Nueva funcionalidad de PaaSOS – tuiSecurity ACL's

La gestión de seguridad en las aplicaciones de gestión es un punto muy importante, tan importante que si una aplicación de gestión no dispone de seguridad de acceso no es válida para muchos clientes (medianos y grandes). Además la LOPD y reglamentos obligan a tener claramente delimitado el control y acceso sobre los datos sensibles.

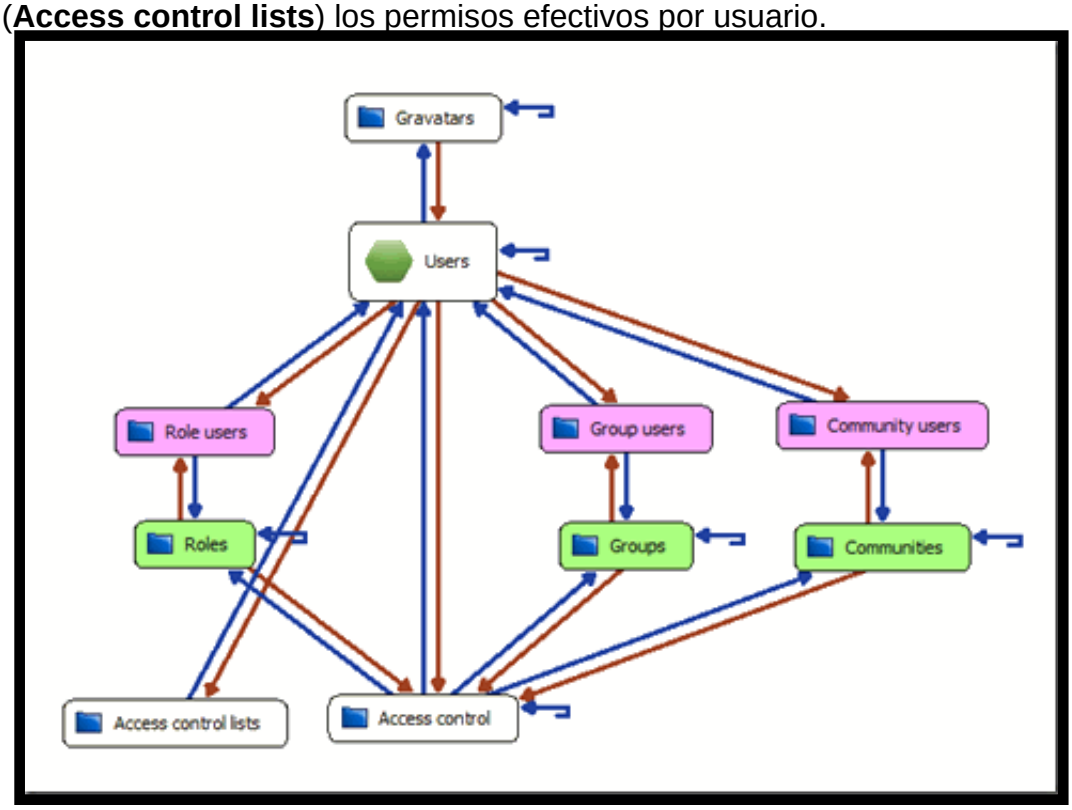
En **PaaSOS** se está teniendo muy en cuenta, en el módulo **tuiSecurity** poco a poco va dando forma a un conjunto de funcionalidades que permiten gestionar seguridad física y lógica a todos los niveles en **PaaSOS**.

- **Seguridad Física (física de acceso)**: por Grupos y Usuarios
- **Seguridad Lógica (lógica de negocio)**: por Roles/Comunidades y Usuarios.

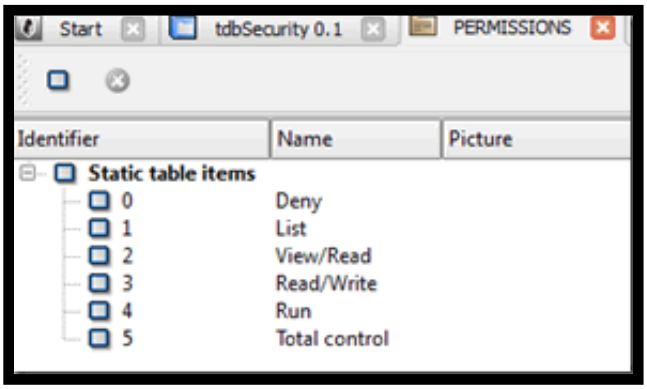
Este módulo es tan importante que supondrá un rediseño sustancial de las plantillas y de los interfaces de usuario de **PaaSOS**. Estas y otras mejoraras introducidas (atomicidad de módulos, seguridad de acceso, persistencia de variables de sesión y acciones centralizadas) en las próximas versiones de plantillas mejorarán sustancialmente la normalización de todo el trabajo realizado en **PaaSOS** y permitirán cerrar el lazo en el diseño del núcleo v0.2.

El diseño del módulo **tuiSecurity** a nivel de datos es relativamente sencillo:

En la tabla **Access control** se almacena toda la configuración de seguridad y en una tabla en memoria (**Access control lists**) los permisos efectivos por usuario.



Sobre otra tabla estática definimos los distintos niveles de permisos (inicialmente seis niveles).



Los permisos son acumulativos.

La única excepción es el permiso *Deny* que deniega digan lo que digan los demás.

En una tabla **MODULES** almacenamos dinámicamente (bajo demanda) el árbol de módulos de datos/interface de nuestro sistema.

El nivel de granularidad de los permisos es a nivel de item en cada módulo por usuario.

Esto que quiere decir… Sencillo que podríamos dar un cierto nivel de permiso a cualquier usuario en cualquier módulo sobre cualquier elemento (bien sean acciones o elementos de lista).

Nosotros decidimos el nivel de granularidad según el módulo.

Aparentemente este montaje es complejo, pero toda esta complejidad queda encapsula en una única función **FNC_SYS_GET_PERMISSIONS_MODULE_ITEM** que permite conocer el estado de un cierto permiso de un usuario sobre un elemento de un módulo.

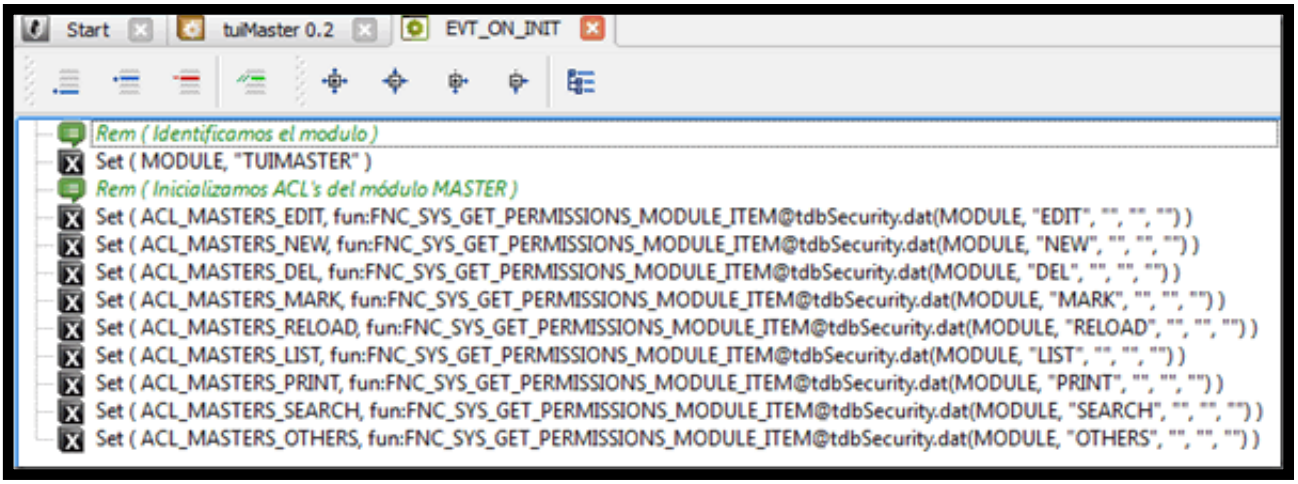
Esta función tiene dos parámetros;

- **MODULE**: Módulo del que deseamos obtener el permiso.
- **ITEM**: Elemento del que deseamos obtener el permiso (Puede ser una acción, un elemento de una lista o cualquier otra cosa que necesites validar.

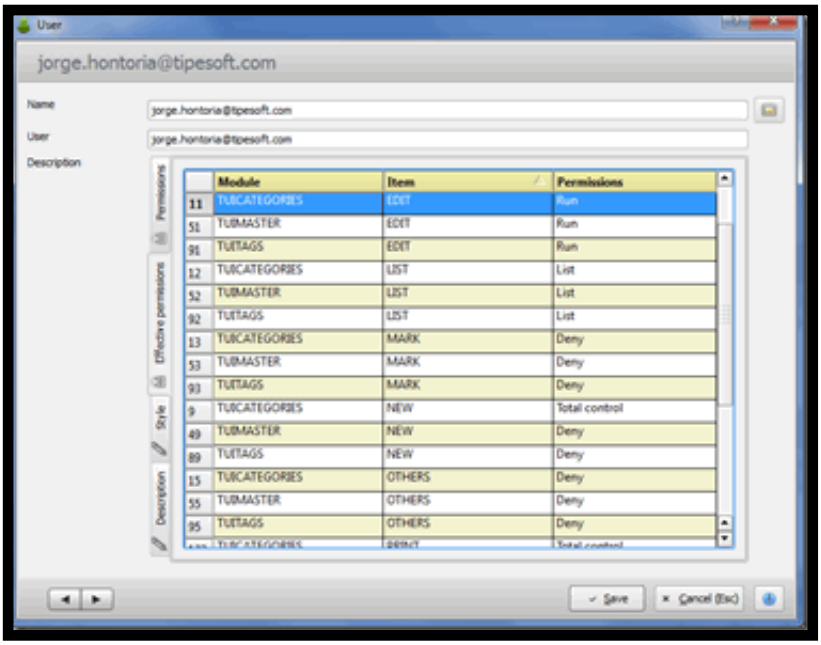
  Los otros tres parámetros son para aplicaciones futuras (actualmente no tienen uso).

Esta función es llamada en los eventos ON_INIT de formularios, rejillas, slots, etc.

Se llaman una sola vez por **ITEM,** recogiendo el nivel de permisos (de 0 a 5) para el usuario actual en una variable local con nombre **ACL_XXXX_YYYY**. Estas variables son las que usaremos en las condiciones de visibilidad y activo para no cargar con múltiples llamadas de función (fundamental para no realizar múltiples peticiones en los refrescos de condiciones). Aquí tenéis un ejemplo de como sería un evento EVT_ON_INIT y sus llamadas:



A nivel del interface de gestión dispondremos de un módulo **tuiSecurity** para consultar los permisos efectivos de un usuario así como para definir o modificar el nivel de permisos de cada usuario/grupo/rol/comunidad por módulo e item



Esperemos que este módulo resuelva el mayor número de problemáticas de seguridad posibles de forma sencilla y práctica. Hemos dedicado muchos esfuerzos en conseguirlo por lo que esperemos que no os defraude.