario está obligado a estructurar estos elementos de una forma significativa y efectiva. Adicionalmente, QuestMap requiere que un usuario ingrese toda la información manualmente. En este aspecto, es similar a los minutos que se utiliza en una reunión, en la que se requiere una persona designada para alimentar de información a los asistentes, ya sea que esto ocurra durante la reunión o después de ella.

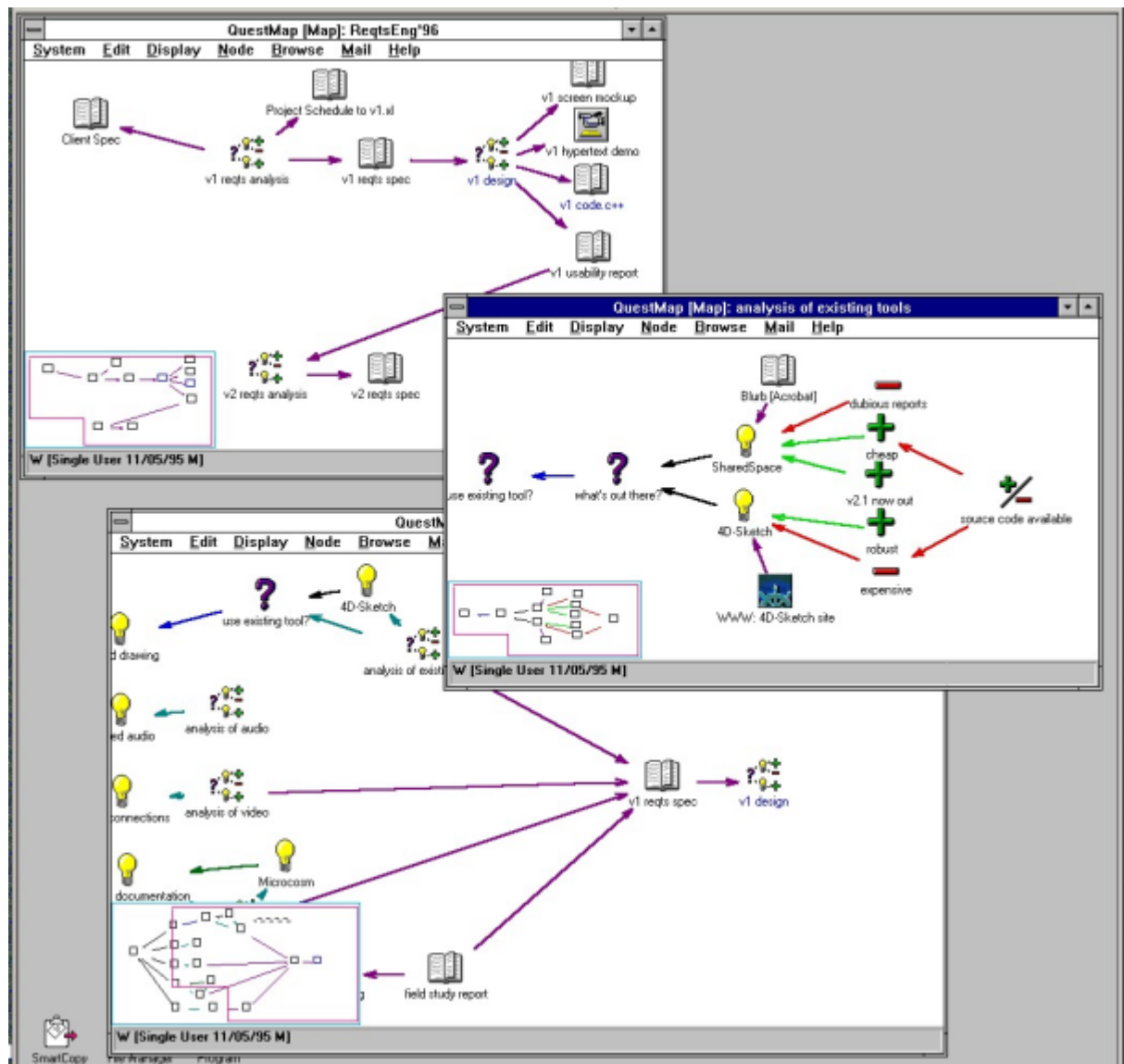


Figura A.1: Interfaz principal de QuestMap TM.