

# Estudio del Control de Acceso en Sistemas Colaborativos

Miguel Sánchez

Dept. de Lenguajes Y Sistemas  
Informáticos  
ETS Ingeniería Informática  
Univ. de Granada  
18071 Granada  
[miguesr@ugr.es](mailto:miguesr@ugr.es)

Beatriz Jiménez

Dept. de Lenguajes Y Sistemas  
Informáticos  
ETS Ingeniería Informática  
Univ. de Granada  
18071 Granada  
[beajv@ugr.es](mailto:beajv@ugr.es)

Francisco L. Gutiérrez

Dept. de Lenguajes Y Sistemas  
Informáticos  
ETS Ingeniería Informática  
Univ. de Granada  
18071 Granada  
[fgutierr@ugr.es](mailto:fgutierr@ugr.es)

## Resumen

Una de las principales características de los sistemas empresariales actuales es la existencia de procesos donde usuarios/subsistema colaboran entre sí para llevar a cabo un objetivo común, siendo la información que comparten, uno de los elementos más importantes y difícil de gestionar. En este artículo nos vamos a centrar en uno de los aspectos de esa gestión, en concreto la seguridad y dentro de ella una de sus principales dimensiones: "el control de acceso". Hemos realizado un estudio de los modelos más importantes que aparecen en la literatura para el control de acceso y presentamos un modelo de organización para representar los aspectos del control de accesos en sistemas empresariales.

## 1. Introducción

El aspecto de la seguridad es un elemento muy importante en la gestión de los procesos de negocio de una organización. La seguridad de la información persigue proteger la información de posibles accesos y modificaciones no autorizadas.

Los principales objetivos de la seguridad de la información se pueden resumir en [4,5]:

- **Confidencialidad:** Describe el estado en el cual la información está protegida de revelaciones no autorizadas, por ejemplo una falta de confidencialidad ocurre cuando el contenido de una comunicación o de un fichero es revelado a personas no autorizadas.
- **Integridad:** Significa que la información no ha sido alterada o destruida, por una acción accidental o por un intento malicioso.
- **Disponibilidad:** Referencia al hecho de que una persona autorizada pueda acceder a la información en un apropiado periodo de tiempo. Las razones de la pérdida de disponibilidad pueden ser ataques o inestabilidades del sistema

- **Responsabilidad:** Asegurar que las acciones realizadas en el sistema por una entidad se puedan asociar únicamente a esa entidad, que será responsable de sus acciones. Es decir que una entidad no pueda negar su implicación en una acción que realice en el sistema.

Para llevar a cabo los objetivos de la seguridad, descritos anteriormente, es necesario definir en la etapa de diseño de los procesos de negocio, un conjunto de mecanismos de seguridad. Algunos de los principales mecanismos de protección se resumen a continuación:

- **Autenticación:** Mecanismo para asegurar la identidad de una entidad (usuarios, subsistemas, etc.). Consta de dos procesos: identificación (obtiene un identificador de la entidad) y verificación (corroboración del vínculo unívoco entre el identificador y la entidad)
- **Control de acceso:** Garantizar la protección de los recursos del sistema de accesos no autorizados; Proceso por el cual los accesos a los recursos del sistema, así como, a la información en el flujo de trabajo son regulados según unas políticas de seguridad y permitiendo el acceso solamente a entidades autorizadas.
- **Cifrado de los datos:** Procesos para el tratamiento de la información que impide que nadie excepto el destinatario de la información pueda leerla. Asegurando, por lo tanto, la confidencialidad.
- **Funciones resumen:** se encargan de garantizar la integridad de los datos.
- **Firma digital:** Asegurar la responsabilidad sobre una secuencia de acciones determinada.
- **Registro de auditoría:** Proveer medidas de auditoría.

Tradicionalmente los aspectos de la seguridad no se han tenido en cuenta hasta las últimas fases del desarrollo software. Sin embargo, es esencial considerarlos desde las primeras fases si queremos desarrollar sistemas fiables y utilizables. Por lo

tanto los requerimientos de seguridad deben ser integrados dentro de todas las fases de desarrollo de los sistemas de negocio [2,3, 5].

En este artículo, prestaremos especial atención a la disponibilidad. Nosotros pensamos que la estructura de una organización es un elemento clave en la gestión de los procesos de negocio de un sistema empresarial y aun más importante en los procesos de carácter colaborativo donde la información debe ser compartida por un gran número de usuarios. Los mecanismos de control de acceso son especialmente indicados para llevar a cabo los objetivos de la disponibilidad de la información. Además el control de acceso es un importante complemento para la caracterización de la interacción de los usuarios y/o los sistemas.

El resto del artículo se estructura de la siguiente manera. En la sección 2 se describen y analizan las características y ventajas de los principales modelos de control de acceso para aplicaciones. En la sección 3 presentamos un modelo de organización para representar organizaciones donde existen procesos de carácter colaborativo incluyendo los elementos necesarios para el control de acceso. Por último, en la sección 4 se presentan algunas conclusiones y planes de trabajo actuales y futuros.

## 2. Trabajos Relacionados

Diferentes modelos han sido propuestos en la literatura para la gestión del control de acceso en aplicaciones distribuidas. Tradicionalmente, los modelos de control de acceso han sido caracterizados mediante modelos DAC (Discretionary Access Control) y modelos MAC (Mandatory Access Control). Posteriormente modelos RBAC (Role-Based Access Control) o modelos TBAC (Task-based access control) han sido propuestos para gestionar los requerimientos de seguridad en un gran conjunto de aplicaciones. A continuación se resumen las características de estos modelos junto con sus limitaciones más importantes.

### 2.1. DAC – Control de Acceso Discrecional

El modelo de control de acceso discrecional (DAC, Discretionary Access Control), también llamado modelo de seguridad limitada, es un modelo no orientado al control del flujo de

información. Todos los sujetos y objetos en el sistema son controlados y se especifican reglas de autorización de acceso para cada sujeto y objeto. Los sujetos pueden ser usuarios, grupos o procesos.

Los modelos DAC están basados en la idea de que el propietario de un objeto, su autor, tiene el control sobre los permisos del objeto. Es decir, el autor es autorizado a permitir u otorgar permisos para este objeto a otros usuarios.

DAC admite la copia de datos desde un objeto a otro por usuarios autorizados de manera que un usuario puede permitir el acceso para copiar datos a otro usuario no autorizado. Este riesgo puede ser extendido a todo el sistema violando un conjunto de objetos de seguridad.

La principal ventaja de DAC es que el usuario se beneficia de la flexibilidad del modelo. Sin embargo es difícil para DAC garantizar las reglas de integridad como ‘least privilege’ o ‘separation of duty’ que son necesarias en los ambientes con procesos colaborativos. DAC es apropiado en ambientes donde la compartición de información es más importante que su protección.

Hay diferentes implementaciones del modelo DAC, la más importante es HRU ((Harrison, Ruzzo and Ullman) y ACM (Access Control Matrix)[7]

En ACM los permisos de acceso son almacenados en una matriz de accesos “A”. Los sujetos son representados por filas y los objetos por columnas.  $A[s,o]$  define permisos de acceso para un sujeto,  $s$ , sobre un objeto,  $a$ . Si dividimos la matriz por columnas, para cada objeto tendremos todos los modos de acceso para cada sujeto. En este caso, tendremos un modelo basado en “autoridad”. Si dividimos por filas, para cada sujeto obtendremos información acerca de que pueden hacer con cada objeto; tendremos en este caso un modelo basado en “capacidades”.

Hay diferentes modelos basados en ACM, Schematic Protection Model (SPM) [8], Typed Access Matrix (TAM) model [9] y Dynamically Typed Access Control (DTAC) model [13], donde la principal aportación es la inclusión del concepto de tipos de seguridad en ACM.

### 2.2. MAC – Control de Acceso Obligatorio

En el modelo de control de acceso obligatorio (MAC, Mandatory Access Control) todos los sujetos y objetos son clasificados basándose en

niveles predefinidos de seguridad que son usados en el proceso de obtención de los permisos de acceso. Para describir estos niveles de seguridad todos los sujetos y objetos son marcados con etiquetas de seguridad que siguen el modelo de clasificación de la información militar (desde “desclasificado” hasta “alto secreto”), formando lo que se conoce como política de seguridad multinivel. Por este motivo se define MAC como un modelo “multinivel”

Este modelo puede ser implementado usando mecanismos de seguridad multinivel que usan reglas “no read-up” y “no write-down” también conocidas como restricciones Bell-Lapadula [1]. Estas reglas son diseñadas para asegurar que la información no fluya desde un nivel alto de sensibilidad a un nivel mas bajo de sensibilidad. La regla “no read-up”, establece que los usuarios tienen la capacidad de acceder a cualquier fragmento de información que se encuentre en o por debajo de su nivel de seguridad. Por ejemplo, si un usuario tiene como nivel asignado “secreto”, este podrá acceder al nivel “básico, medio y secreto”, pero no podrá acceder al nivel “ultra secreto”. La regla “no write-down”, declara que un sujeto con un nivel de seguridad dado no debe escribir en ningún objeto etiquetado con un nivel mas bajo de seguridad. Por ejemplo, si un usuario tiene como nivel asignado “secreto”, este podrá acceder a escribir cosas en el nivel “secreto” o “ultra secreto”.

Un importante objetivo del modelo MAC es controlar el flujo de información en orden a asegurar su confidencialidad y su integridad, objetivo no alcanzado por los modelos DAC.

A diferencia de DAC, los modelos MAC proporcionan mecanismos más sólidos para la protección de datos, y tratan con requerimientos de seguridad más específicos, así como, los requerimientos derivados de las políticas de control de los flujos de información. Además, en los modelos MAC es el sistema quien protege los recursos u objetos, el administrador es el que impone las reglas de forma segura, a diferencia del DAC en el cual el dueño es quien protege los recursos Sin embargo, asegurar las políticas MAC es a menudo una tarea difícil, particularmente en procesos colaborativos, ya que no proporcionan soluciones factibles dado que les falta suficiente flexibilidad [10]

### 2.3. RBAC – Control de Acceso Basado en Rol

El principal objetivo del modelo de control de acceso basado en rol (RBAC, Role Based Access Control) es prevenir que los usuarios tengan libre acceso a la información de la organización. [11]. El modelo introduce el concepto de rol y asocia a los usuarios con los roles por los que va pasando durante la vida del sistema. Los permisos de acceso están asociados a los roles. El rol es un concepto típico usado en empresas para ordenar y estructurar sus actividades organizativas. RBAC permite modelar la seguridad desde de una perspectiva empresarial puesto que podemos conectar los requerimientos de seguridad con los roles y las responsabilidades existentes en la organización.

RBAC está basado en la definición de un conjunto de elementos y de relaciones entre ellos (figura 1). A nivel general describe un grupo de usuarios que pueden estar actuando bajo un conjunto de roles y realizando operaciones en las que utilizan un conjunto de objetos como recursos. En una organización, un rol puede ser definido como una función que describe la autoridad y responsabilidad dada a un usuario en un instante determinado.

Entre estos cuatro elementos se establecen relaciones del tipo:

- Relaciones entre usuario y roles, modelando los diferentes roles que puede adoptar un usuario.
- Conjunto de operaciones que se pueden realizar sobre cada uno de los objetos. A los elementos de esta relación se les denomina permisos.
- Relaciones entre los permisos y los roles. Modelamos cuándo un usuario, por estar en un rol determinado, tiene permiso para realizar una operación sobre un objeto.

El modelo RBAC incluye un conjunto de sesiones donde cada sesión es la relación entre un usuario y un subconjunto de roles que son activados en el momento de establecer dicha sesión. Cada sesión esta asociada con un único usuario. Mientras que un usuario puede tener una o más sesiones asociadas. Los permisos disponibles para un usuario son el conjunto de permisos asignados a los roles que están activados en todas las sesiones del usuario, sin tener en cuenta las sesiones establecidas por otros usuarios en el sistema.

RBAC añade la posibilidad de modelar una jerarquía de roles de forma que se puedan realizar generalizaciones y especializaciones en los

controles de acceso y se facilite la modelización de la seguridad en sistemas complejos.

Otro aspecto importante en el modelo RBAC es la posibilidad de especificar restricciones sobre la relación usuario/rol y sobre la activación de un conjunto de roles de usuario. Estas restricciones son un fuerte mecanismo para establecer políticas organizacionales de alto nivel. Las restricciones pueden ser de dos tipos: estáticas o dinámicas. Las restricciones estáticas nos permiten solucionar conflictos de intereses y reglas de cardinalidad de roles desde una perspectiva de política de seguridad. La asociación de un usuario con un rol puede estar sujeta de las siguientes restricciones:

- Un usuario es autorizado para un rol solo si el rol no es mutuamente excluyente con cualquier rol autorizado del usuario (Static Separation of Duty, SSD).
- El número de usuarios autorizados para un rol no puede exceder la cardinalidad del rol (Role Cardinality)

Por otro lado, las restricciones dinámicas (Dynamic Separation of Duty, DSD) al igual que las SSD, limitan los permisos que son disponibles para un usuario. Sin embargo DSD difieren de las SSD por el contexto en el cual estas limitaciones son impuestas. Las DSD limitan la disponibilidad de los permisos aplicando las restricciones sobre los roles que pueden ser activados durante una sesión de usuario. En otras palabras, un usuario puede ser activado para sólo uno de los dos roles distintos que le son asignados, mientras que su sesión de usuario siga activa.

El control de acceso basado en roles permite expresar de forma sencilla y natural la política de accesos a los recursos de una organización compleja. Al usar este modelo como representación de la seguridad en un sistema colaborativo estamos integrando los aspectos de seguridad con los funcionales, lo que nos va a dar mucha mas potencia.

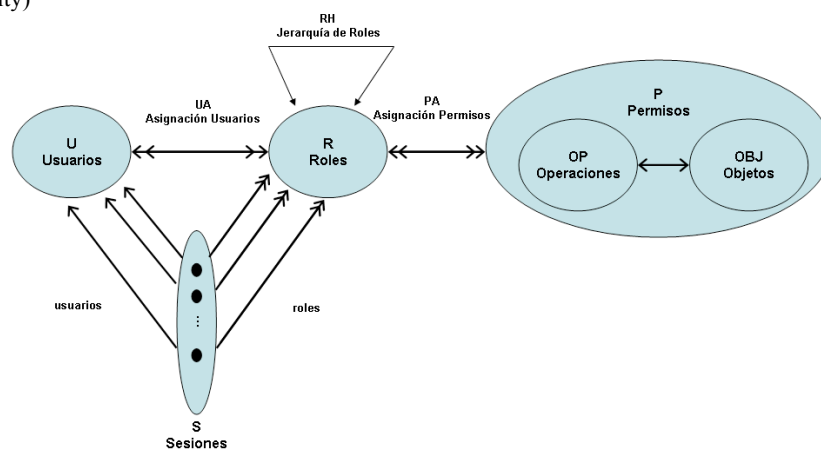


Figura 1. Modelo RBAC

Sin embargo pensamos que RBAC presenta una serie de carencias para el control de acceso en procesos de naturaleza colaborativa:

- En RBAC la naturaleza de los roles puede ser denominada estática, ya que carecen de flexibilidad y sensibilidad para el entorno en el cual son usados.
- RBAC soporta la noción de roles activos para un usuario con el concepto sesión, obteniendo a partir de estos roles activos el conjunto de permisos disponibles para un usuario, pero no

tiene en consideración las sesiones establecidas por otros usuarios en el sistema, es decir que el modelo no engloba todo el contexto asociado con el sistema. Por ejemplo, en un entorno educativo, RBAC no permite dar temporalmente permisos exclusivos del rol Director al rol Subdirector como consecuencia de la ausencia en el sistema de un usuario ejerciendo el rol Director.

- No es capaz de especificar un control de grano fino sobre usuarios individuales en ciertos

roles y sobre instancias de objetos individuales. Por ejemplo, en el ambiente de un hospital donde se crea un grupo de trabajadores sanitarios para dar asistencia médica a un paciente en concreto, en este caso sólo los miembros de este grupo podrán tener acceso al expediente del paciente, además los miembros del grupo que ejerzan el rol Celador no tendrán acceso a las pruebas médicas del paciente.

- En el escenario descrito anteriormente se observada la necesidad de establecer permisos comunes a grupos de usuario. Esto es conseguido en el modelo RBAC creando un rol específico y asignando de forma individual este rol a cada usuario perteneciente al grupo. La posibilidad de la existencia de un gran número de grupos de usuarios en los sistemas colaborativos y que la mayoría de estos grupos sean de carácter temporal, provoca que el sistema de control de acceso sea más difícil de modelar y de controlar

#### 2.4. TBAC – Acceso de Control Basado en Tareas

El control de acceso basado en tareas (TBAC, Task Based Access Control) permite controlar el acceso en entornos representados por workflow. El modelo TBAC extiende los tradicionales modelos de control basados en sujetos/objetos incluyendo aspectos que aportan información contextual basada en las actividades o tareas [12].

El control de acceso en TBAC es garantizado por medio de “Etapas de autorización”. Las “Etapas de autorización” son un concepto abstracto introducido por TBAC para modelar y manejar un sistema de permisos relacionados con el progreso de las tareas o actividades dentro del contexto de un workflow. Este concepto esta compuesto por una serie de elementos y atributos. A continuación se describen los elementos más representativos:

- Estado del Proceso: Indica como ha progresado la "etapa de autorización" en su ciclo de vida.
- Estado de Protección: Define todos los permisos que pueden ser activados por la “etapa de autorización” y que son mantenidos por la propia “etapa de autorización”. El valor del estado de protección, en un momento

dado, nos da una instantánea de los permisos activos en ese momento. El contenido del estado de protección puede cambiar en base al proceso de la tarea o a la pérdida de validez de los permisos. Esto último es debido a que con cada permiso se asocia una especificación de validez y de uso que nos detalla las condiciones que hay que cumplir para que los permisos asociados con una “etapa de autorización” se han validos y puedan ser usados. El estado de protección de cada “etapa de autorización” es único y disjuncto con respecto a los estados de protección de otras etapas.

- Conjunto de administradores: Contiene información relevante acerca del conjunto de administradores que potencialmente pueden conceder/invocar la “etapa de autorización” así como sus identidades de usuario y sus roles.
- Administrador Ejecutor: Identifica el miembro del conjunto de administradores que eventualmente invoca la “etapa de autorización”.

En la figura 2 se muestran los conceptos características y componentes que hacen a TBAC un modelo de seguridad activo, donde se observa:

- Incluye la noción de control de acceso basado en el uso. Controlando que un permiso activo otorgado por una autorización no implique una licencia ilimitada de accesos para ese permiso, establece atributos de validez, uso y expiración para evitar que la activación de un permiso por una etapa de autorización no implique una licencia ilimitada de accesos para ese permiso. Además estos atributos nos van a permitir monitorizar el uso de los permisos en tiempo de ejecución.
- Permite mantener por separado los estados de protección de cada “etapa de autorización”.
- Da soporte para el modelado de la autorización en las tareas y en workflow, así como, la monitorización y gestión del procesado de la autorización como del progreso de las tareas.
- Activación y desactivación de los permisos de los estados protección de forma dinámica en tiempo de ejecución.
- También da soporte para características de control de acceso basado en tipos.

El modelo TBAC presenta varias carencias cuando es aplicado en sistemas colaborativos, las principales carencias serian:

- TBAC reconoce la necesidad de la inclusión de la información de contexto para realizar el control de acceso, pero centrándose solo en la información contextual referente a las tareas, así como al proceso del workflow y al uso o

validez de los permisos. Siendo necesario en sistemas colaborativos considerar una información de contexto más amplia.

- La especificación de políticas de seguridad complejas y la gestión, delegación y revocación de los privilegios son muy primitivas.

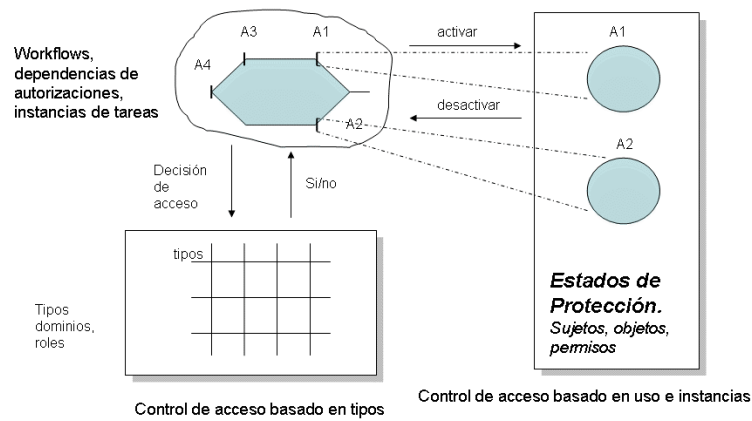


Figura 2. Modelo TBAC

### 3. Modelo de Organización

En trabajos previos [6] presentamos los principales requisitos que debían cumplir los modelos de control de acceso para sistemas colaborativos:

En la Tabla 1 se muestra un resumen del grado de cumplimiento dichos requisitos por parte de los modelos descritos en los apartados anteriores.

	DAC	MAC	RBAC	TBAC
Complejidad	No	No	Bajo	Bajo
Entendible	Si	Si	Si	Si
Facilidad de uso	Bajo	Bajo	Si	Si
Aplicabilidad	Bajo	Bajo	Si	Si
Grupos de Usuarios	Bajo	Bajo	Si	Si
Especificación de Políticas	Bajo	Bajo	Si	Si
Aplicación de las políticas	Bajo	Bajo	Si	Bajo
Control de Grano Fino	No	No	Bajo	Bajo
Dinámico	No	No	No	Si
Información Contextual	No	No	Bajo	Bajo

Tabla 1. Comparación entre modelos.

Como podemos observar en este resumen ninguno de los principales modelos estudiados cumplen o se adaptan en su totalidad a los requisitos para el control de acceso en procesos colaborativos.

RBAC sería un buen punto de partida para la definición de un nuevo modelo de control de acceso para sistemas colaborativos, ya que nos permite de una manera fácil y natural integrar los aspectos de la seguridad con los aspectos funcionales debido, entre otras cosas, a su definición en roles. Además permite expresar políticas de seguridad de alto nivel, utilizando mecanismos de restricciones estáticas y dinámicas nos permite solucionar conflictos de intereses y establecer políticas organizacionales de alto nivel.

Nuestra propuesta es la de integrar al modelo RBAC las aportaciones del modelo TBAC, es decir, incluir las características necesarias para que el modelo RBAC tenga en cuenta el proceso de workflow de la organización, así como, la información contextual asociada a las tareas o actividades que se lleven a cabo en la organización

Con el objetivo de introducir estos elementos de la seguridad desde las primeras fases del desarrollo, para obtener sistemas mas fiables y utilizables, hemos definido un modelo de organización conceptual (usando un diagrama de clases UML) para describir organizaciones donde existen procesos de carácter colaborativo[14]

En la Figura 3 se muestra los elementos del modelo de organización que nos va a permitir definir los requisitos de seguridad vinculados con el control de acceso.

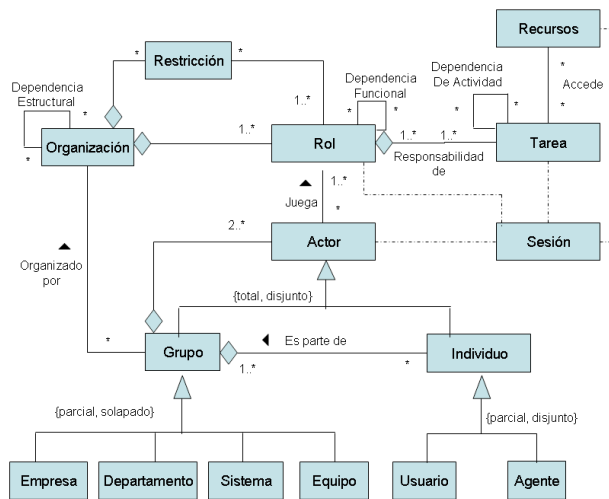


Figura 3. Modelo Organizacional

Este modelo conceptual define una organización como un conjunto de roles y dependencias funcionales entre ellos. Como consecuencia podemos modelar asociaciones de diferente naturaleza, por ejemplo la posibilidad de los usuarios de cambiar de un rol a otro, Además al aplicar restricciones a los roles dentro de la organización (cardinalidad de los roles, separación de obligaciones,...) junto con las dependencias funcionales nos permiten darle un carácter dinámico a la asignación de roles aportando sensibilidad y flexibilidad para el entorno en el cual son usados

El concepto de actor incluye tanto individuos (un usuario, un agente software, un robot, etc.) como a grupos. Al incluir los grupos en el concepto de actor podemos asignar capacidades comunes a grupos de usuarios. Un actor (organizacional o individual) juega al menos un rol en la organización. Jugar un rol implica que el actor es responsable para llevar a cabo actividades asociadas con ese rol. Implícitamente asumimos que un actor debe tener los permisos y capacidades requeridas para llevar a cabo las

actividades correspondientes y para usar los recursos asociados.

El modelo nos va a permitir conocer a través del concepto de sesión, los roles que están activos para un actor determinado, así como, el estado actual del proceso de workflow de la organización, que actor esta realizando una tarea, con que rol la esta llevando a cabo y que recurso esta utilizando, Toda esta información nos permitirá otorgar permisos de acceso teniendo en cuenta una amplia información contextual de la organización. Además con esta información podremos llevar a cabo mecanismos de auditoria y conocer cual ha sido el proceso de autorización realizado en la organización.

#### 4. Conclusión

En este trabajo hemos presentado la necesidad de tener en cuenta los requerimientos de seguridad en todas las fases del desarrollo de un sistema, si nosotros queremos garantizar un sistema usable y fiable. Hemos prestado especial atención a los

requerimientos de control de acceso, considerándolos como elementos base para obtener un alto grado de disponibilidad de la información y de los recursos en un sistema organizacional.

Hemos presentado un estudio sobre algunos de los modelos de control de accesos más relevantes (DAC, MAC, RBAC y TBAC). Describiendo las características más importantes de cada uno, así como las deficiencias que presentan para definir el control de acceso para procesos de negocio con carácter colaborativo.

Por último hemos presentado un modelo de organización que usamos para modelar el control de acceso en sistemas colaborativos.

En la actualidad estamos trabajando en la propuesta de una arquitectura completa para sistemas colaborativos basada en Servicios Web donde se integraran los servicios necesarios para llevar a cabo el control de acceso basado en modelos.

En el caso concreto del control de acceso pensamos que es muy interesante poder aplicar patrones conceptuales durante su modelado de forma que podamos definir políticas de control de acceso generales que puedan ser aplicadas en cualquier sistema. Esto reduce el esfuerzo de modelización y permite generar soluciones de diseño más optimizadas, estamos trabajando en la definición de patrones de organización [6] y en su extensión para modelar dichas políticas.

El modelo de organización presentado esta siendo extendido para incluir nuevos elementos que nos permitan describir el resto de requisitos de seguridad: confidencialidad, integridad y responsabilidad.

**Agradecimientos.** Este trabajo esta financiado por la Comisión Interministerial para la Ciencia y la Tecnología (CICYT) proyecto AMENITIES - TIN2004-08000-C03-02.

## Referencias

- [1] Bell DE, LaPadula LJ (1974) Secure Computer Systems: Mathematical Foundations and Models. Mitre Report M74-244, Mitre Corporation, Bedford, Massachusetts
- [2] Firesmith DG (2003) Engineering Security Requirements. *J Object Technology* 2: 53-68
- [3] Firesmith DG (2004) Specifying Reusable Security Requirements. *J Object Technology* 3: 61-75
- [4] Gerber M, von Solms R, Overbeek P (2001) Formalizing information security requirements. *J Information Management & Computer Security* 9: 32-37
- [5] Gutiérrez C, Fernández-Medina E, Piattini M (2004) A Survey of Web Services Security. *Computational Science and Its Applications - ICCSA 2004 vol 3043/2004 pp 968-977*
- [6] Gutiérrez FL, Isla JL, Paderewski P, Sánchez M, Jiménez B (2007) An architecture for access control management in collaborative enterprise systems based on organization models. *J Sci Comput Program* 66: 44-59
- [7] Harrison MH, Ruzzo WL, and Ullman JD (1976) Protection in operating systems. *Commun ACM* 19: 461-471
- [8] Sandhu RS (1988) The schematic protection model: its definition and analysis for acyclic attenuating schemes. *J ACM* 35: 404-432
- [9] Sandhu RS (1992) The typed access matrix model. In: *Proceedings of the 1992 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Washington, DC, pp 122-136
- [10] Sandhu RS (1993) Lattice-based access control models. *IEEE Computer* 26:9-19
- [11] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (2006) Role-based access control models. *IEEE Computer* 29: 38-47
- [12] Thomas RK, Sandhu RS (1997) Task-based Authorization Controls(TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Security XI: Status and Prospects*, pp 166-181
- [13] Tidswell J, Potter J (1998) A Dynamically Typed Access Control Model. In: *Proceedings of the Third Australasian Conference on information Security and Privacy C. Boyd and E. Dawson (eds), Lecture Notes In Computer Science, vol 1438, Springer-Verlag, London, pp 308-319*
- [14] Van Welie M, Van der Veer GC (1998) An ontology for task world models. In: *Design, Specification and Verification of Interactive System'98, Springer Computer Science*