White Paper MABAC

(Multi Level Attribute Based Access Control)

by Gustavo Giorgetti & Claudio Vaucheret. (marzo 2008)

Evolución de los Métodos de Autorización

MAC → DAC → RBAC → ABAC → MABAC

Desde los sistemas locales con pocos usuarios a los sistemas basados en Internet donde la cantidad de usuarios crecen exponencialmente y las autorizaciones se complejizan, los modelos de autorización de usuarios han evolucionado buscando facilitar las actividades de autorización.

Se desarrolla a continuación una mención de las características de cada uno de estos modelos en uso hasta llegar al MABAC (Multi Level Attribute Based Access Control) introducido por PECAS como una innovación necesaria para poder implementar el modelo de INTEGRABILIDAD en infraestructuras de gobierno electrónico.

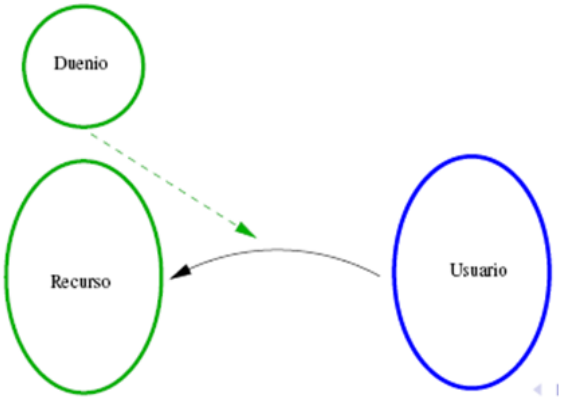
Los tipos de Control de acceso son:

Mandatory Access Control (MAC)

El administrador define quien está autorizado a operar un recurso, es un modelo Centralizado, rígido y no integrable.

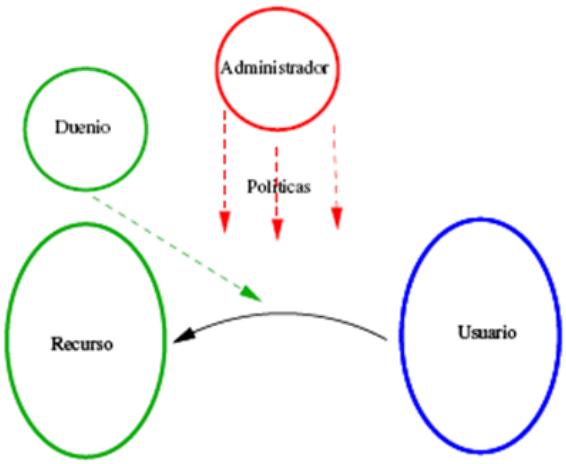
Discretionary Access Control (DAC)

El "dueño" de cada recurso autoriza a operar a otros.
Ej. Sistema Unix. Distribuido, flexible.



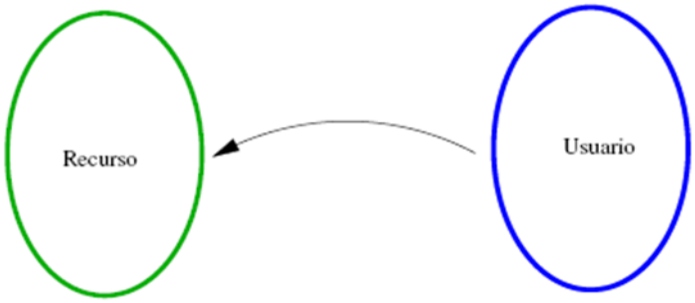
Separación de Deberes SSD/DSD

Se mantiene distribuido, pero existen políticas que previenen a un usuario de actividades incompatibles. Permite reglas por Defecto.



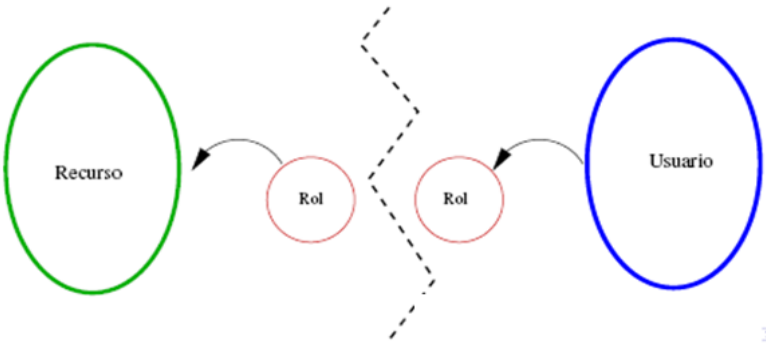
Identity Based Access Control (IBAC)

Los permisos se asocian a un usuario en particular



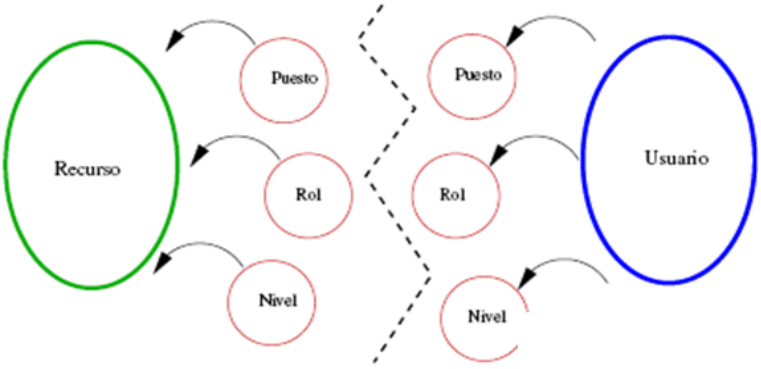
Role Based Access Control (RBAC)

Se separa la asignación, tanto a lo recursos como los usuarios se le asigna una propiedad (Ej. Rol).



Attribute Based Access Control (ABAC)

Se generaliza RBAC, permitiendo asignar varias propiedades.

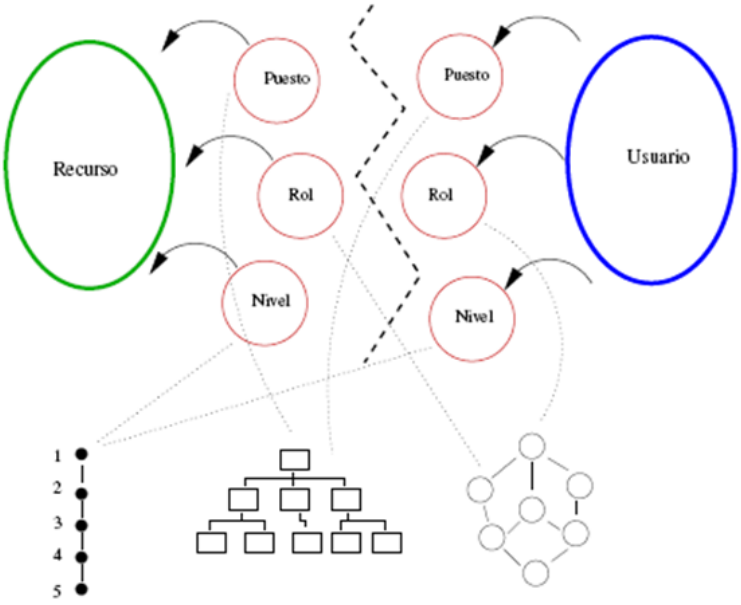


LRBAC/HRBAC

Los valores de las propiedades pueden ser un conjunto “parcialmente ordenado”

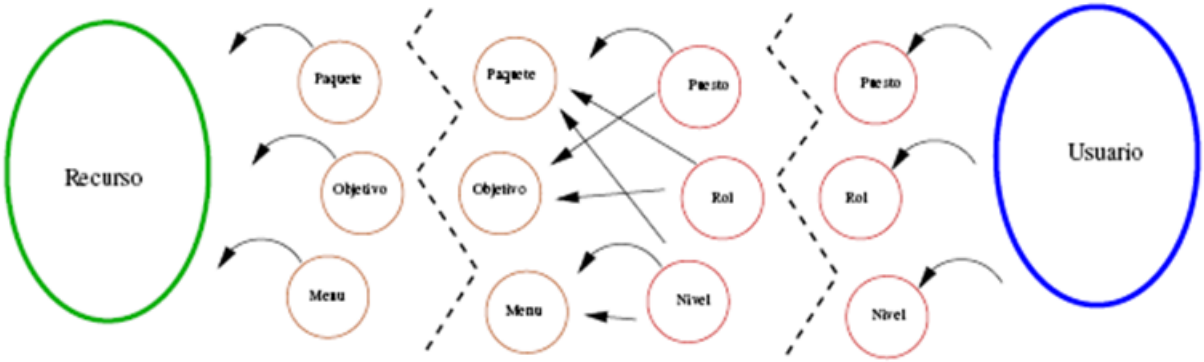
- Árboles, Retículos,
- Arboles invertidos,
- Secuencias,
- Estructuras jerárquicas

Permite utilizar por ejemplo <= nivel1 o > director etc.



Multi Level Attribute Based Access Control (MABAC) (PECAS)

Generaliza ABAC, permitiendo agrupaciones de recursos, además de usuarios.



Recursos Una instancia de proceso puede asignar dinámicamente un recurso

Usuarios Una sesión puede asignar dinámicamente a un usuario

Conclusiones sobre los modelos

- El grado de distribución de la autorización (MAC/DAC) es independiente de las formas de agrupamiento (RBAC/ABAC/MABAC).
- Los modelos RBAC y ABAC permiten la asignación grupal de permisos. Ej. el cambio de una propiedad en el usuario cambia automáticamente sus permisos.
- Los Atributos "parcialmente ordenados" pueden modelar información organizacional de los sistemas heredados de otros análisis. (organigrama, áreas, comités, grupos, equipos)
- MABAC permite asignación grupal de recursos, extendiendo las ventajas de los modelos anteriores. (paquetes informes, objetivos indicadores, ítems de menú, roles de proceso)
- La multiplicidad de niveles permite discriminar niveles con asignación dinámica y con asignación estática.