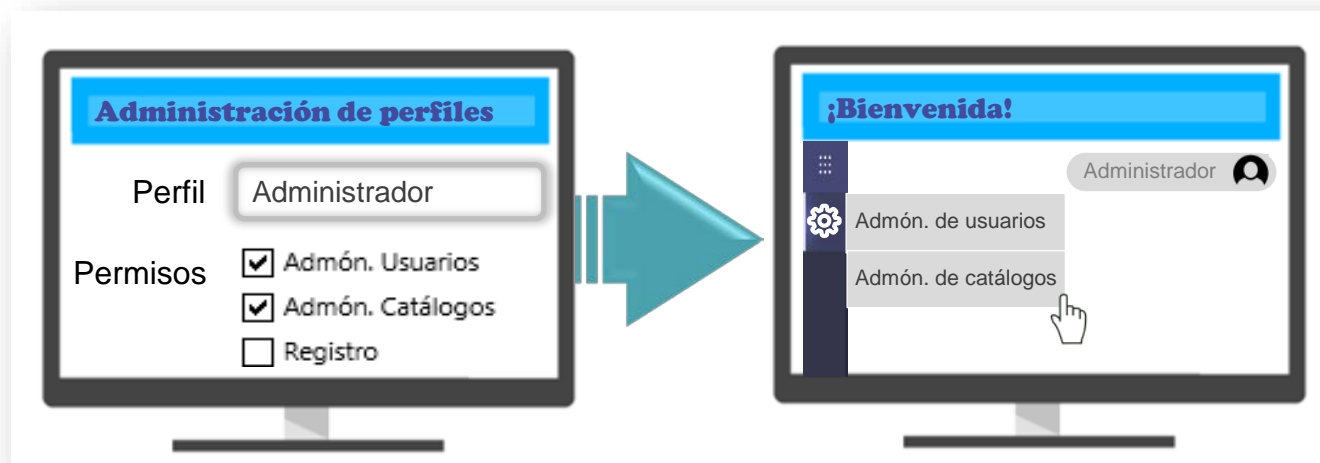


# ¿La información / funcionalidad sólo se le presenta a los usuarios autorizados?

Para identificar si presenta la información o la funcionalidad al usuario autorizado se recomienda aplicar los casos de prueba descritos más adelante.



La revisión tiene que realizarse por usuario, verificando que:

- ❑ Al usuario únicamente le muestre la información correspondiente al perfil asociado (ni menos, ni más).
- ❑ El usuario únicamente tenga acceso y realice los movimientos de las secciones correspondientes al perfil asociado (los mismos, ni menos, ni más, ni diferentes).



En la revisión de los movimientos permitidos se debe considerar que normalmente los permisos se presentan por sección, por ejemplo:

- » El permiso para 'administrar catálogos' contempla los movimientos: agregar, editar, eliminar tanto los catálogos como de sus opciones.
- » El permiso para 'administrar usuarios' contempla los movimientos: agregar, editar, eliminar, habilitar / deshabilitar a los usuarios, reiniciar contraseña, desbloquear al usuario.

Caso de prueba: Asignar a un usuario un perfil con un permiso asociado.

- Paso 1.** Crear un usuario y asignar un perfil con un sólo permiso asociado.
- Paso 2.** Autenticarse, consultar la información y realizar el/los movimiento(s) permitido(s) de acuerdo con el perfil del usuario.
- Nota.** En caso de que el software permita consultar menos o más información, o bien, realizar diferentes acciones de las asociadas a su perfil, se tendrá que reportar como defecto.
- Paso 3.** Editar el usuario y cambiar el perfil con otro permiso asociado y verificar nuevamente su funcionalidad, repetirlo hasta probar con todos los permisos.



Se sugiere que el orden para asignar los permisos corresponda a los pasos del flujo de información. Por ejemplo: iniciar con los permisos para administrar usuarios, catálogos u otra configuración previa necesaria, continuar con permisos para registrar, seguidos de los movimientos subsecuentes, hasta llegar a la generación de informes.



En ocasiones para poder realizar un movimiento se debe contar con más de un permiso, en estos casos el software debe asignarlos de forma automática. Asimismo, considerar que no todo el software da la posibilidad de elegir los permisos asociados a un perfil, en algunos casos, los perfiles cuentan con permisos específicos, por lo que las pruebas se deben ajustar a dicha funcionalidad.

Caso de prueba: Asignar a un usuario un perfil con más de un permiso asociado.

- Paso 1.** Crear dos usuarios. A cada usuario asignar un perfil con permisos intercalados respecto al flujo de información. Por ejemplo, considerando el siguiente flujo:



- Paso 2.** Cada usuario deberá autenticarse, consultar la información de las secciones autorizadas y realizar los movimientos que tiene permitidos del flujo de información, revisando el intercambio de datos respecto al otro usuario.



Un elemento a considerar es que la mayoría del software restringe la información a presentar al usuario, por ejemplo, un usuario solo puede consultar y/o realizar movimientos en los registros que él mismo generó, o bien, de una entidad federativa o dependencia / entidad en específico.

### Caso de prueba: Asignar a un usuario un perfil con todos los permisos asociados.

**Paso 1.** Crear un usuario y asignar un perfil con todos los permisos asociados.

**Paso 2.** Autenticarse y consultar la información de las diversas secciones, en este caso normalmente podría ver la información de todos los usuarios y realizar un flujo de información completo, se recomienda dar seguimiento a registros de otros usuarios.

### Caso de prueba: Autenticarse con un usuario, cerrar sesión y autenticarse con otro usuario.

En un mismo navegador:

**Paso 1.** Autenticarse con un usuario que tenga todos los permisos asignados, realizar movimientos que impliquen guardar información y cerrar sesión.

**Paso 2.** Autenticarse con otro usuario que cuente con menos privilegios, navegar mediante las flechas del teclado o los botones del navegador, retrocediendo y avanzando.

**Paso 3.** Realizar movimientos que impliquen guardar información.

Durante la prueba verificar que el software siempre presente la información del último usuario y guarde adecuadamente los cambios aplicados, sin mezclar con la cuenta del usuario anterior.

### Caso de prueba: En el mismo navegador autenticarse con diferentes usuarios.

En un mismo navegador:

**Paso 1.** Autenticarse con diferentes usuarios en diferentes pestañas de un mismo navegador.

En caso de que el sistema no permita tener las dos sesiones en un mismo navegador, verificar que se presente la información del último usuario autenticado. De lo contrario, en caso de que se permita tener las dos sesiones en un mismo navegador, con cada usuario realizar movimientos que impliquen guardar información, para verificar que no se mezcla los datos de ambas cuentas.

### Caso de prueba: Intentar ingresar a la información o a las secciones no permitidas mediante la URL.

**Paso 1.** Autenticarse con un usuario que tenga privilegios limitados.

**Paso 2.** Manipular la URL agregando identificadores de registros no permitidos para el usuario o de secciones a las que no tiene acceso el usuario. El sistema no debe permitirlo.