**CIPOLWeb**

**Configurador Interactivo de Políticas**

**de Seguridad de los sistemas COA**

MANUAL DEL USUARIO

*Fecha del documento: 07/06/17*

*Versión Aplicativo CIPOLWEB 1.0.11.0*



Desarrollado por COA S.A.

|  |
| --- |
| **Contenido** |

[Capítulo 1 - Antes de Comenzar 3](#_Toc484614202)

[Acerca del Manual del Usuario 3](#_Toc484614203)

[Convenciones del documento 4](#_Toc484614204)

[Capítulo 2 - Introducción 5](#_Toc484614205)

[Objetivos 5](#_Toc484614206)

[Alcance 5](#_Toc484614207)

[Arquitectura 5](#_Toc484614208)

[Capítulo 3 - Conceptos Básicos 7](#_Toc484614209)

[Ingreso al Sistema 7](#_Toc484614210)

[Panel de Ejecución 8](#_Toc484614211)

[Ingreso a los sistemas aplicativos 9](#_Toc484614212)

[Cambio de contraseña de usuario 9](#_Toc484614213)

[Terminar la sesión 10](#_Toc484614214)

[Modalidad de la implementación 10](#_Toc484614215)

[Selección de la modalidad 11](#_Toc484614216)

[Configuración inicial 13](#_Toc484614217)

[Políticas de Seguridad 13](#_Toc484614218)

[Administración de Usuarios 13](#_Toc484614219)

[Capítulo 4 - Módulo Administrador 14](#_Toc484614220)

[Menú del Sistema 14](#_Toc484614221)

[Sistemas 15](#_Toc484614222)

[Definición de Políticas Generales. 15](#_Toc484614223)

[Habilitación de Terminales Operativas 16](#_Toc484614224)

[Agrupamiento de Tareas 18](#_Toc484614225)

[Bloqueo de Sistemas 21](#_Toc484614226)

[Administración de Roles 23](#_Toc484614227)

[Administración de Usuarios 26](#_Toc484614228)

[Visor de Sucesos 37](#_Toc484614229)

[Reportes 39](#_Toc484614230)

[Listado: Usuarios por Roles 40](#_Toc484614231)

[Listado: Usuarios por Áreas 41](#_Toc484614232)

[Listado: Roles por Usuario 41](#_Toc484614233)

[Listado: Composición de Roles 42](#_Toc484614234)

[Listado: Terminales 43](#_Toc484614235)

[Listado: Usuarios 44](#_Toc484614236)

[Listado: Usuarios sin Acceso 44](#_Toc484614237)

[Listado: Control de Inactividad 45](#_Toc484614238)

[Herramientas 46](#_Toc484614239)

[Monitor de Actividades 46](#_Toc484614240)

[ABM de Áreas 47](#_Toc484614241)

[ABM de Sistemas 48](#_Toc484614242)

[ABM Tareas Autorizantes 51](#_Toc484614243)

[ABM Tareas Primitivas 55](#_Toc484614244)

[Análisis de Auditoria 56](#_Toc484614245)

[Cambiar nombre del Dominio. 59](#_Toc484614246)

[Cambio de contraseña de usuario 59](#_Toc484614247)

[Acerca de 59](#_Toc484614248)

[Cerrar el Sistema 60](#_Toc484614249)

[Revisiones del documento 61](#_Toc484614250)

**Capítulo 1**

# Antes de Comenzar

Bienvenido a **CIPOL** , el sistema que permite administrar la seguridad de otras aplicaciones, facilitando su integración modular desde una plataforma centralizada.

## Acerca del Manual del Usuario

El presente Manual del Usuario provee información sobre tareas de configuración y administración de **CIPOL**  como proveedor de seguridad a otros aplicativos, y describe los procedimientos para efectuar dichas tareas.

Está dirigido a los administradores de sistemas, administradores de la seguridad informática o administradores de red, conforme a las responsabilidades delegadas en materia de seguridad en su empresa u organización.

Este manual asume que el lector está familiarizado con la implementación de políticas de seguridad en sistemas informáticos, no obstante constituye por sí mismo una fuente de información para conceptos relacionados con seguridad. También se asume que se tiene conocimiento de cómo operar los sistemas operativos Windows® de Microsoft® (7 o superior).

La documentación está estructurada a través de los siguientes capítulos:

* Capítulo 1: Antes de Comenzar
* Capítulo 2: Introducción
* Capítulo 3: Conceptos Básicos
* Capítulo 4: Módulo Administrador

## Convenciones del documento

En este manual se utilizan las siguientes convenciones para distinguir elementos de texto:

|  |  |
| --- | --- |
| Símbolo o estilo de escritura | Propósito |
| **Negrita** | Nombres de campos en formularios |
| Nombres de elementos de la interfaz del usuario (botones, menús, ventanas, etc.) |
| *Itálica* | Término nuevo |
| Palabras enfatizadas |
| Títulos de documentos |
| 10 pt. Courier New | Código de programa |
| Nombres de archivos, directorios, rutas. |
| <Alt> | Tecla que debe presionar |

Además se incluyen comentarios y sugerencias para aclarar o ampliar los conceptos desarrollados, en el formato que se muestra a continuación:

🛈 *La barra de estado al pie de pantalla está dividida en 3 paneles, indicando la versión del programa, la identificación de la base de datos y la fecha y hora respectivamente.*

**Capítulo 2**

# Introducción

Desde el punto de vista de la arquitectura de software **CIPOL**  es, esencialmente, una capa que se interpone entre el sistema operativo y otras aplicaciones. Esto permite incorporar, en forma modular, diversos subsistemas o aplicativos que harán uso de **CIPOL**  como proveedor centralizado de la seguridad.

Si bien para su operación no es imprescindible contar con conocimientos o experiencia previa en sistemas, es recomendable que el responsable de la administración de la seguridad de los sistemas que controla **CIPOL** , se interiorice en los conceptos que implementa.

Esta guía se encuentra organizada de acuerdo a las funciones principales de **CIPOL** , de tal forma que el usuario pueda seguir una secuencia lógica en el aprendizaje.

En la gran mayoría de los temas, se han incorporados ejemplos gráficos que ayudan la comprensión del texto explicativo.

## Objetivos

**CIPOL**  otorga un soporte centralizado e integrado a las funciones operativas propias de la seguridad de sistemas, tales como la implementación de políticas, administración de usuarios, acceso a subsistemas y configuración de roles, brindando la información adecuada y necesaria para conformar un entorno seguro para los aplicativos que se ejecutan en su entorno.

## Alcance

**CIPOL**  consta de dos componentes bien diferenciados, que si bien conviven encapsulados en un solo programa ejecutable, manifiestan interfases diferentes de acuerdo al tipo y rol de usuario que lo inicia. Estos son:

* *Módulo Administrador:* es la interfase disponible para los usuarios Administradores de la Seguridad para el manejo de políticas, altas bajas y modificaciones de usuarios y terminales, roles, y niveles de autorización.
* *Módulo Cliente:* la que se instancia para el resto de los usuarios finales de los aplicativos controlados por **CIPOL** . Conforma el núcleo de la seguridad. Integra a los aplicativos que maneja, es decir que el usuario sólo debe ejecutar este componente y a partir de allí tendrá acceso a los subsistemas para los que esté autorizado.

## Arquitectura

La siguiente figura, presenta una vista lógica de cómo **CIPOL**  está estructurado:

Identificación única del usuario (login)

Usuario “master”

Otros usuarios

Base de datos

**Módulo Administrador**

Definición y mantenimiento de:

* Políticas de seguridad
* Tareas y Roles
* Tareas autorizantes
* Usuario
* Terminales Habilitadas

**Módulo Cliente**

Panel de ejecución:

**Módulo Cliente**

Agente controlante

por sistema

Sistema3

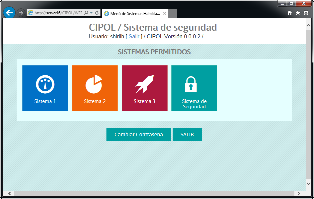
Sistema2

Sistema1

Usuario habilitado Roles del usuario (indica sistemas y tareas permitidas)

actualiza

Si es un usuario con Rol de Administrador de seguridad



**Capítulo 3**

# Conceptos Básicos

Si bien para su uso **CIPOL**  necesita solo un explorador de Internet (admite la mayoría de los estándares del mercado), es posible que, con algunos, determinadas funciones de **CIPOL**  se vean reducidas, limitadas o disponibles únicamente a través de procedimientos alternativos.

Debido a las características de diseño de **CIPOL** , distinguiremos dos modalidades de uso a los efectos de facilitar la comprensión:

* *Modo Administrador:* Corresponde a la instancia en que **CIPOL**  ejecuta el Sistema de Seguridad mencionado en el capítulo anterior. Requiere que el usuario posea atributos de administrador de la seguridad.
* Modo *Cliente:* la disponible para los usuario que inician la sesión en **CIPOL** para ejecutar y operar los sistemas aplicativos para los cuales tengan acceso autorizado y sean controlados (para acceso y uso) por el propio **CIPOL** .

Ambas modalidades utilizan la misma forma de ingreso del usuario al sistema, **CIPOL**  se encarga de verificar cuáles son los atributos del mismo y actúa en consecuencia.

Esta guía está organizada entorno a las funciones del sistema, proporcionadas a través de los menús de **CIPOL** , como así también por los íconos de acceso rápido y de las solapas que titulan las carpetas en las que se encuentra distribuida la información.

Antes de comenzar la lectura de los capítulos en los que se explican los comandos de menús, aconsejamos completar la lectura de este capítulo, donde encontrará información necesaria aplicable en el manejo del entorno interactivo de **CIPOL** .

Si bien en el desarrollo de los temas, se presentan imágenes del sistema, debe considerarse que son meramente ilustrativas, pudiendo diferir a las realmente implementadas.

## Ingreso al Sistema

Para iniciar **CIPOL**  se debe ingresar a la URL donde se aloja el sistema (solicitarla al personal de administración del sistema). A continuación se presentará una pantalla de presentación, donde el usuario se deberá registrar como tal mediante el ingreso del nombre de usuario que le fue asignado y su contraseña, las que serán validadas contra la lista de usuarios autorizados, previamente habilitados dentro de **CIPOL**  por el Administrador de la Seguridad.

A continuación se muestra un ejemplo gráfico de la pantalla de conexión al sistema:



El valor de “Usuario” (nombre de usuario) no es sensible a las letras mayúsculas y minúsculas, por lo cual no es necesario que el operador tome recaudos al respecto, no siendo este el caso para la contraseña en la que sí se distingue entre mayúsculas y minúsculas con lo cual se deberá prestar atención la forma de ingreso de la misma.

## Panel de Ejecución

Cuando el usuario se ha identificado correctamente, si se trata de una cuenta de usuario distinta a “master”, el sistema desplegará una nueva pantalla con el *Panel de Ejecución de Sistemas Habilitados* que él pueda operar.



La figura anterior muestra como **CIPOL** establece la apariencia del Panel, en función del usuario que inicia la sesión, disponiendo de los accesos para la ejecución de los aplicativos a los que dicho usuario tiene autorizado operar (3 en el ejemplo de la figura).

🛈 *La cuenta de usuario “master” (Superusuario) es una cuenta de usuario exclusiva del módulo Administrador de* ***CIPOL*** *. En consecuencia, para ella no se presenta el Panel de Ejecución al validar la cuenta y contraseña. Directamente* ***CIPOL***  *lanza la ejecución del sistema de Seguridad.*

El Panel de Ejecución inicia el *Módulo cliente* de **CIPOL** , y se trata de la única interfase visual que ofrece este modo operativo. Una vez que se inician las ejecuciones particulares de los aplicativos controlados por **CIPOL** , este establece un agente que se instancia en memoria interactuando con el programa aplicativo activando o desactivando controles y permisos según los Roles del usuario activo.

Esto significa que el *Módulo cliente*, si bien será el que más tiempo estará operativo en la red (estará acompañando la ejecución de todos los aplicativos y para todos los usuarios), será un aplicativo que pase inadvertido para los usuarios finales.

## Ingreso a los sistemas aplicativos

Para ejecutar los sistemas controlados por **CIPOL** , bastará con hacer click sobre los accesos disponibles en el Panel en el área central.

Cada uno de los accesos presentará como etiqueta el nombre y una imagen representativa del sistema asociado.

El Panel de Ejecución presentará tantos accesos como sistemas habilitados a operar tenga el usuario activo.

Luego de seleccionar un acceso a un aplicativo, **CIPOL**  pasará a segundo plano, dejando el panel en otra ventana del navegador de Internet.

## Cambio de contraseña de usuario

El usuario podrá cambiar su contraseña tantas veces como lo desee. Para ello dispone del acceso **Cambiar contraseña**. Al hace click sobre el mismo, se mostrará en pantalla una nueva ventana donde se le solicitará que ingrese la contraseña actual (este paso permite verificar que quién está operando sea el dueño de la cuenta de usuario activa) y luego que ingrese 2 veces la nueva contraseña (para verificar el tipeo correcto).

Si los 3 ingresos son correctos, al pulsar el botón **Cambiar Contraseña**, la nueva contraseña quedará establecida como vigente.



🛈 *Si la seguridad está establecida como “Integrada al Dominio”, este acceso estará inhibido. Para el cambio de contraseña del usuario se deberá utilizar el mecanismo que ofrece el propio sistema operativo.*

🛈 *Posiblemente existan políticas de seguridad establecidas que restrinjan el formato de la nueva contraseña, como por ejemplo longitud, que no repita alguna de las n anteriores utilizadas, etc. Consulte al Administrador de Seguridad acerca de las restricciones impuestas al sistema.*

## Terminar la sesión

El pulsar el botón **SALIR**,provocará la finalización de la sesión de usuario.

🛈 *si luego de ingresar en un sistema, el usuario cierra la ventana de* ***CIPOL*** *, al cerrar dicho sistema no podrá acceder a ningún otro, debiendo loguearse nuevamente.*

## Modalidad de la implementación

**CIPOL**  provee dos modalidades de funcionamiento mutuamente excluyentes entre sí, es decir una vez seleccionada una de ellas, continuará siempre bajo ese esquema. Estas refieren al *origen* de las cuentas de usuario y el entorno que se hace cargo de la parametrización y control de las políticas básicas de seguridad.

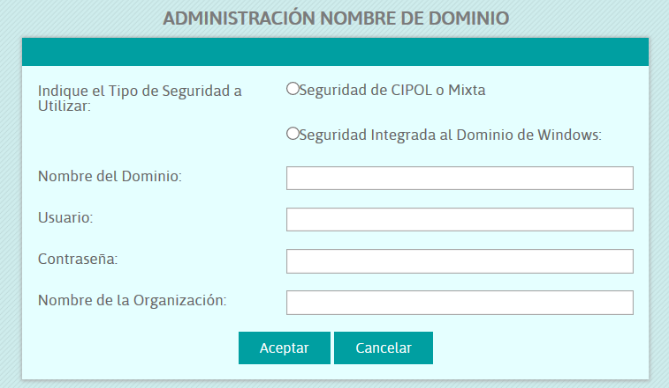
Las modalidades son:

* *Administrada por* ***CIPOL*** . En este caso el usuario administrador debe ingresar las cuentas usuario y todos sus datos asociados, además deberá establecer los parámetros, que conforman las **Políticas de Seguridad** que regirán en los sistemas. Esta información se registrará en la base de datos propia de **CIPOL**  y se administrará desde el mismo aplicativo.
* *Integrada al dominio*. Este modo permite que **CIPOL**  obtenga las cuentas de usuario desde el controlador de dominio, evitando de esta manera la duplicidad de dichas cuentas con el objeto de facilitar la administración. Además delega hacia el sistema operativo, funciones y parametría de la seguridad tales como bloqueo de cuentas, longitud mínima de la contraseña, duración máxima y mínima de la contraseña, cambio de contraseña, etc.

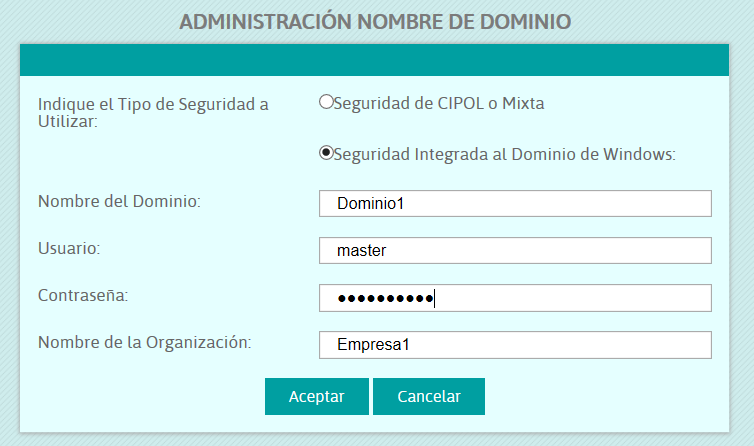
🛈 *Si bien la modalidad Integrada ofrece numerosas ventajas, tiene como condicionante la existencia de un dominio de Windows. Por ese motivo* ***CIPOL***  *provee la capacidad adicional de manejo de cuentas y políticas, de manera tal de permitir su uso en entornos donde no haya un controlador de dominio. Este es el caso, por ejemplo, de grupos de trabajo o entornos híbridos Windows/Unix .*

#### Selección de la modalidad

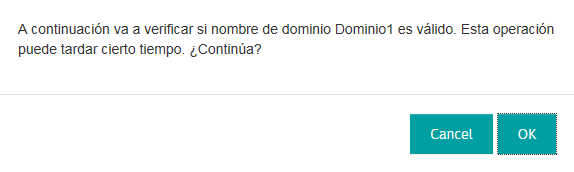
En el primer inicio de sesión a **CIPOL** , luego de su instalación, se desplegará la siguiente ventana:



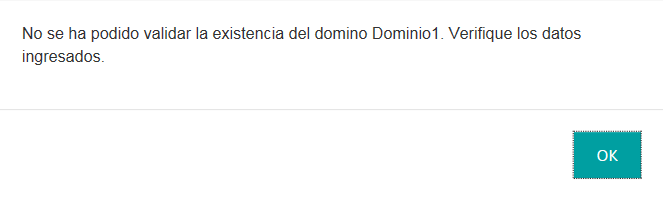
El usuario administrador deberá elegir una de las opciones mencionadas, de acuerdo al esquema que se adopte. A continuación nos concentraremos en las particularidades que presenta la modalidad **Integrada al dominio Windows**.



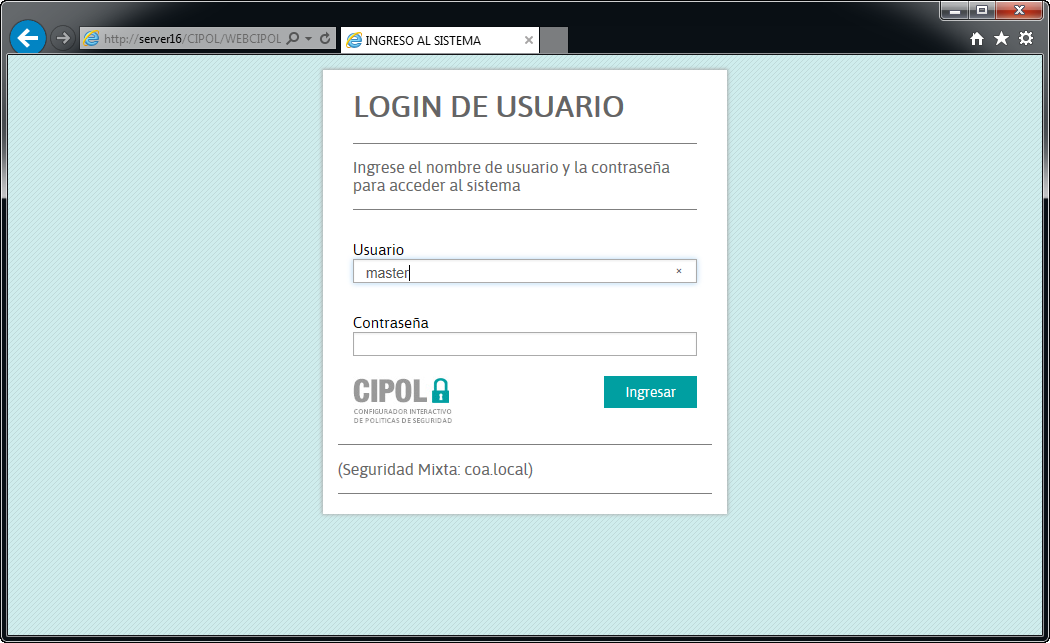
Los datos asociados a ésta selección son **Nombre del Dominio** y **Nombre de la Organización**. Una vez ingresados **CIPOL**  validará el nombre del dominio:



En casos de error en la especificación del dominio, o que debido a problemas de red no sea posible conectarse, el sistema mostrará el mensaje:



Si la validación es satisfactoria se presentará la pantalla de conexión:



En esta instancia es necesario ingresar a **CIPOL**  como “master” dado que aún no se ha configurado el entorno inicial de usuarios del sistema. Por este motivo existe la opción **Cambiar Usuario**, que permite activar la caja de texto **Usuario** para identificarse como master.

#### Configuración inicial

A partir de las actividades previamente descriptas, selección de la modalidad y primer ingreso como SuperUsuario, es necesario establecer el entorno inicial de **CIPOL** . Esto comprende, fundamentalmente:

* Implementación de las Políticas de seguridad (parametría)
* Asignación de los usuarios del dominio hacia el entorno de **CIPOL**

A continuación se mencionarán los aspectos distintivos de esta modalidad sin profundizar en las descripciones, ni en la secuencia operativa, ya que eso se tratará en el próximo capítulo.

#### Políticas de Seguridad

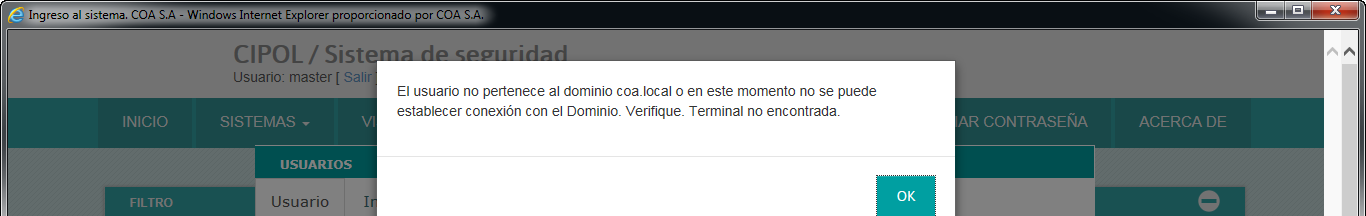
En el modo integrado sólo se puede establecer lo siguiente:

* Modo de asignación de tareas y roles

Como ya hemos mencionado, **CIPOL**  delega la administración y control de esas políticas de seguridad hacia el sistema operativo.

#### Administración de Usuarios

Otra característica de la modalidad integrada de **CIPOL**  es el alta de Usuarios para todos los aplicativos que forman parte de su entorno de seguridad. Consiste en ingresar el nombre de la cuenta de usuario, sus datos asociados y posteriormente **CIPOL**  convalidará la existencia de la cuenta en el dominio declarado.



**Capítulo 4**

# Módulo Administrador

Como se mencionó anteriormente, uno de los modos de ejecución de **CIPOL**  corresponde a la instancia en que **CIPOL**  ejecuta el Sistema de Seguridad

Este módulo se inicia al hacer clic en el botón de acceso a **Sistema de Seguridad** en el *Panel de Ejecución* o bien ingresando al sistema con la cuenta de usuario “master”.

De este modo, **CIPOL**  inicia el módulo Administrador mostrando el menú principal de la aplicación.

## Menú del Sistema

Este menú presenta las opciones para ejecutar la funcionalidad del módulo según lo muestra la siguiente figura.



En **CIPOL**  el establecimiento de la seguridad de las aplicaciones que controla se logra a partir de definir la configuración inicial del entorno, que comprende actividades de:

* Definición de Políticas Generales
* Administración de Áreas
* Habilitación de Terminales
* Definir agrupamiento de tareas
* Administración de tareas autorizantes
* Administración de Sistemas
* Administración de Tareas Primitivas
* Administración de Roles y
* Creación de los usuarios que puedan operar los sistemas.

Estas capacidades podrán aprovecharse ejecutando las acciones asociadas a las diferentes opciones disponibles en el menú principal.

En la barra de estado podemos ver la versión del aplicativo.

A continuación se encuentra el detalle de cada una de las opciones menú.

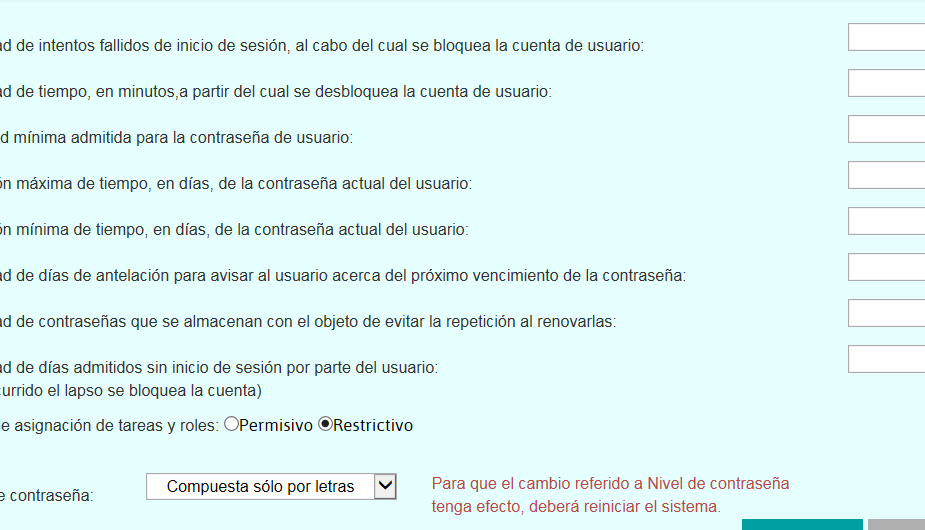
## Sistemas



#### Definición de Políticas Generales.

Al seleccionar **Definición de Políticas Generales**, **CIPOL**  presenta una nueva ventanacon múltiples campos de valores, las que se encuentran debidamente rotuladas para facilitar la comprensión del objeto de cada uno de los parámetros.

En la siguiente figura vemos un ejemplo de pantalla:



Este conjunto de políticas se almacenan en una estructura residente en el sistema administrador de base de datos, la cual es consultada por **CIPOL** , garantizando en todo momento el cumplimientos de las mismas para todos los aplicativos que corren en su entorno.

**Descripción de los parámetros**

Como bien se indica en la propia pantalla, un valor 0(cero) en los parámetros estará indicando que el mismo sea ignorado, a excepción del último, en el que este valor será considerado como el máximo admitido (2 minutos). Las aclaraciones siguientes valen para valores distintos de 0.

|  |  |
| --- | --- |
| ***Parámetro*** | ***Aclaraciones*** |
| **Cantidad de intentos fallidos de inicio de sesión, al cabo del cual se bloquea la cuenta de usuario.** | Alcanzada esta cantidad tope, la cuenta de usuario no podrá operar los sistemas hasta tanto un Administrador de Seguridad la desbloquee desde el módulo Administrador o bien transcurran los minutos establecidos en el parámetro siguiente. |
| **Cantidad de tiempo, en minutos, a partir del cual se desbloquea la cuenta de usuario.** | Indica los minutos que una vez transcurridos, una cuenta bloqueada será desbloqueada de manera automática sin intervención de un Administrador. |
| **Longitud mínima admitida para la contraseña de usuario.** | Cantidad mínima de caracteres que podrá tener una contraseña de usuario. |
| **Duración máxima de tiempo, en días, de la contraseña actual del usuario.** | Cantidad de días tope que **CIPOL**  permitirá mantener la misma contraseña. Vencido el plazo, obligará su cambio. |
| **Duración mínima de tiempo, en días, de la contraseña actual del usuario.** | Cantidad mínima de días de duración de las contraseñas. Si no se alcanzó el valor, **CIPOL**  no permitirá cambiarla. |
| **Cantidad de días de antelación para avisar al usuario acerca del próximo vencimiento de la contraseña.** | Cuando se alcancen los días establecidos, en cada inicio de sesión, **CIPOL**  informará que la contraseña está próxima a vencer. |
| **Cantidad de contraseñas que se almacenan con el objeto de evitar la repetición al renovarlas.** | Permitirá a **CIPOL**  que en cada cambio de contraseña controle que la nueva propuesta no coincida con las últimas usadas. |
| **Cantidad de días admitidos sin inicio de sesión por parte de un usuario. Transcurrido el lapso se bloquea la cuenta** | En cada nuevo inicio de sesión, **CIPOL**  verifica que este plazo no sea superado. De ser así, la cuenta será bloqueada automáticamente no permitiendo operar los sistemas a la cuenta en cuestión. |
| **Modo de asignación de tareas y roles** | Establece el comportamiento de los permisos otorgados a los usuarios cuando a un determinado rol existente se agregan nuevas tareas.  Si se consigna “Permisivo”, significa que cuando se agregan tareas a un rol se habilitan automáticamente para todos los usuarios que previamente lo hayan tenido asignado.  Por el contrario, en “Restrictivo”, los cambios al Rol no se propagarán hacia los usuarios, exigiéndose en este caso la edición de cada uno de ellos para activar las nuevas tareas. |
| **Nivel de contraseña** | Configura el nivel de complejidad exigido para las contraseñas de los usuarios, los valores posibles son:   * Sin requerimiento específico * Compuesta sólo por letras * Compuesta sólo por números * Compuesta por letras y números * Compuesta por letras, números y caracteres especiales |

#### Habilitación de Terminales Operativas

Otra de las capacidades que ofrece **CIPOL** , es poder controlar en que terminales de la red se pueden o no ejecutar los aplicativos bajo su control. Para esto requiere la registración (identificación) de todas las computadoras en las que se quieran operar los aplicativos. Esto se utiliza posteriormente para la habilitación del uso de las mismas por parte de los usuarios del sistema.

Esta registración conforma una medida adicional de seguridad ya que impide que en una terminal no registrada, se puedan ejecutar las aplicaciones controladas por **CIPOL** , aún en el caso en que se hayan instalado los aplicativos y se hayan conectado a la red local.

Para ejecutar esta funcionalidad, bastará con seleccionar del submenú **Sistemas**, la opción **Habilitación de Terminales Operativas.**

El cuerpo de la pantalla presenta dos vistas.

* **Filtro:** permite realizar una búsqueda más precisa sobre las terminales registradas hasta el momento.
* **Terminales:** Muestra la lista con las terminales registradas hasta el momento, según los filtros aplicados.

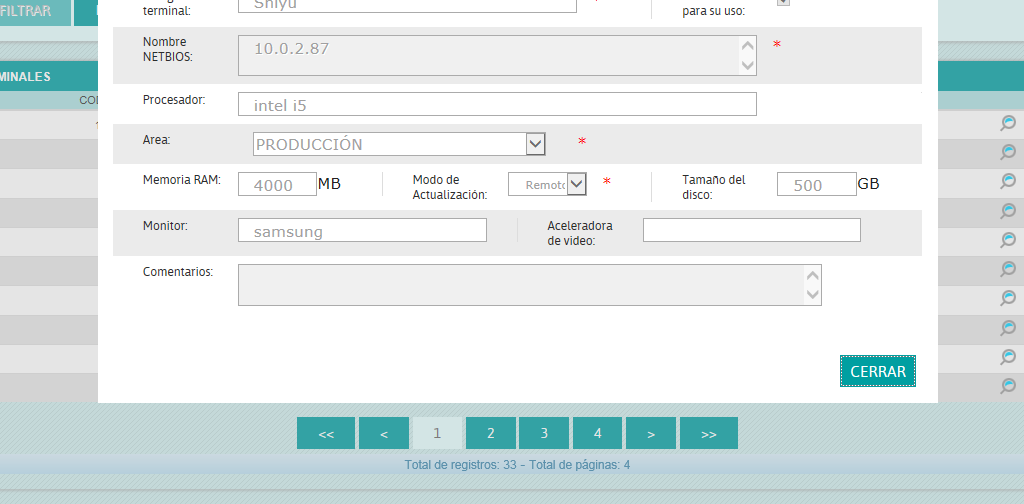
De acuerdo a los filtros, se muestra:

**Lista de Terminales:**



A través del botón  presente en cada uno de los renglones obtenidos en la búsqueda, se podrá acceder al detalle de esa terminal en particular.

**Detalle.**



En esta pantalla no se podrá hacer ningún tipo de modificación.

A través del botón  **(modificar)** presente en cada uno de los renglones obtenidos en la búsqueda, se podrá acceder a la modificación de esa terminal en particular.

A través del botón  **(eliminar)** presente en cada uno de los renglones obtenidos en la búsqueda, se podrá eliminar esa terminal en particular.

**Botón Nuevo:**

Este botón permitirá registrar una nueva terminal. Al presionar ese muestra un Pop-Up con todos los campos habilitados para ingresar los datos correspondientes.

**Botón Modificar:** 

Previamente se deberá encontrar el registro en la grilla y luego presionar el botón Modificar, el sistema muestra un Pop-Up con todos los campos habilitados para modificar los datos correspondientes.

**Botón Eliminar:** 

Previamente se deberá encontrar el registro en la grilla y luego presionar el botón eliminar para realizar la eliminación del mismo.

Dentro de la vista de detalle o el Pop-Up de nuevo/modificar, se puede encontrar lo siguiente:

**Casilla Habilitada para su uso**:

Por defecto al registrar una nueva terminal, esta opción se encuentra seleccionada. Pero esta opción también permite inhabilitar una terminal (por ejemplo, el usuario que tiene asignada esa terminal estará ausente por un tiempo prolongado, entonces se decide que nadie pueda operar los sistemas desde esa terminal), esto se logra desactivando la casilla.

A los efectos de facilitar las tareas administrativas, **CIPOL**  provee la posibilidad de obtener la lista de nombres NetBios de los equipos que conforman el dominio manteniéndolos sincronizados con los registrados en su propia base.

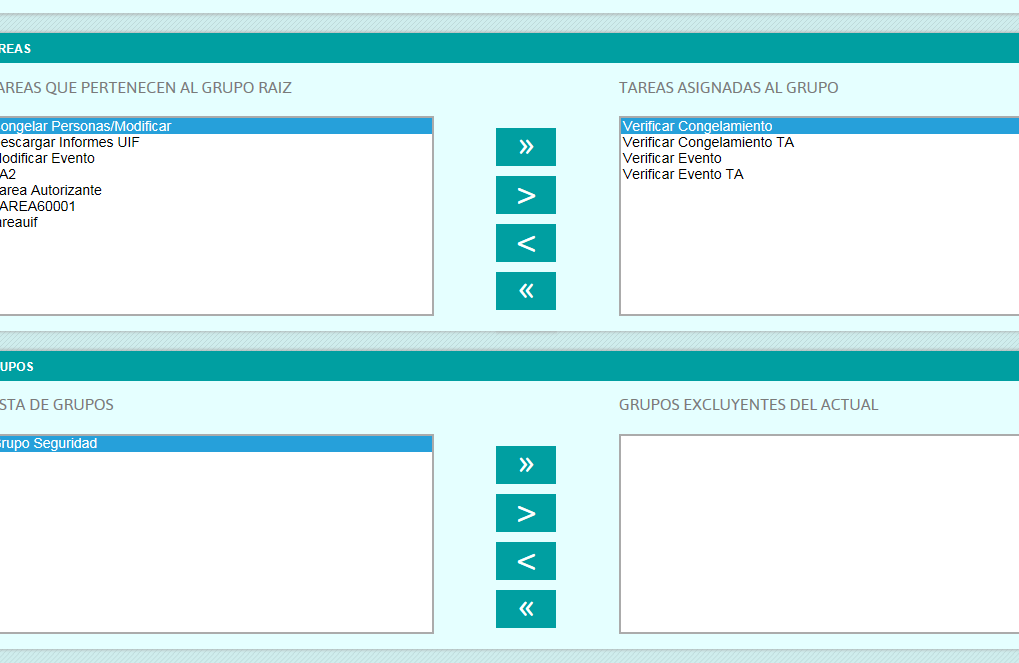
#### Agrupamiento de Tareas

El modelo de la seguridad en **CIPOL** está basado en tareas, las cuales son el nexo entre el aplicativo que delega la seguridad y los procesos que la implementan dentro de **CIPOL** . En **CIPOL**  inicialmente todas las tareas pertenecen a un grupo denominado *Grupo Raíz,* a partir de él pueden generarse nuevos grupos con las siguientes finalidades principales:

* Concentrar un conjunto de tareas en unidades lógicas que respondan a la estructura interna de la entidad y sus necesidades operativas en cuanto a la segregación de funciones.
* Establecer grupos excluyentes y establecer el control por oposición, cuando sea requerido para el cumplimiento de normativas internas de la entidad. Esto trae como consecuencia la imposibilidad de generar roles que contengan grupos de tareas que sean excluyentes entre sí.

La generación de nuevos grupos no es obligatoria, siendo recomendable su utilización cuando algunas de las características mencionadas precedentemente son aplicables para una implementación en particular.

El siguiente gráfico representa la interfase de **CIPOL**  destinada a la creación, modificación y eliminación de grupos, como así también para la designación de exclusiones entre ellos.



Descripción de cada una de las partes del formulario:

* **Grupos Existentes:** En la lista desplegable del encabezado se encuentra los grupos que se crearon. Esta lista crecerá cuando seleccionemos la opción Nuevo.
* **Tareas que pertenecen al Grupo Raíz:** Dentro de esta lista se encuentran las tareas que pertenecen al grupo raíz, permiten seleccionar las tareas mediante los botones de asignación, asignándolas a tareas asignadas al grupo. Esta lista se completa al seleccionar el sistema del combo Nombre del Sistema.
* **Tareas asignadas al grupo:** Dentro de esta lista se encuentran las tareas que se seleccionaron del grupo raíz, y que forman parte de las tareas asignadas al grupo.
* **Filtrada para el sistema:** Dentro de esta lista desplegable se encuentran los sistemas habilitados que se crearon en el sistema.
* **Lista de Grupos:** Lista los grupos existentes.
* **Grupos excluyentes del actual:** Se utilizan para implementar la exclusión. Se encuentran los grupos que estas excluidos del grupo actual.

**Consulta:**

Seleccionando un Grupo de la lista de Grupos existentes, las listas de los formularios se completan acorde a los datos cargados. Al seleccionar otro grupo de la lista de Grupos existentes, las listas de los formularios, cambiará acorde a lo que se encuentra registrado en cada sección.

Al ingresar a la pantalla, los botones de acción Nuevo, Modificar y Eliminar se encuentran habilitados.

**Botón Nuevo:**

Este botón permitirá registrar un nuevo grupo. Presionando este botón, se habilitará el campo Grupo Existentes, las botones de asignación y la lista **Filtrada para el sistema.**

Seleccionando un sistema de la lista Filtrada para el sistema, se completa el formulario Tareas que pertenecen al Grupo Raíz, los botones de asignación se utilizaran para mover las tareas al grupo que se está creando, como así también se realizará la misma acción para la lista de grupos excluyente del actual.

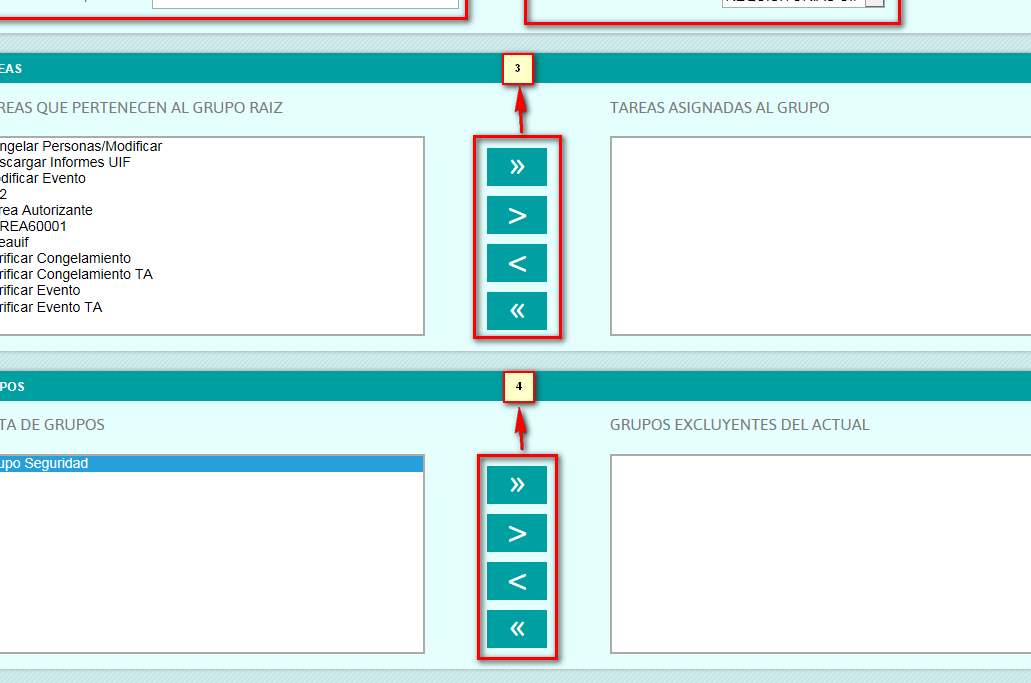
**Botón Modificar.**

Previamente seleccionar un grupo de la lista de Grupos Existentes que se desea modificar y presionar el botón Modificar, el sistema habilita todas las listas del formulario, la lista de filtrada para el sistema y los botones de asignación para realizar la modificación necesarias.

**Botón Eliminar:**

Previamente seleccionar un grupo de la lista de Grupos Existentes a eliminar, y presionar el botón eliminar para eliminar el grupo.

Vista al presionar el Botón Nuevo:



Pasos para ingresar un grupo NUEVO:

1. En la sección de Grupos Existentes (1), ingresar un nombre para asignarle al nuevo grupo.
2. En la sección filtrar para el sistema (2), seleccionar el sistema del cual se desea seleccionar las tareas. Al seleccionar el sistema la lista de Tareas que pertenecen al Grupo Raíz se completa.
3. Con los botones de asignación (3) mover las tareas del grupo Raíz y las tareas asignadas al grupo.
4. Con los botones de asignación que se encuentran en la sección (4), se puede excluir grupos.
5. Finalizada las selección de tareas y grupos, oprimir el botón **Guardar**, para registrar los datos ingresados.

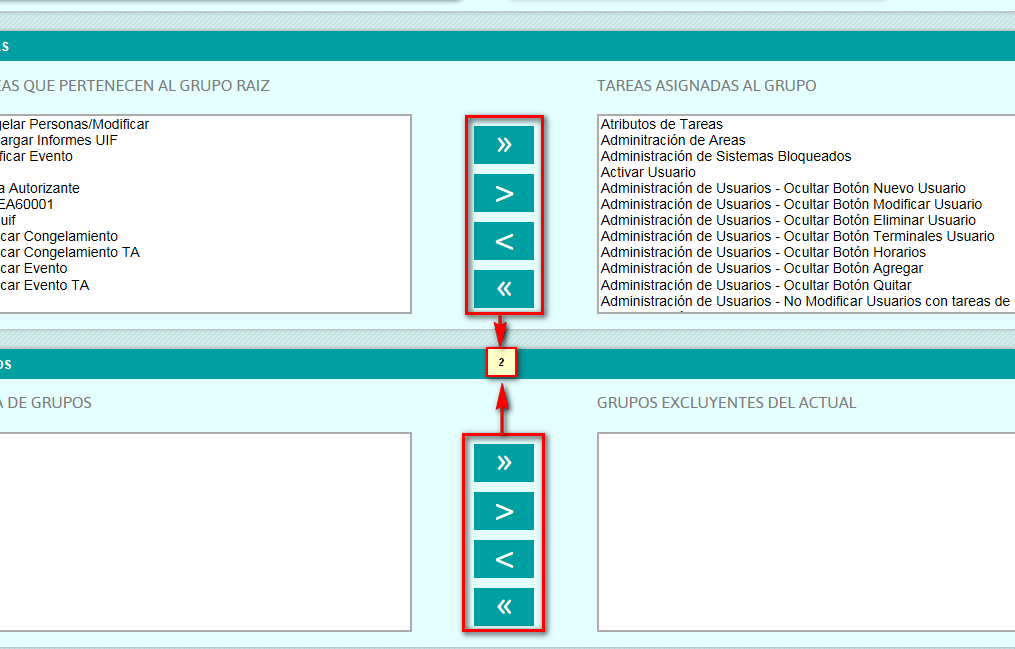
🛈 *Una Tarea puede pertenecer sólo a un Grupo y éste puede tener contener más de una Tarea.*

Vista al presionar Modificar:

Pasos para Modificar un Grupo Existente:

1. Seleccionar un grupo de la lista de Grupos Excluyentes (1) y presionar Modificar.
2. El sistema habilita el campo Grupos Existentes, los botones de selección (2), la lista desplegable de filtrada para el sistema (3) y las 4 listas, para poder realizar las modificaciones necesarias.
3. Una vez realizamos las modificaciones, presionar **Guardar.**

En el sistema quedará establecida la exclusión, lo cual conformará un esquema de seguridad que se utilizará posteriormente en la instancia de generación de roles.



🛈 *La implementación de Grupos en* ***CIPOL***  *no es obligatoria. Es importante tener presente que su utilización representa una carga administrativa considerable, normalmente justificada por una estricta política de seguridad.*

#### Bloqueo de Sistemas

Esta función se utiliza para deshabilitar el acceso de los usuarios a uno o más sistemas (de los que se ejecutan en su entorno), permitiendo el acceso a algunos usuarios designados por el administrador.

Esta función se encuentra disponible al acceder desde el Submenú Sistemas y seleccionar la opción Bloqueo de sistemas, la pantalla se encuentra distribuida en 4 listas:

* **Sistemas Desbloqueados:** Se encuentran los sistemas existentes.
* **Sistemas Bloqueados:** En esta lista se ubican los sistemas bloqueados. Inicialmente se encuentra vacía.
* **Lista de usuarios bloqueados:** Esta lista se completa cuando seleccionamos un sistema de la lista de Sistemas Desbloqueados y lo pasamos a Sistemas Bloqueados. En la lista de usuarios bloqueados, se encuentran todos los usuarios activos del sistema.
* **Lista de usuarios desbloqueados:** El administrador seleccionar uno o más usuarios de la lista de usuarios bloqueados y con los botones de asignación los pasa a la lista de usuarios desbloqueados para permitirles el acceso.



Al presionar el botón Modificar, se habilita la pantalla de la siguiente manera:



A continuación se detalla el funcionamiento de la misma

En la lista de Sistemas Bloqueados, se encuentra el sistema REQUISITORIAS UIF y Sistema de Seguridad que es el sistema a bloquear. Los usuarios pertenecientes a este sistema son, los que se encuentran en la Lista de Usuarios Bloqueados. En la lista de Usuarios Desbloqueados son los 3 usuarios o administradores seleccionados para operar en el sistema.

Al presionar **Guardar** quedarán establecidos los bloqueos realizados, con lo cual permitirá efectuar las tareas de mantenimiento o procesos especiales por parte del/los administradores o usuarios especiales del sistema.

#### Administración de Roles

Un rol es un conjunto de tareas que se define a los efectos de permitir a los usuarios realizar actividades que responden a las reglas internas de la entidad y adicionalmente a las reglas de validación propias de cada aplicativo.

🛈 *A diferencia de los Grupos, la generación de Roles y su asignación a los usuarios habilitados, es obligatoria para acceder a los aplicativos que se ejecutan bajo el entorno de seguridad de* ***CIPOL*** *. La única excepción es el propio* ***CIPOL***  *que posee un usuario “master” generado durante la instalación, el cual accede a todas las funcionalidades con el objeto de realizar la configuración inicial de la seguridad.*

En **CIPOL**  es obligatorio implementar al menos un rol para cada aplicativo, ya que es la mínima unidad de asignación de permisos hacia los usuarios.

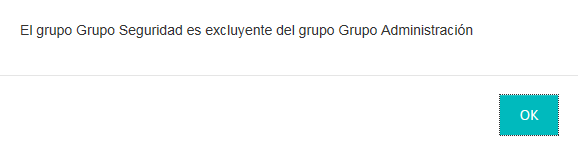
Un rol puede contener:

* Uno o más *Grupos*
* Una o más *Tareas*
* La combinación de ambos

La metodología elegida para configurar los roles en **CIPOL** depende de la forma de trabajo del administrador de la seguridad y de las características propias de cada aplicativo.

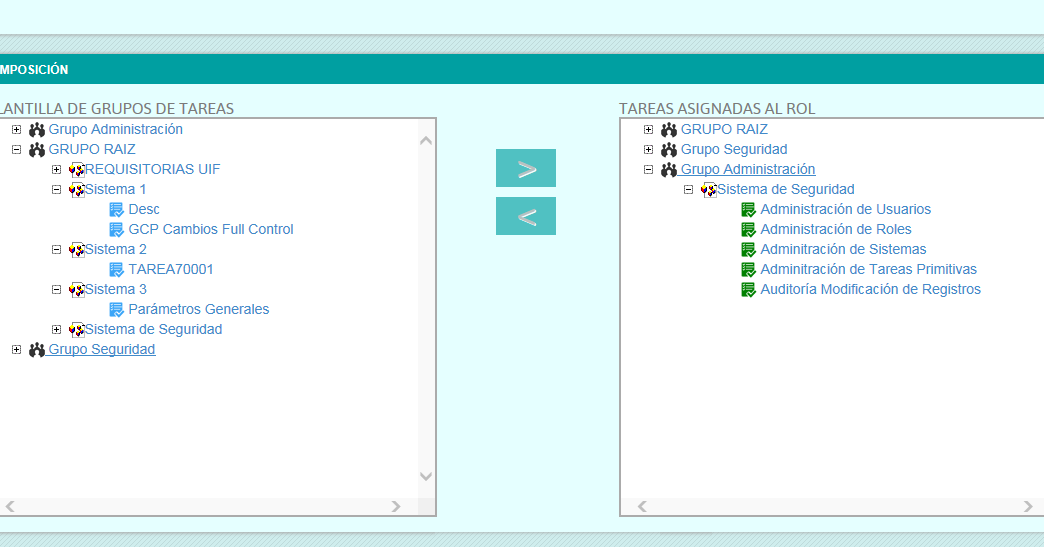
Como se mencionó oportunamente, el esquema de grupos excluyentes sirve para establecer controles, si estos fueron definidos es recomendable utilizarlos en la instancia de generación de roles ya que es allí donde **CIPOL**  verifica que no se transgredan las restricciones.

Si el usuario administrador intenta incorporar dos grupos dentro de un rol, definidos como mutuamente excluyentes, **CIPOL**  mostrará el mensaje:



Mediante este mensaje se advierte que el Rol que se pretende implementar se contradice con las reglas previamente definidas, con lo cual se fuerza a una revisión del esquema propuesto.

Esta función se encuentra disponible al acceder desde el Submenú Sistemas y seleccionar la opción Administración de Roles, el sistema despliega el formulario que permite efectuar las altas, bajas y modificaciones de roles, al ingresar, la pantalla se visualizará de la siguiente manera:



Consta de dos ventanas organizadas mediante un árbol que esquematiza la jerarquía *Grupo – Sistema – Tarea*, con las siguientes características distintivas:

* **Plantilla de Grupos de Tareas**. Contiene las tareas disponibles de todos los aplicativos o sistemas instalados bajo el entorno de seguridad **CIPOL** , ordenadas según el esquema *Grupo – Sistema – Tarea*, mencionado previamente. Cuando el administrador de la seguridad haya optado por no generar *Grupos,* se mantiene el ordenamiento a través del *Grupo Raíz* el cual es el predeterminado para indicar dicha situación.
* **Tareas Asignadas al Rol**. Muestra las tareas asociadas al rol seleccionado en el encabezado, mediante la lista desplegable *Roles Existentes*.

**Consulta:**

Al seleccionar un Rol de la lista de Roles Existentes, las listas de los formularios: Planilla de Grupos de Tareas y Tareas asignadas al Rol, se completaran acorde a los datos que se encuentran asignados en cada lista dependiendo del Rol seleccionado.

Al ingresar a la pantalla, los botones de acción Nuevo, Modificar, Eliminar y Cerrar se encuentran habilitados.

**Botón Nuevo:**

Este botón permitirá registrar un nuevo Rol. Al presionar este botón, se habilitarán las listas, utilizando los botones de asignación se pasará lo seleccionado de una lista a la otra.

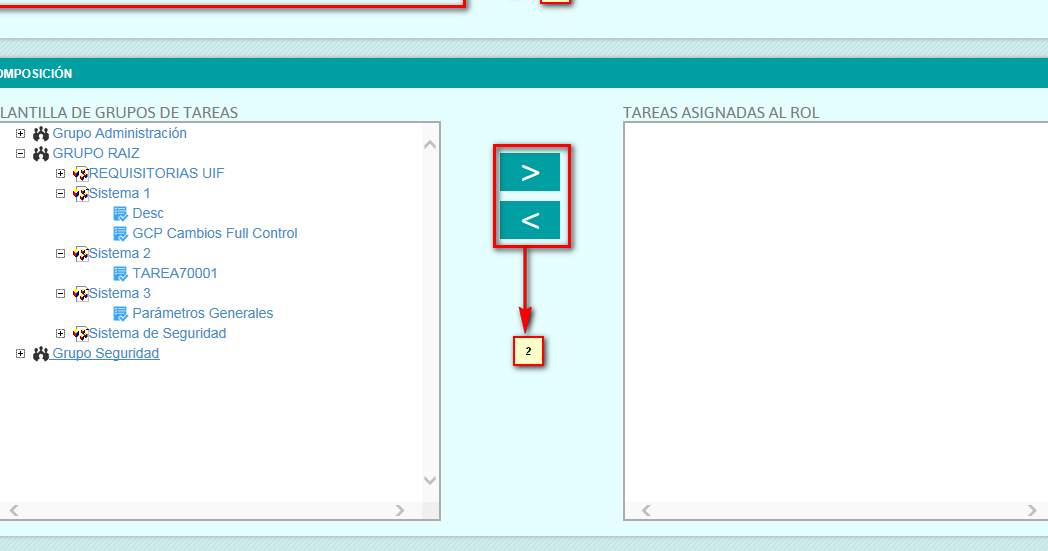
**Botón Modificar.**

Previamente se deberá seleccionar un Rol de la lista desplegable de Roles Existentes que se desea modificar y luego presionar el botón Modificar, el sistema habilita las listas del formulario y los botones de asignación para realizar la modificación necesaria.

**Botón Eliminar:**

Previamente se deberá seleccionar un Rol de la lista desplegable Roles Existentes, y presionando el botón eliminar.

Vista al presionar el Botón Nuevo:

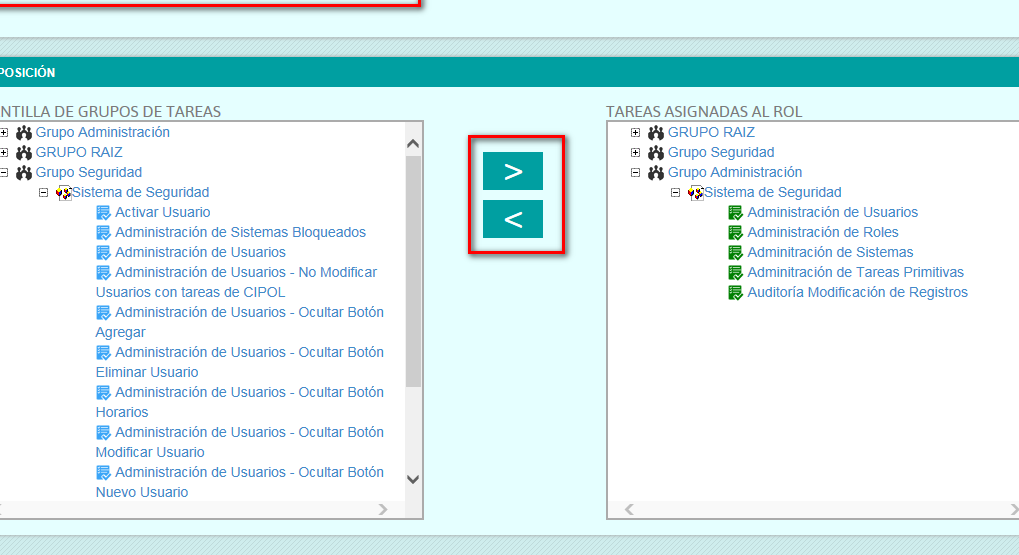


1. Al presionar el botón **NUEVO,** la caja de texto **Roles Existentes** (1), se encuentra en modo editable, en este lugar se debe especificar el nombre del nuevo rol.
2. Con los botones de asignación (2), se selecciona desde la ventana **Plantilla de Grupos de Tareas**, las *Tareas / Grupos / Sistemas* que se desean incorporar al rol, para ello se resalta mediante el mouse el elemento elegido y luego se presiona tecla simbolizada “>” lo cual migrará de ventana a dicho elemento. Esta secuencia se puede utilizar nuevamente para agregar al rol actual nuevas tareas o grupos, hasta completar la configuración del rol.
3. Una vez finalizada la selección se presiona el botón Guardar y el sistema registra los datos ingresados.

El usuario administrador de la seguridad, o en su defecto el usuario al que se delegue la administración de *Roles*, deberá tener en cuenta que la asignación de *Tareas* o *Grupos* para el armado de los *Roles*, requiere del conocimiento de las interfases que componen los aplicativos. Caso contrario puede ocurrir que un *Rol* sea incompleto, esto sucede cuando por ejemplo se incorporan a un *Rol* las *Tareas* asociadas a los objetos que componen una pantalla del aplicativo, pero se omite la que corresponde al ítem de menú para acceder a la misma.

A continuación se ejemplifica la secuencia operativa para la Modificación de un Rol:

1. Seleccionar un Rol de la lista desplegable Roles existentes, y presionar el botón Modificar.
2. Todos los datos en pantalla se encuentran habilitados para realizar las modificaciones necesarias.
3. Una vez finalizada todas las modificaciones, presionar Guardar y el sistema registrará los datos ingresados.



🛈 *Por cuestiones didácticas los ejemplos mostrados para la implementación de Grupos y Roles se realizaron sobre las Tareas del propio sistema* ***CIPOL*** *, siendo extensible la metodología para todos los aplicativos que instalados bajo su entorno de seguridad .*

#### Administración de Usuarios

De manera similar a lo descripto para *Terminales Operativas,* **CIPOL**  mantiene su propio registro de usuarios. Esta función se encuentra disponible al acceder desde el Submenú Sistemas y seleccionar la opción Administración de Usuarios.

En la grilla se provee un resumen de las características usualmente consultadas por el usuario administrador de la seguridad, tales como:

* Cuenta de Usuario
* Nombre y Apellido
* Área a la cual pertenece cada usuario del sistema
* Fecha de baja

En la misma pantalla se disponen, en su parte inferior, el botón de Nuevo usuario. Y dentro de cada renglón para cada uno de los usuarios, se cuenta con los botones de Vista Previa, Modificación y Eliminación.

Adicionalmente, para facilitar la búsquedas, se provee de filtros para facilitar la búsqueda de los registros, y luego visualizarlos en la grilla.

El filtrado actúa sobre los atributos: **Cuenta de Usuario** o **Nombre y Apellido** o **Área** y de acuerdo a los criterios:

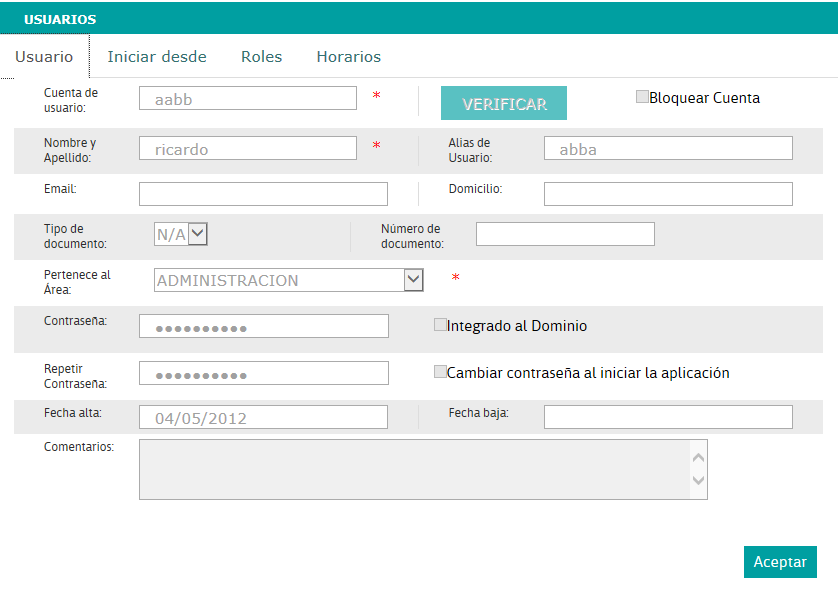
* **que comienzan con:** Selecciona todos los registros cuyo atributo previamente seleccionado comienza con la cadena de caracteres especificada.
* **Filtrar por subcadenas:** Selecciona todos los registros que contiene a la cadena de caracteres especificada.



Los botones: Nuevo, Modificar, Eliminar y Vista Previa pueden ser deshabilitados (ocultos) por medio de la asignación al usuario de la Tarea correspondiente.

**Consulta:**

Al seleccionar un usuario de la grilla, y presionar el botón Vista previa se puede acceder al detalle del usuario, donde se muestran todos sus datos. Además se podrá acceder a las opciones Iniciar Desde, Horarios y Roles para visualizar los datos del mismo en cada una de las opciones señaladas. Todos estos datos como los que se encuentran en cada uno de los botones también se encuentran en modo no editable.

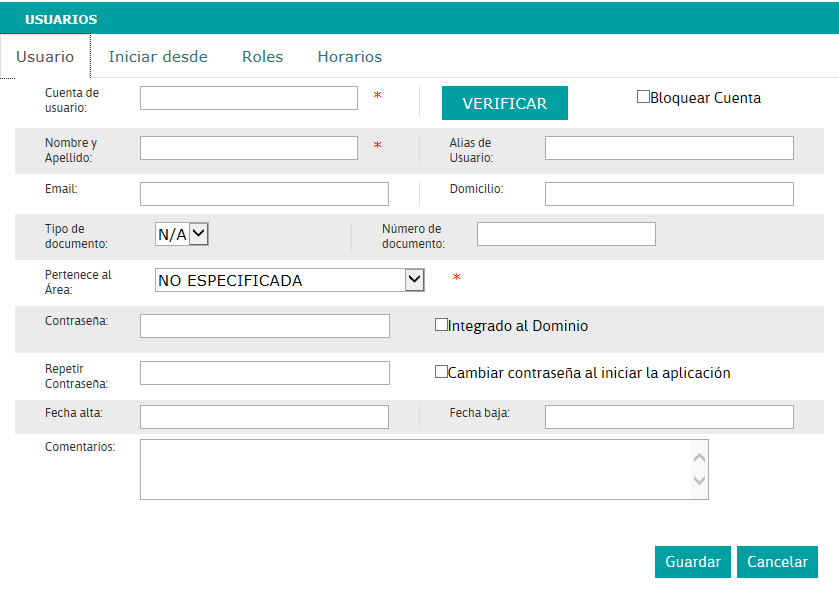


Los botones: “Iniciar Desde”, “Horarios” y “Roles” pueden ser deshabilitados (ocultos) por medio de la asignación al usuario de la Tarea correspondiente.

**Botón Nuevo:**

Al presionar el botón **Nuevo** se inicia la secuencia de alta de una cuenta de usuario, abriendo un Pop-Up para cargar los datos del nuevo usuario.

Este botón permitirá registrar un nuevo usuario. Al presionar este botón, se habilitarán todos los campos, además en los botones Iniciar Desde, Horarios y Roles, también se encuentran habilitados para ingresar datos, según corresponda en cada caso.



🛈 *Al efectuar el alta de una cuenta de usuario, el administrador debe comunicar el nombre de la cuenta y la contraseña preestablecida a la persona que hará uso de la misma. Por esta razón se activa la casilla “Cambiar contraseña al iniciar la aplicación”, para obligar al nuevo usuario del sistema a especificar una nueva contraseña que sea sólo de su conocimiento .*

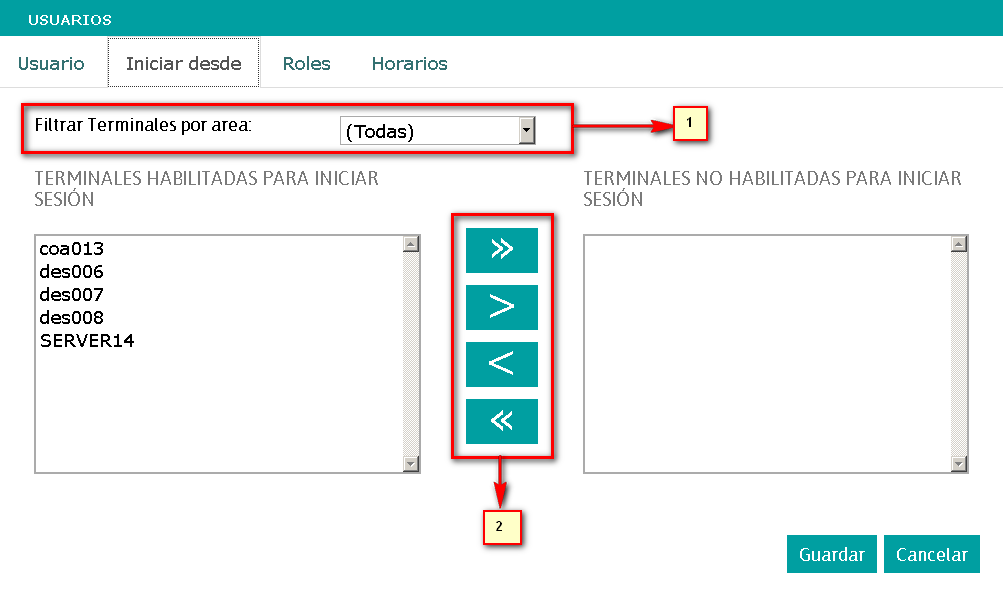
Al marcar la opción Integrado al Dominio, el botón Verificar se habilita, y se inhabilita los campos Contraseña y Repetir Contraseña.

Descripción de las acciones que realizan cada uno de los botones de la pantalla.

**Verificar:** Este botón verifica si el usuario ingresado se encuentra integrado al dominio o no. Este botón solo estará disponible para cuando el sistema se encuentra integrado al dominio, de lo contrario se visualizará inhabilitado.

**Iniciar Desde:**

En forma predeterminada **CIPOL**  permite que un usuario inicie una sesión desde cualquier terminal que se encuentre previamente habilitada. No obstante, mediante esta opción es posible inhibir el uso de terminales por parte del usuario.



1. Seleccionado un área en la sección **Filtro de terminales por Área (1),** se listan las terminales que se encuentran asignadas en el área seleccionada.
2. Mediante los botones de asignación (2), es posible seleccionar la/las terminales en las cuales se desea que el usuario no inicie sesión. Se podrá seleccionar una o más terminales de la lista.
3. Finalizada la selección se presiona el botón Guardar y se registra las actualizaciones para el usuario.

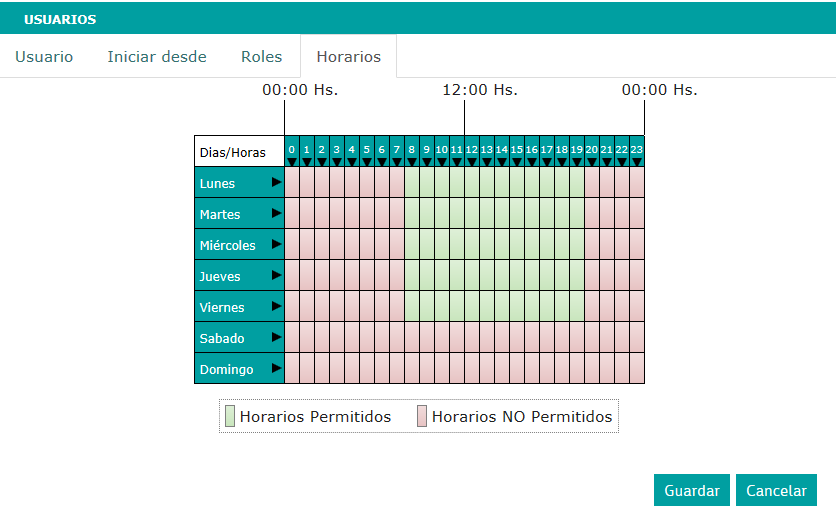
🛈 *La restricción del uso de terminales es particularmente útil cuando se desean establecer áreas restringidas en las que los aplicativos sólo sean accedidos por el personal asignado a ella.*

**Horarios**

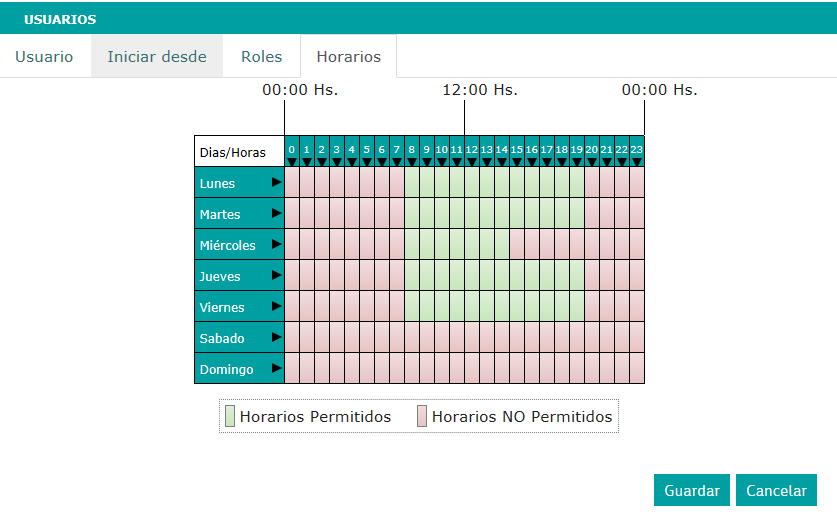
Al seleccionar esta función **CIPOL**  ofrece un cuadro a modo de plantilla horaria, como el que se muestra a continuación donde se aprecia una cuadrícula dividida:

* Sector verde: Horario Permitido
* Sector rojo: Horario NO Permitido.

Es posible establecer un horario personalizado para la cuenta de usuario actualmente editada.

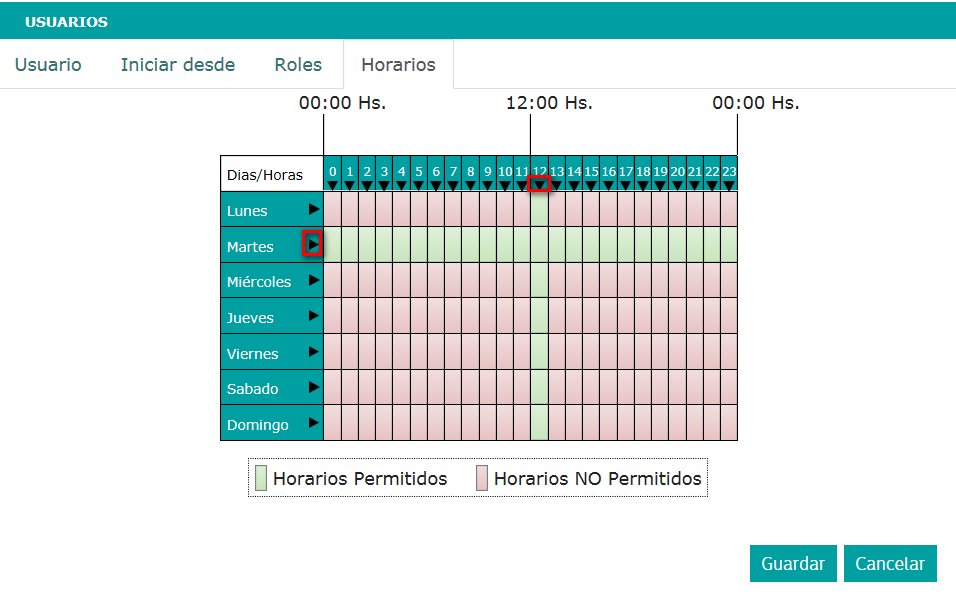


Para ello se dispone del puntero del mouse, simbolizado por una mano señalando, con el cual se pueden seleccionar cuadrículas a los efectos de **Permitir** o **No Permitir** la adición del nuevo sector al horario actual.



En la última figura ejemplificamos una disminución del horario admitido para los inicios de sesión de la cuenta de usuario editada.

A fin de facilitar la carga de varios horarios, el usuario puede presionar sobre las flechas presentes en cada día y en cada hora. Con esto provocará que toda la fila (o columna) se habilite o deshabilite según corresponda.



Finalizada la selección, presionar **Guardar** y los datos ingresados se graban, y retornan a la pantalla principal de la administración de usuarios.

**Roles**

Esta función de **CIPOL**  implementa las altas, bajas y modificaciones de permisos sobre los aplicativos, para la cuenta de usuario editada, mediante la asignación de los *Roles* previamente configurados por el administrador de la seguridad.

Al presionar **Roles** se accede a la ventana:

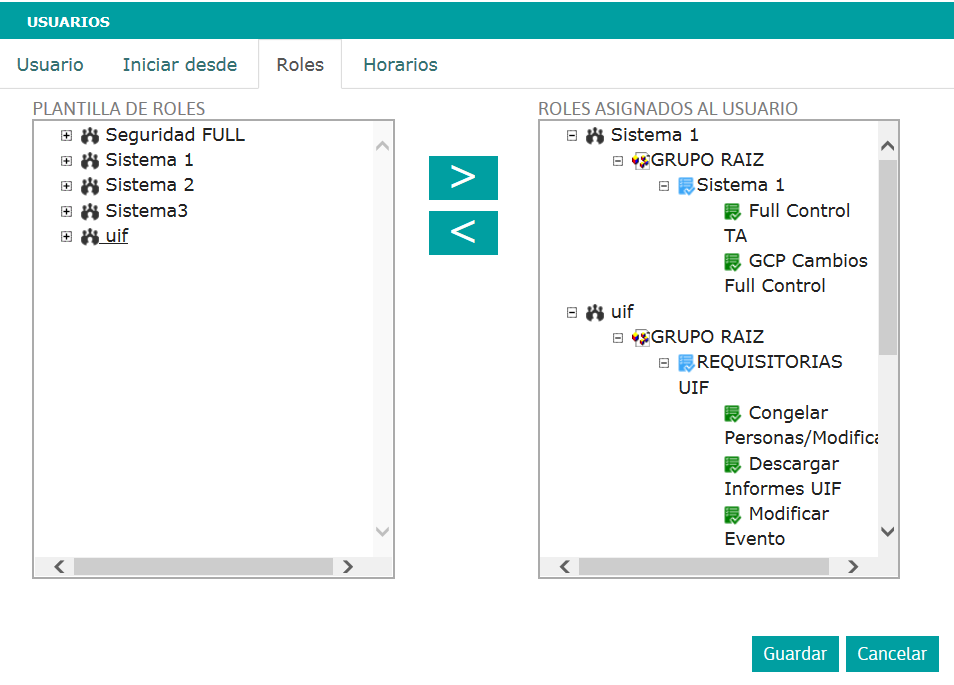


En la lista Plantilla de Roles, se listan los *Roles* disponibles, a través de una estructura jerárquica en árbol.

1. La asignación de roles al usuario, consiste en la selección de cada uno de los *Roles* deseado presionando los botones de asignación (1).

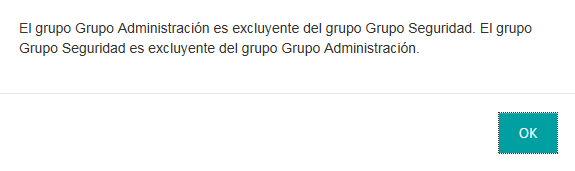
Se pueden seleccionar uno o más de un rol para el mismo usuario.

En la siguiente figura se muestra el perfil de un usuario que posee dos roles a modo de ejemplo.



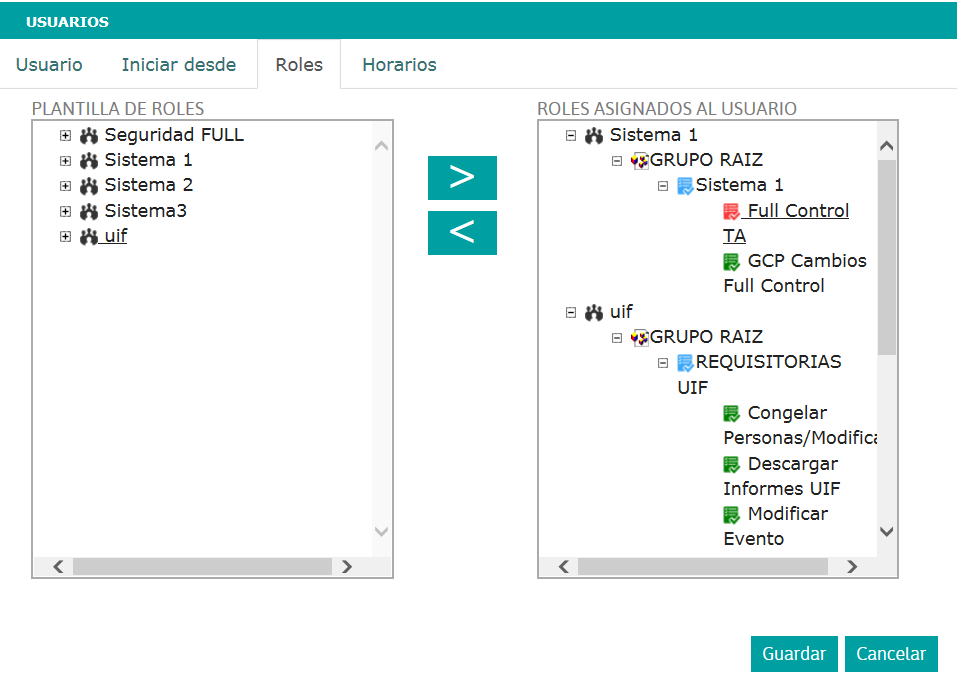
A continuación observamos que no es posible asignar *Roles* que provienen de *Grupos* excluyentes. Es decir, el usuario administrador de la seguridad diseño un esquema de *Grupos* de manera tal de impedir la acumulación de funciones operativas sobre un mismo usuario. Esto implica que los *Roles* que son incompatibles a través de la herencia que plantean los *Grupos* excluyentes, deben ser asignados a distintos usuarios planteando el concepto de “control por oposición de funciones”.

El sistema detecta que se asignaron roles de grupos excluyentes y muestra le mensaje que se observa a continuación:



Es importante destacar una situación que se produce al agregar una *Tarea* a un Rol existente. Si este *Rol* ya ha sido asignado a cuentas de usuario, **CIPOL**  actúa en forma *restrictiva* en el sentido de que no habilitará el uso de la tarea hasta que el usuario administrador de la seguridad lo active manualmente. En la siguiente figura se aprecia el efecto mencionado:

El sentido de esta característica es evitar que una modificación en los Roles existentes tenga un impacto no deseado sobre los permisos adjudicados a todos los usuarios del sistema. Para habilitar la *Tarea,* en las cuentas de usuario que correspondiera, se deberá hacer doble clic sobre ella provocando el cambio del ícono tal como se observa:



De manera inversa, este procedimiento es aplicable en los casos en que se desea restringir el uso de algunas tareas que componen un *Rol* que se asignó a una cuenta de usuario. Para ello bastará con **Modificar** la cuenta de usuario, seleccionar **Roles**, desplegar el árbol jerárquico en la lista **Roles Asignados al Usuario**, identificar la Tarea que se quiere inhibir y hacer doble clic sobre ella, el efecto se visualizará por el cambio en el ícono.

Para aplicar el cambio producido, se debe presionar **Guardar.**

🛈 *Inhibir el uso de Tareas permite al administrador hacer rápidamente ajustes en el perfil de seguridad de los usuarios, aunque no es recomendable abusar de este recurso ya que se pierde claridad .*

Una vez finalizada todas las actualizaciones, presionar el botón Guardar, para registrar en el sistemas la información ingresada.

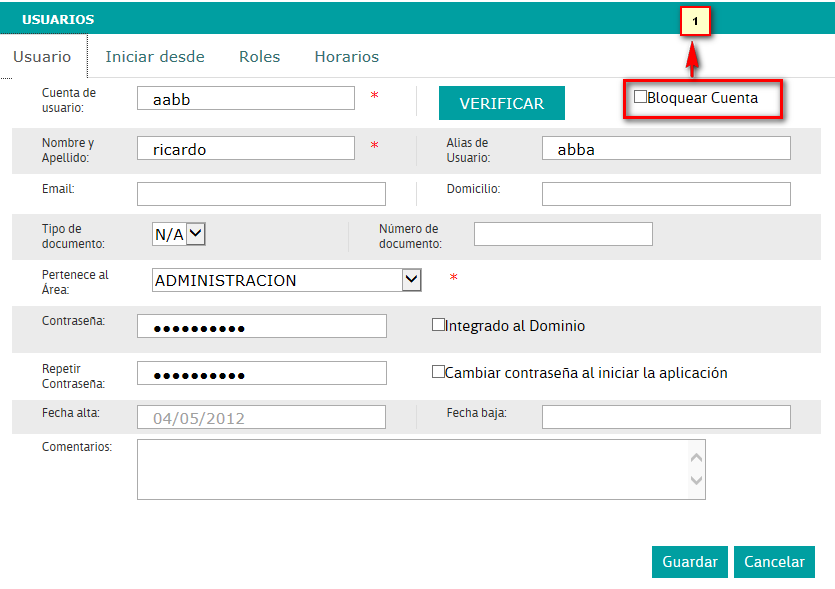
Otros campos:



1. **Fecha Alta:** Este campo se completa al presionar el botón Guardar.
2. **Integrado al Dominio:** Al seleccionar esta opción el botón Verificar se activa.
3. **Botón Guardar:** al presionar este botón en el alta se registra todas las actualizaciones de los datos ingresados.

**Botón Modificar.**

Previamente se deberá seleccionar un Usuario de la grilla, y presionar el botón Modificar, el sistema habilita los campos para realizar las modificaciones necesarias, como así también los botones: Iniciar Desde, Horario y Roles. La pantalla se visualizará como muestra la siguiente imagen:

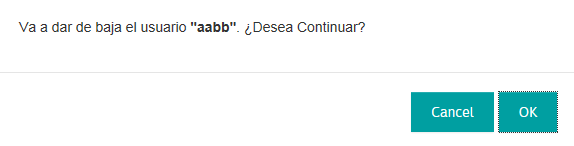


El check marcado con 1 en la pantalla tiene el siguiente funcionamiento.

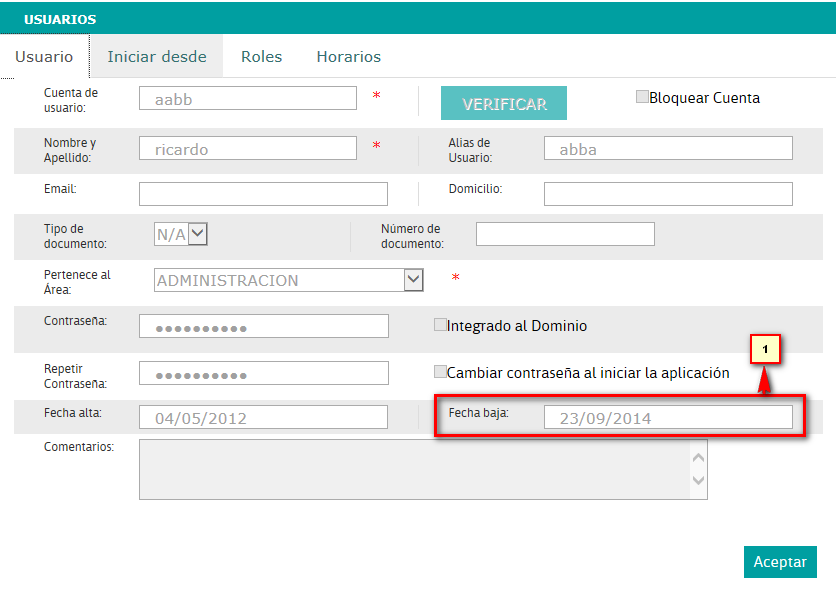
1. **Bloquear cuenta:** Permite al administrador bloquear una cuenta de usuario, seleccionando una fecha hasta la cual se encontrará bloqueada la misma. Si se ingresa desde la grilla anterior mediante el botón Modificar y esta se encuentra previamente tildada, significa que se alcanzó el tope admitido de algunos de los parámetros de seguridad relacionados, por ejemplo la cantidad máxima de intentos de inicio de sesión erróneos.

**Botón Eliminar:**

Previamente se deberá seleccionar un Usuario de la grilla y presionando el botón eliminar. El sistema muestra el siguiente mensaje:



Visualización del Detalle del registro eliminado.



El campo marcado con 1 en la pantalla presenta el siguiente funcionamiento.

1. **Fecha Baja:** Este campo se completa cuando al seleccionar un usuario de la grilla se presiona el botón eliminar.

🛈 *La Eliminación de cuentas de usuario es en realidad una baja lógica, esto es, se le asocia la fecha actual como fecha de baja de la cuenta, quedando inhibida para operar los sistemas. De esta manera se garantiza la disponibilidad de los datos asociados a cuentas de usuario que poseen registros de auditoría en el sistema.*

**Botón Activar:**

Al seleccionar un registro que tiene fecha de baja, el botón Eliminar se modifica por Activar.



Al presionar el botón Activar, el sistema habilita nuevamente el usuario.

🛈 *Si bien es posible efectuar todas las tareas de administración de la seguridad mediante el uso de la cuenta de usuario”master”, se recomienda que sólo sea utilizada en la configuración inicial de todo el entorno, cambiando luego la contraseña y procediendo a su almacenamiento. Previamente se deberá delegar en uno o más usuarios todas las actividades relacionadas con la seguridad.*

*De esta manera,* ***CIPOL***  *registrará en su esquema de auditoría a cuentas de usuario que se corresponden con personas físicas, evitando inconvenientes en la identificación de responsables.*

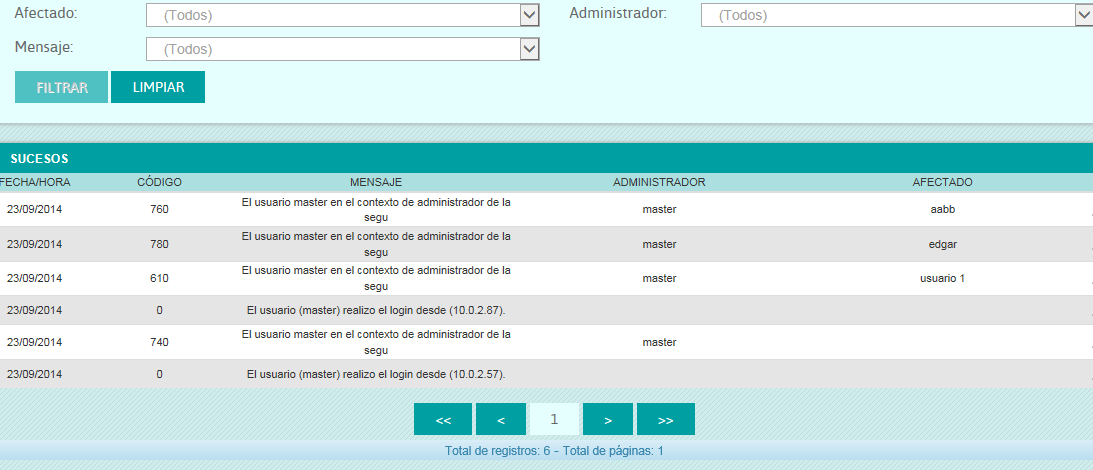
## Visor de Sucesos

Los eventos relacionados con la seguridad son registrados en **CIPOL**  en una estructura de datos acorde a las necesidades del administrador en cuanto al análisis y control de los mismos.

Para ello **CIPOL**  implementa el **Visor de sucesos Seguridad**, al cual se accede de la siguiente manera:



Desplegando la siguiente pantalla:



Esta ventana consta de dos áreas:

* **Filtros:** Los mismos se encuentran en la parte superior de la pantalla
* **Sucesos:** Donde se listan los registros que coinciden con los datos ingresados en los filtros.

Al iniciar por primera vez, la grilla de sucesos se encuentra vacía hasta realizar un filtrado.

La aplicación de los Filtros consta de tres criterios, estos son:

* **Fecha** Compuesto por los delimitadores **Desde** y **Hasta**. Como su nombre lo indica, se trata simplemente de establecer un entorno en el que se desea efectuar un análisis.
* **Usuarios** Consta de dos componentes:
  + **Administrador:** Es quien realizó alguna actividad en **CIPOL**
  + **Afectado:** Representa la cuenta *sobre* la que se efectuó alguna actividad.

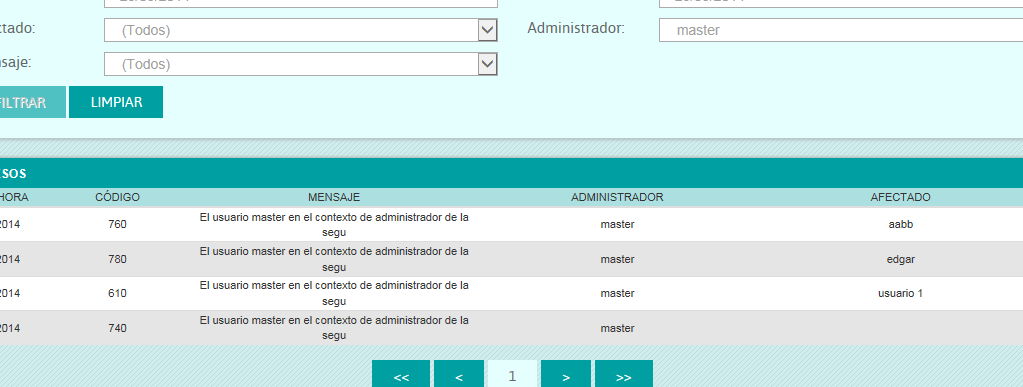
Un caso típico es cuando el administrador de la seguridad cambia la contraseña de un usuario a partir de una solicitud por no recordarla.

* **Mensaje** Permite la selección uno o más códigos de mensaje, de acuerdo a la tipificación implementada para los eventos.

Estas opciones son acumulativas, lo cual permite acotar la búsqueda mediante la utilización simultánea de todos los criterios.

**Botón Filtrar:**

Una vez ingresado los datos en los filtros y presionar este botón Filtrar, el sistema muestra en la grilla los datos que coinciden con los datos ingresados en los filtros.



**Botón Limpiar:**

El botón **Limpiar** vuelve al estado inicial, o sea limpia la grilla de sucesos y resetea los valores de los filtros tal como lo hace al ingresar por primera vez.

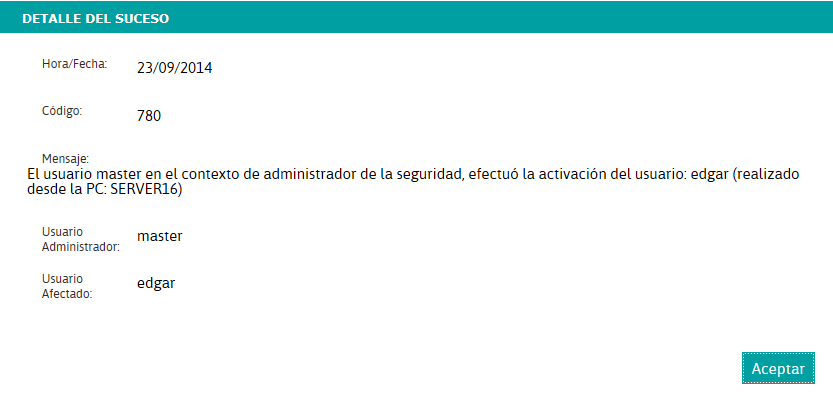
**Botón Imprimir:**

Al presionar este botón, el sistema imprime todos los registros que coinciden con los datos ingresados en los filtros.

El reporte se emite en una nueva ventana.

**Botón Ver Mensaje:**

Este botón está presente para cada suceso de la grilla. Al presionarlo, el sistema genera una ventana con el detalle del mensaje asociado al registro de seleccionado de la grilla, tal como se muestra:



## Reportes

Esta opción presenta los reportes que dispone **CIPOL** para consulta de la información que administra. Proporcionan una herramienta muy útil para las actividades diarias del usuario Administrador de la Seguridad.

Al seleccionar la opción del menú, se despliega la lista con los reportes disponibles



Específicamente, proporciona vistas de las configuraciones de la seguridad, las que se detallan a continuación:

* **Usuarios por Roles** Permite conocer cuáles usuarios tienen asociado un determinado *Rol,* proporcionando información adicional como la fecha y usuario que se lo otorgó, y si lo posee con todas las tareas habilitadas o parcialmente.

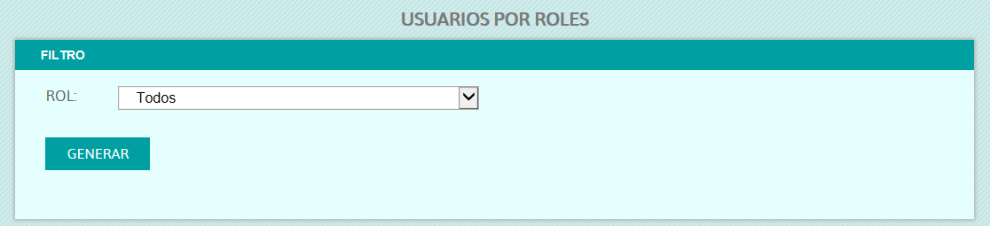
También permite generar un informe detallado con la descripción de las Tareas Asignadas e Inhibidas.

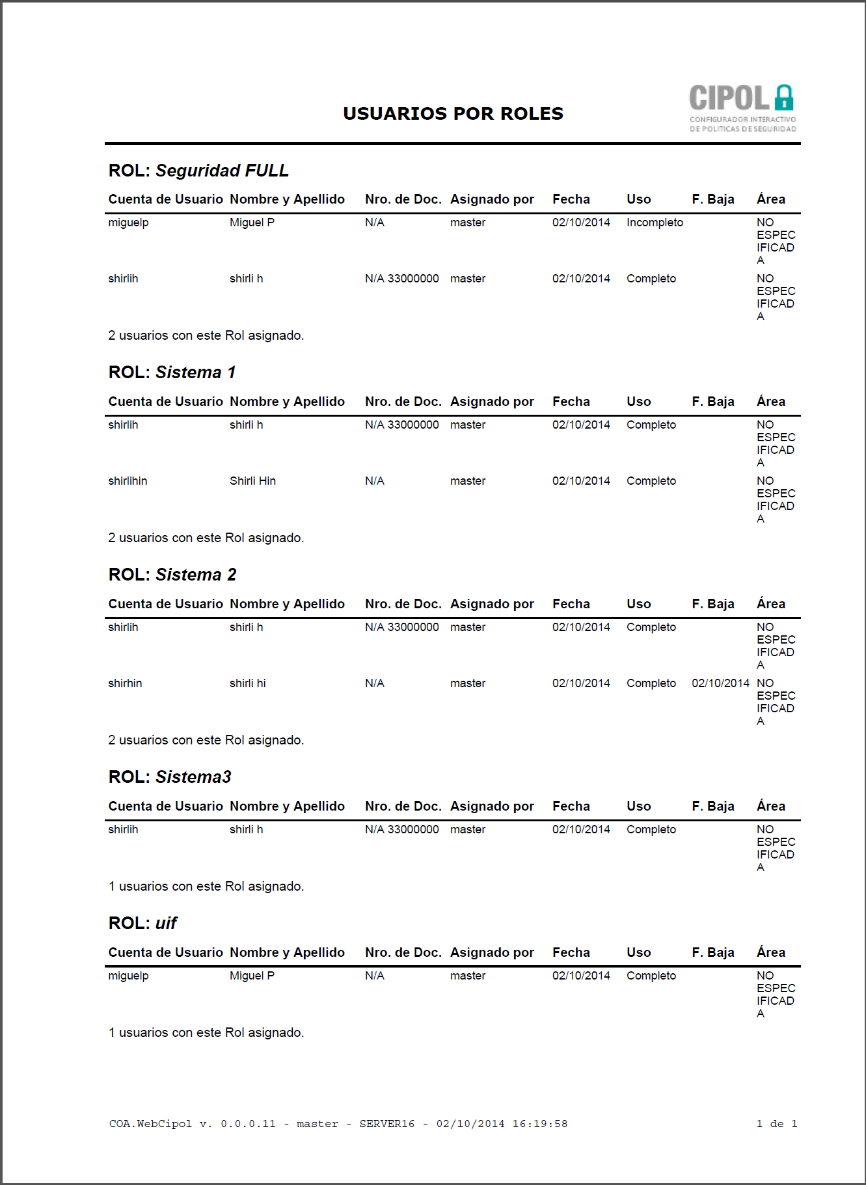
* **Usuarios por Áreas** Permite conocer cuáles son los usuarios asociados a un *Área* determinada, proporcionando información adicional como la cuenta el Usuario, Nombre, Documento, Fecha de Alta y Baja del usuario al área seleccionada.
* **Roles por Usuarios** Es el criterio inverso al reporte de *Usuarios x Roles*, es decir, muestra información relacionada con la cuenta de usuario y los Roles que posee al momento de la emisión.

Permite generar, además, un informe detallado con la descripción de las Tareas Asignadas e Inhibidas.

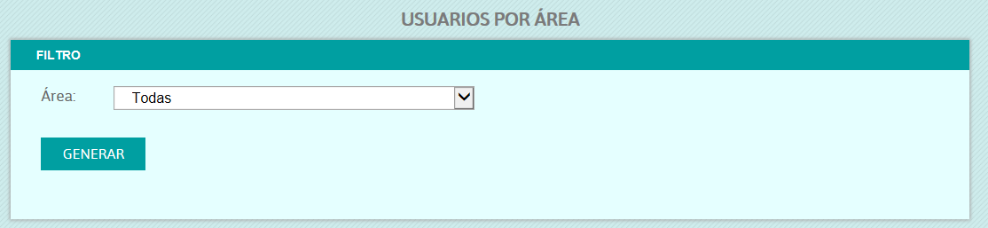
* **Descripción de Roles** Muestra las tareas, y su sistema asociado, que componen un Rol seleccionado.
* **Áreas** Muestra las áreas registradas en el sistema, activas o eliminadas, y además información adicional tal como los Responsables del Área y Cargo del Responsable.
* **Terminales** Permite conocer las terminales que se encuentran habilitadas por áreas. También proporciona información adicional sobre el Código y Nombre de la terminal, como así también datos relacionados con el hardware de la máquina.
* **Usuarios** Muestra información de los Usuarios del sistema, tal como: Horarios habilitados, Cuenta de Usuario, Documento, Área, Terminales de acceso, Roles asignados, Fecha de Alta y Baja.
* **Usuarios sin Acceso** Muestra la información de los Usuarios que se encuentran sin acceso. Se puede seleccionar entre los estados *“Bloqueado*”, *“Baja”* y *“Bloqueado y Baja”.* Permite ver información adicional del usuario y la *Fecha del Bloqueo y/o Fecha de Baja* del mismos al sistema*.*
* **Control de Inactividad** Permite efectuar el control de inactividad de los usuarios en el sistema, los cuales se encuentran ordenados por áreas. Además, muestra información adicional tal como: cuando fue la última sesión, área a la que pertenece y datos complementarios de los mismos.

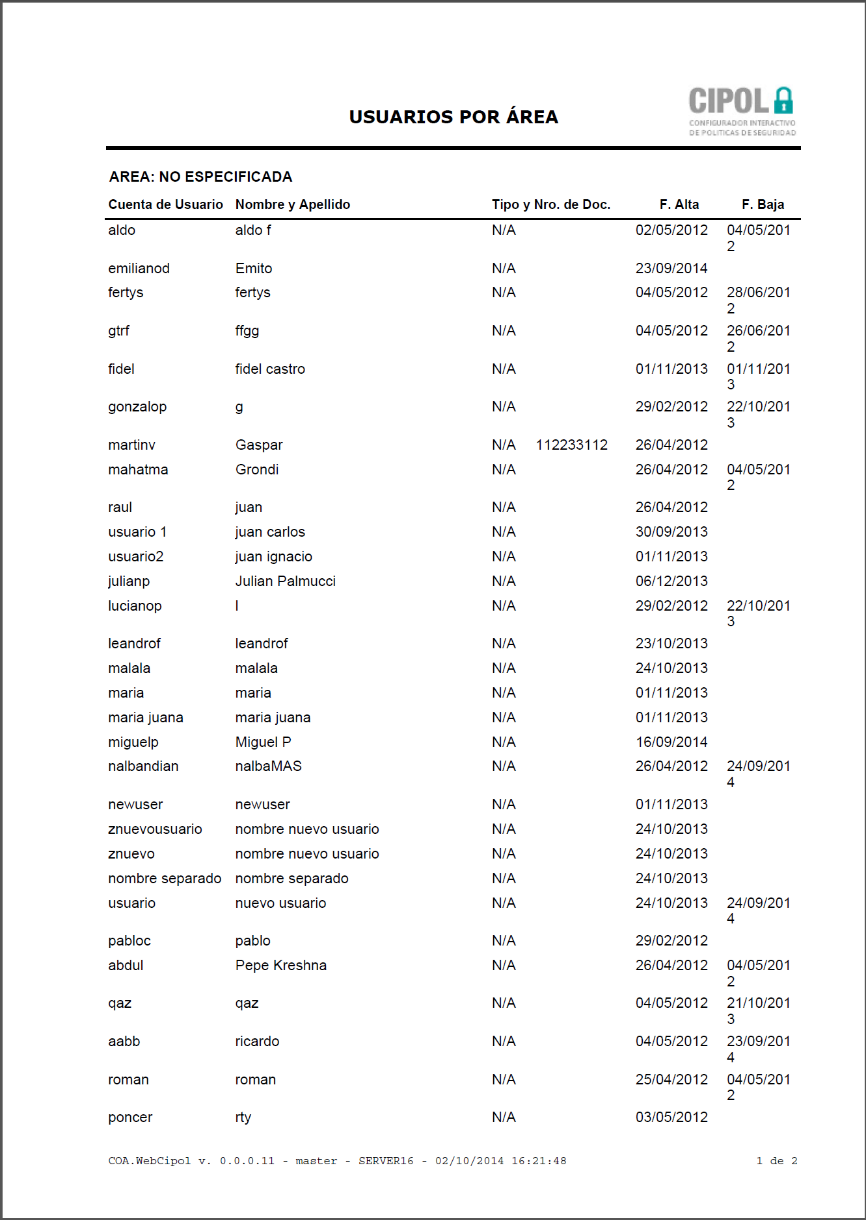
#### Listado: Usuarios por Roles



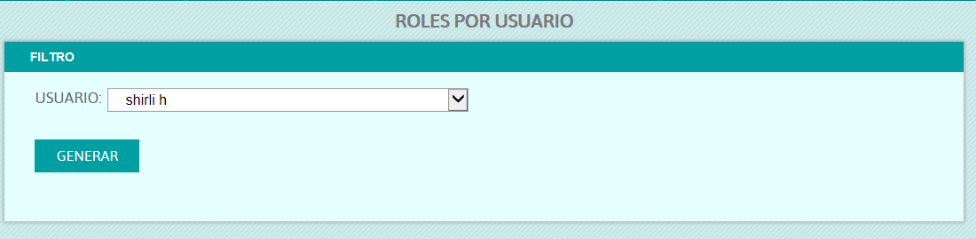


#### Listado: Usuarios por Áreas



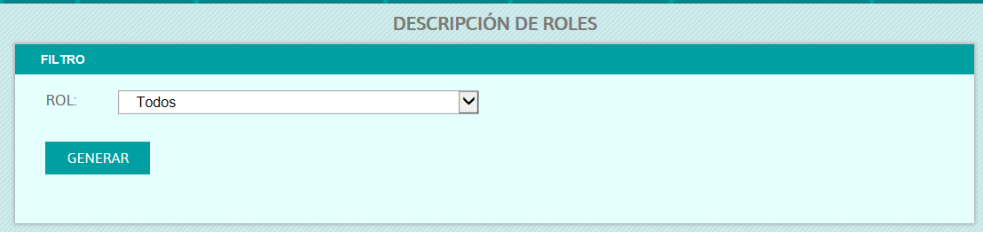


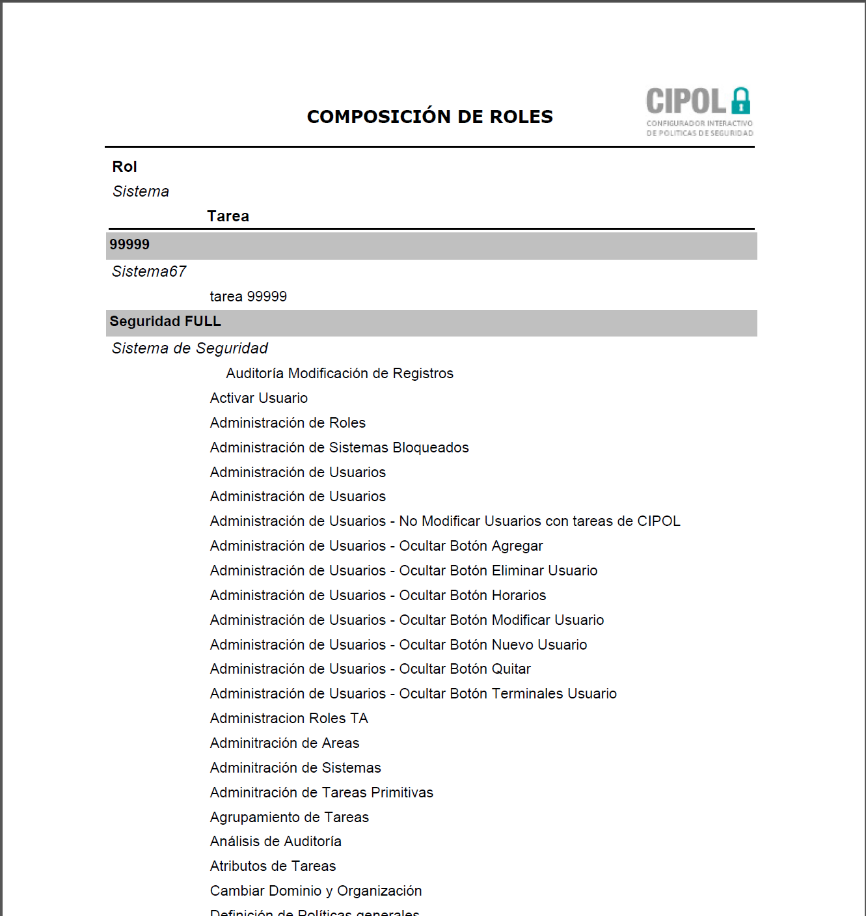
#### Listado: Roles por Usuario



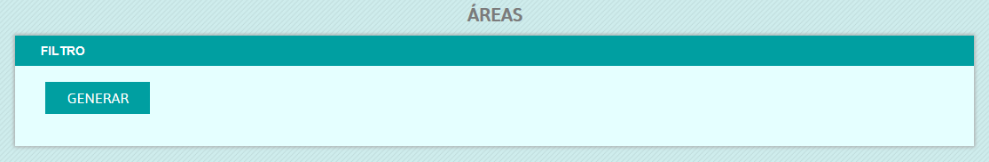


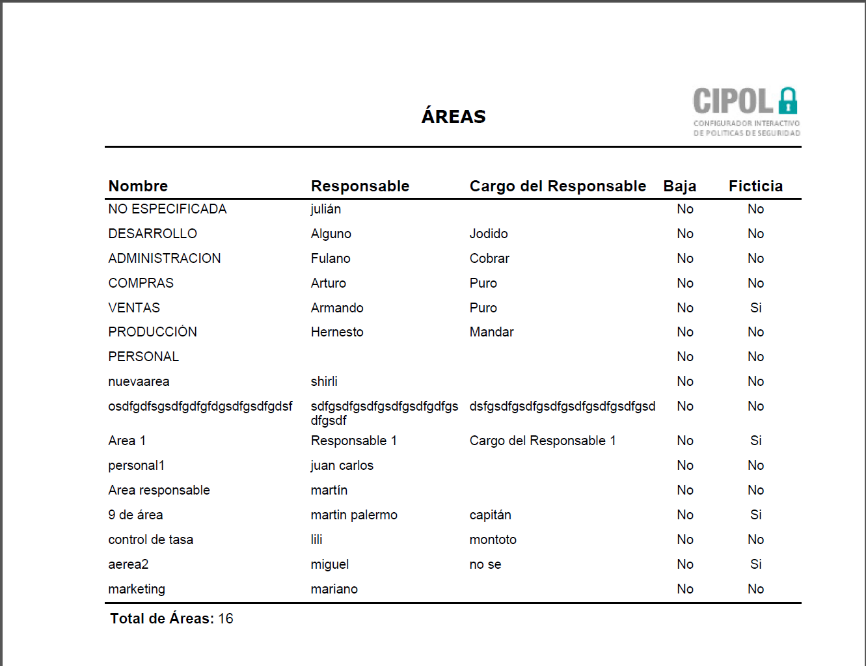
#### Listado: Composición de Roles



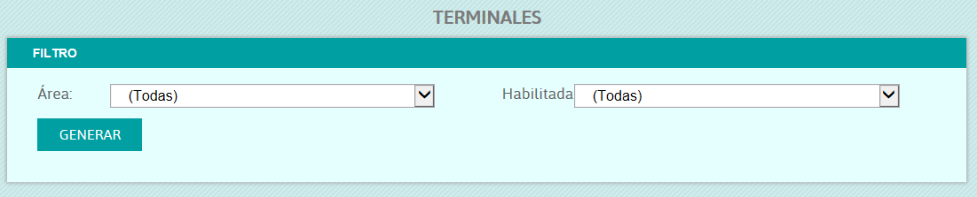


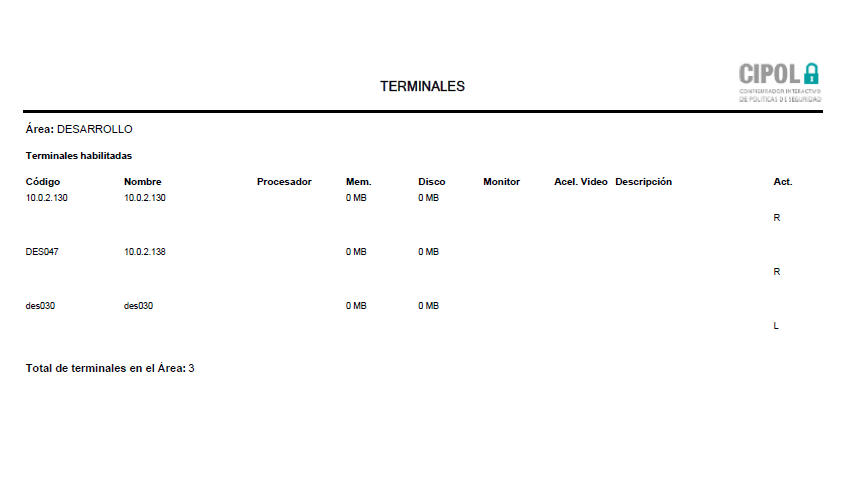
**Listado: Áreas**





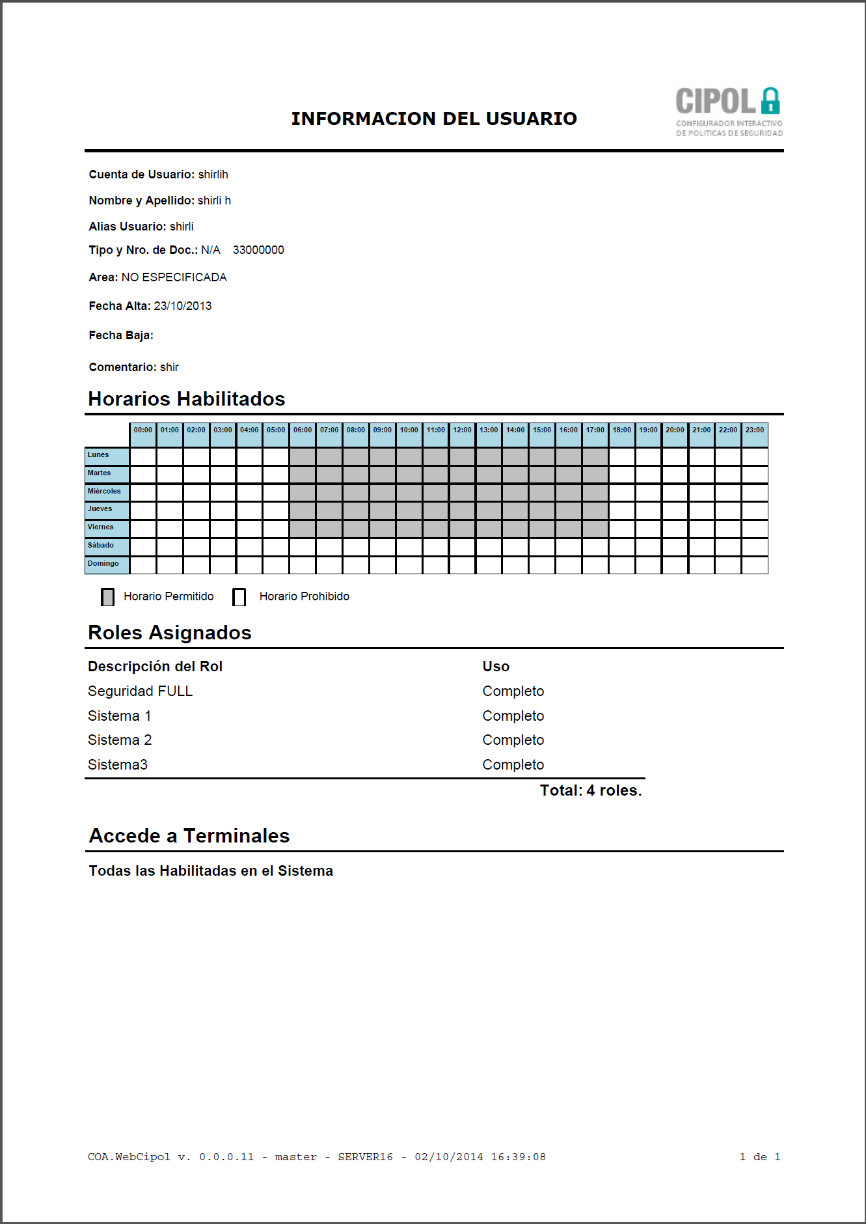
#### Listado: Terminales





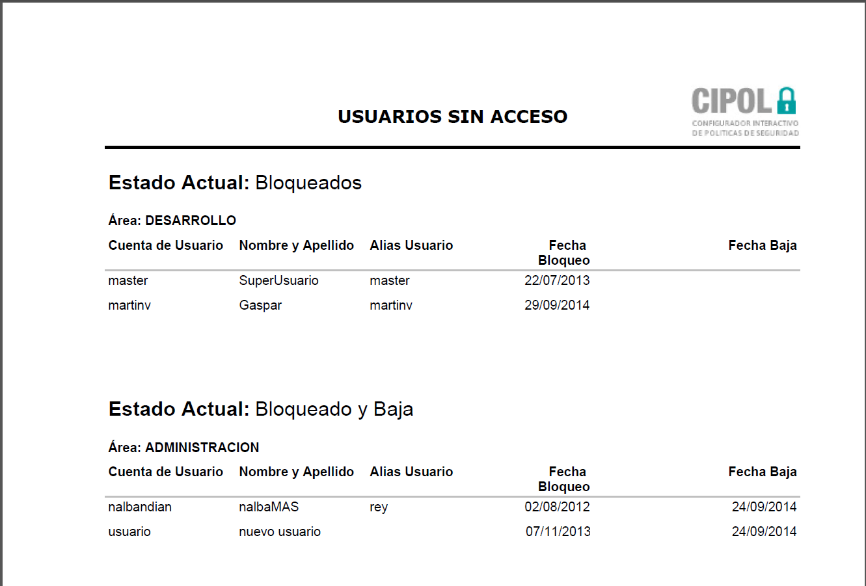
#### Listado: Usuarios



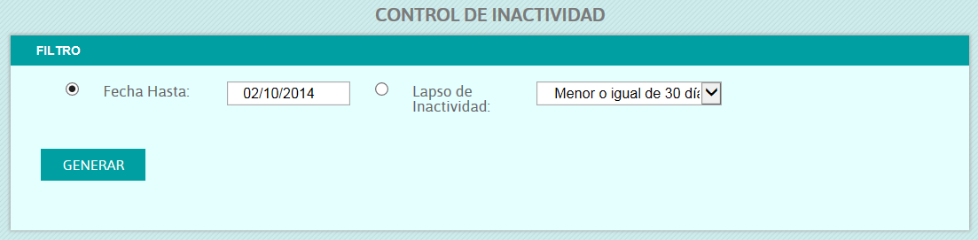


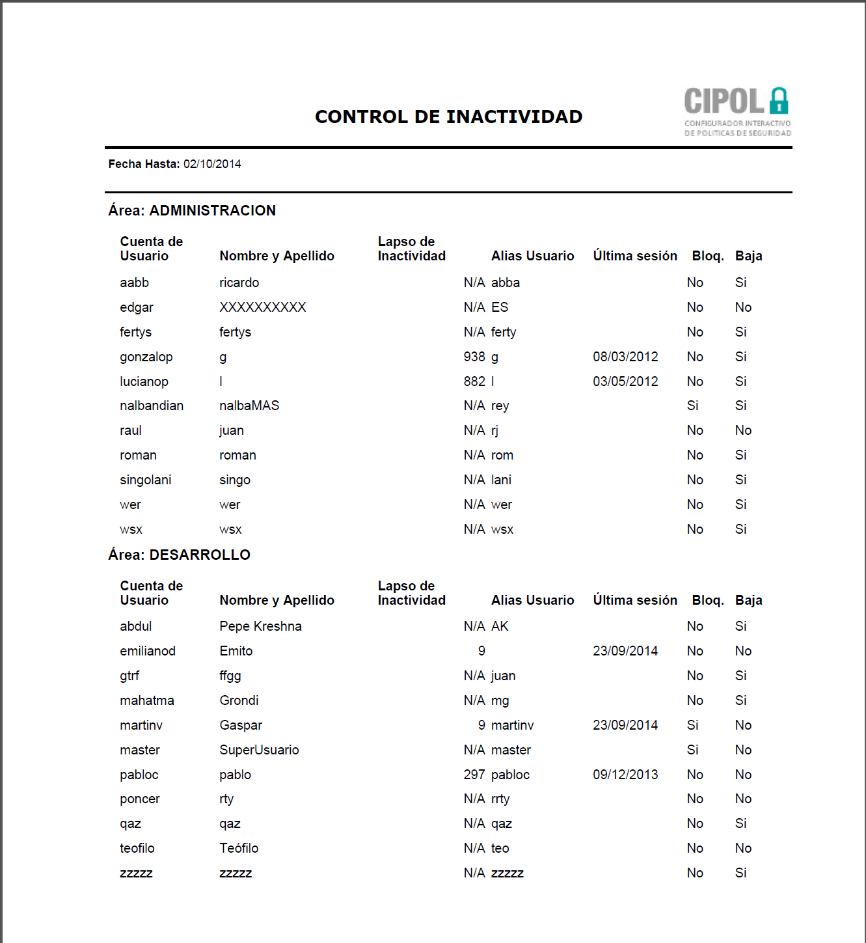
#### Listado: Usuarios sin Acceso





#### Listado: Control de Inactividad





🛈 *El control de inactividad está estrechamente vinculado con las políticas de seguridad de la empresa y/o entidades rectoras, en el sentido de que permite detectar las cuentas de usuario que deben ser bloqueadas o dadas de baja.*

## Herramientas

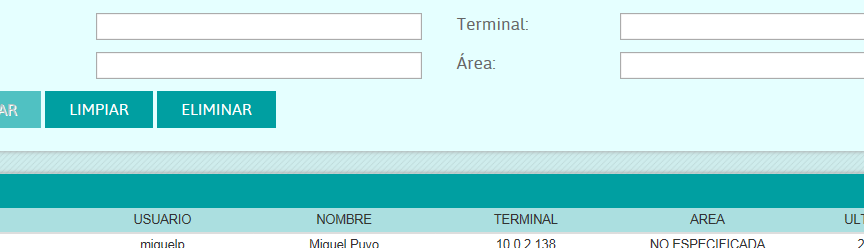
**CIPOL**, en la opción **Herramientas**, ofrece opciones de control y de definición de parametría para configurar el uso de los aplicativos..



#### Monitor de Actividades

**CIPOL** ofrece en la opción **Monitor de Actividades** una herramienta de control de las sesiones de usuarios activas en el sistema.

Esta opción se encuentra disponible en el submenú Herramientas. Permite al operador verificar cuántos y qué usuarios están actualmente operando alguno de los sistemas controlados por **CIPOL** . Al seleccionarla despliega una pantalla como la siguiente:



**Botón Eliminar:**

Seleccionar un registro de la grilla y presionar el botón Eliminar,el sistema borra el registro de la base de datos, permitiendo al usuario volver a operar el sistema.

Esta capacidad será de utilidad cuando alguno de los sistemas haya terminado de manera anormal su ejecución y como consecuencia de ello, **CIPOL**  inhiba cualquier otra operación del usuario afectado o no permita ejecutar los sistemas en el puesto en cuestión.

Su uso debe ser controlado ya que si se elimina un registro de actividad, se estarán eliminando referencias de control que el propio **CIPOL**  utiliza para aplicar algunas de las políticas de seguridad implementadas.

**Botón Filtrar:**

Se utiliza para realizar una búsqueda a partir de los datos ingresados en los filtros. Tener en cuenta que el sistema no refresca por defecto el contenido de la grilla continuamente.

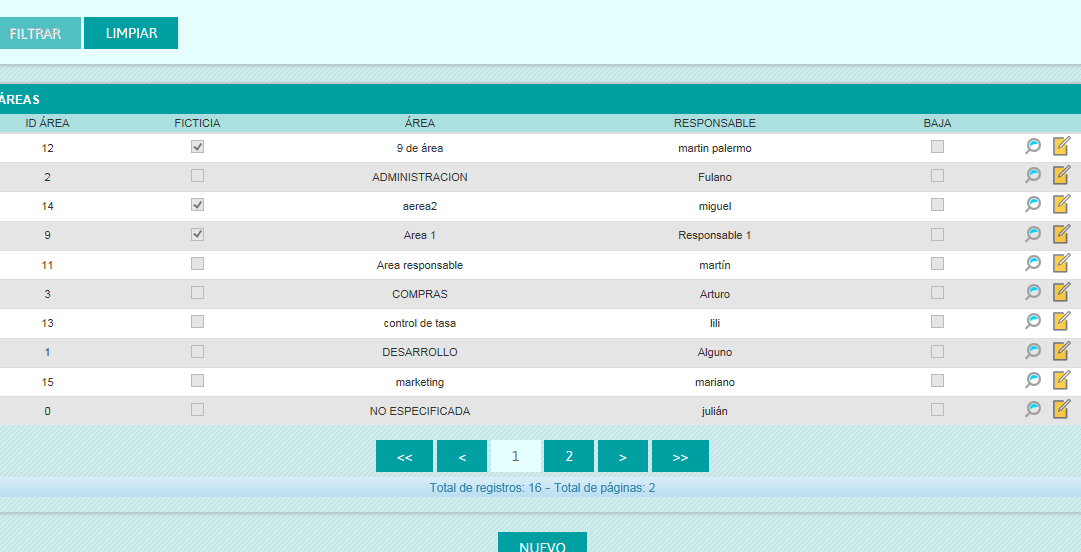
**Limpiar Filtros:**

Permite borrar las opciones de filtrado ingresadas hasta el momento y además realizar una nueva búsqueda cuando ya se ha realizado una previamente.

#### ABM de Áreas

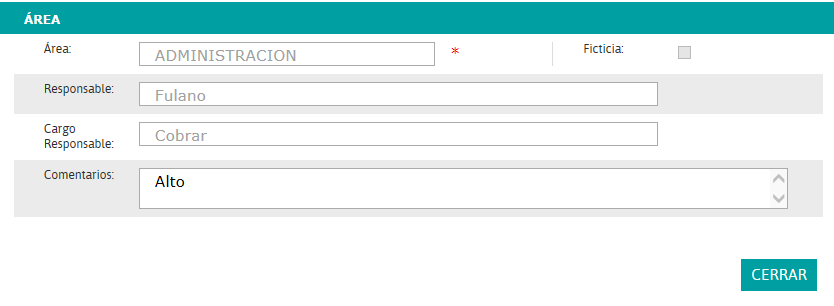
Al seleccionar del submenú Herramientas el ítem de menú **ABM de Áreas**, **CIPOL**  despliega un filtro y una grilla donde se listarán las áreas actualmente registradas en el sistema y permite operar de la manera típica de un ABM, a los efectos de gestionar la habilitación de las mismas.

En la siguiente figura se muestra la pantalla:



**Consulta:**

Al seleccionar un registro de la grilla, y presionar su respectivo botón “Vista Previa” se muestra una pantalla con los datos del registro seleccionado.



Aquí no se podrá realizar ningún tipo de búsqueda.

**Botón Nuevo:**

Este botón permitirá registrar una nueva Área. Al presionar este botón se abre una pantalla donde todos los campos se encuentran habilitados para ingresar los datos correspondientes en cada campo.

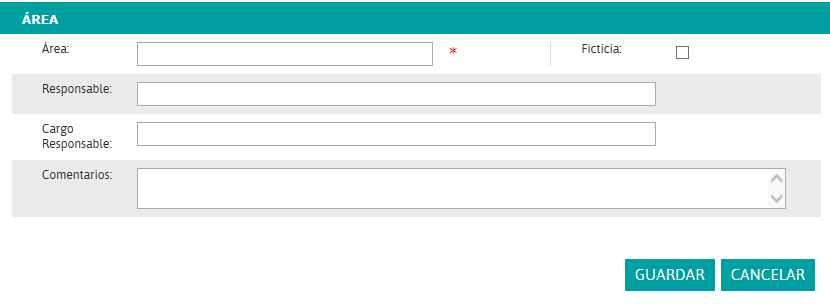
**Botón Modificar.**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema muestra una ventana con los campos habilitados en modo de edición para realizar las modificaciones necesarias.

**Botón Eliminar:**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema da de baja lógica el registro. En la columna Baja, se mostrará un tilde en aquellas áreas que están dadas de baja.

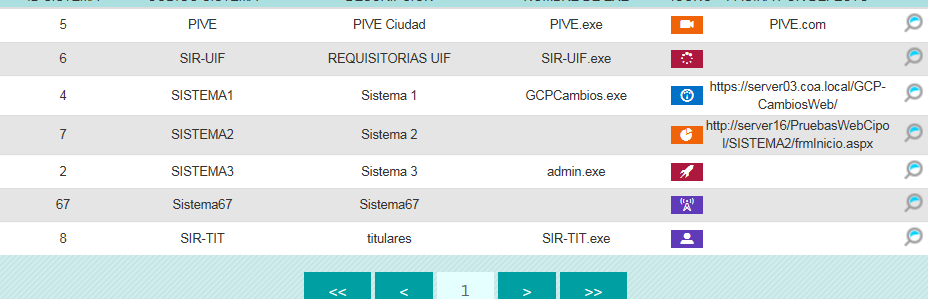
La siguiente pantalla es la que se visualiza al presionar el **botón Nuevo** de la pantalla:



#### ABM de Sistemas

Al seleccionar del submenú Herramientas el ítem de menú **ABM de Sistemas**, **CIPOL**  despliega una nueva ventanacon la lista de los sistemas habilitados actualmente y permite operar de la manera típica de un ABM, a los efectos de gestionar la habilitación de las mismas.

En la siguiente figura se muestra la pantalla:



**Consulta:**

Al seleccionar un registro de la grilla, presionar el respectivo botón “Vista Previa”. Se despliega una ventana donde no se podrá realizar ningún cambio.



**Botón Nuevo:**

Este botón permitirá registrar un nuevo Sistema. Al presionar este botón se abre una pantalla donde todos los campos se encuentran habilitados para ingresar los datos correspondientes en cada campo.

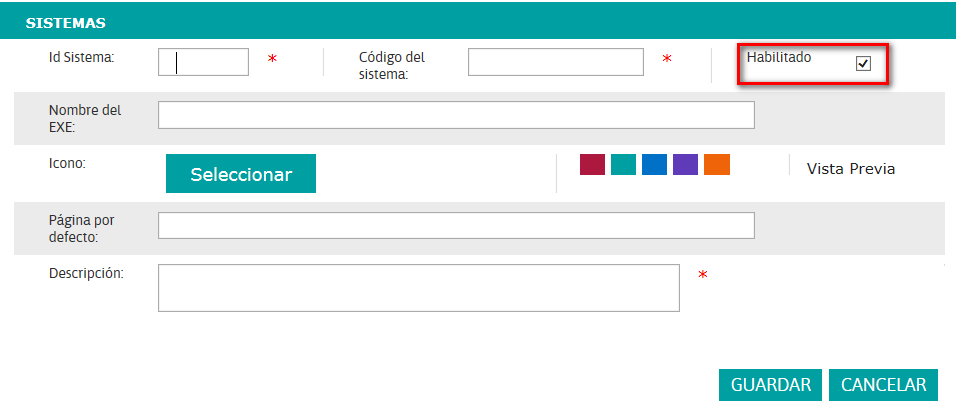
**Botón Modificar.**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema muestra una ventana con los campos habilitados en modo de edición para realizar las modificaciones necesarias.

**Botón Eliminar:**

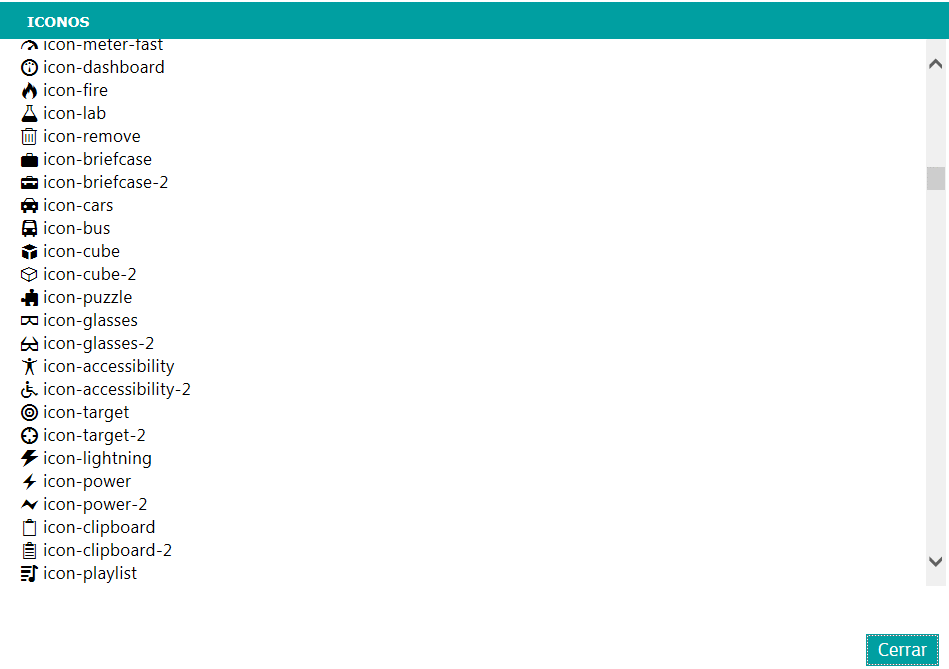
Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema elimina el sistema.

La siguiente pantalla es la que se visualiza al presionar el botón Nuevo de la pantalla:

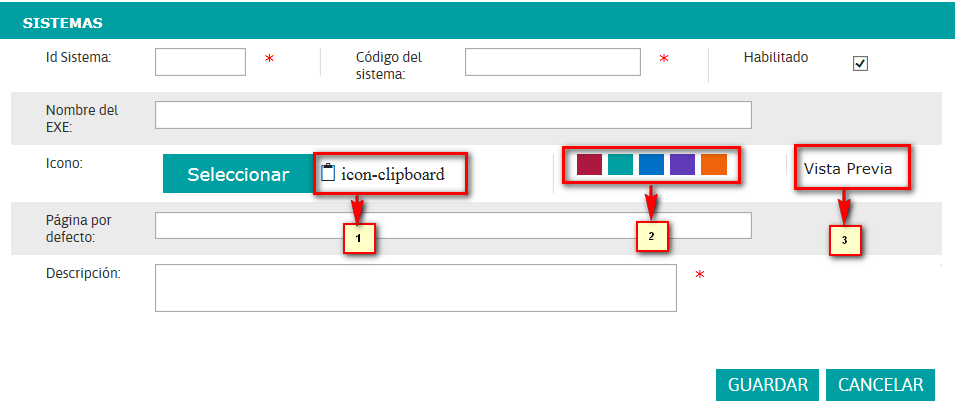


El tilde de la opción Habilitado, se utiliza cuando se quiere deshabilitar un sistema por alguna causa.

Al momento de definir el ícono del sistema, **CIPOL**  provee una serie de imágenes para que el usuario selecciona la más representativa del sistema que está dando de alta. Para esto, el usuario primero debe presionar el botón “Seleccionar” y se mostrará una lista de imágenes como se muestra a continuación.



Una vez que el usuario selecciona una imagen y presiona el botón “Cerrar”, se muestra una el ícono seleccionado (1). Para completar la selección del ícono, el usuario debe elegir un color que va a ser utilizado como fondo de la imagen seleccionada (2) haciendo click sobre el mismo.



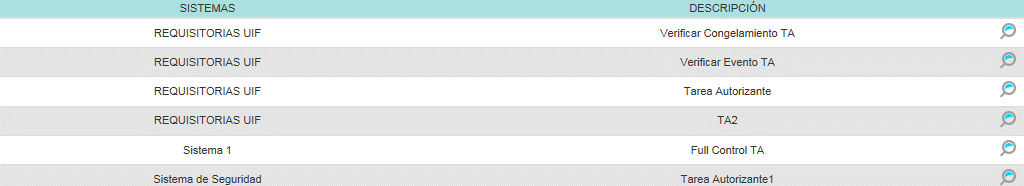
Una vez realizados ambos pasos, el usuario puede acceder a una “Vista Previa” del ícono creado a través del botón con el mismo nombre (3).



#### ABM Tareas Autorizantes

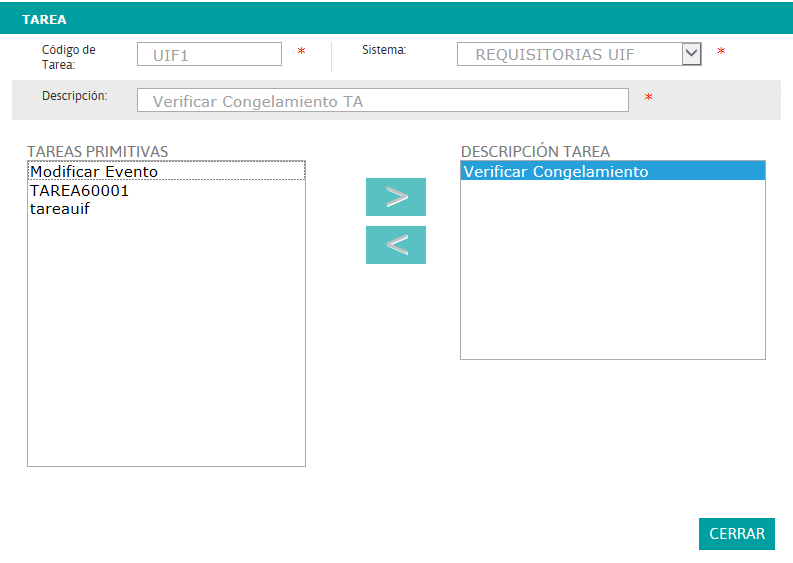
Al seleccionar del submenú Herramientas el ítem de menú **ABM Tareas Autorizantes**, **CIPOL**  ofrece la posibilidad de implementar un esquema de supervisión sobre aquellas tareas operativas que sean identificadas como críticas. En otras palabras, esta funcionalidad permite establecer una categorización de usuarios de aplicativos, una parte de ellos se encargará de la registración de datos mientras que otros, los designados como *Supervisores,* realizarán la aprobación de lo registrado.

En la siguiente figura se muestra la pantalla, esta muestra una lista de todas las *Tareas Autorizantes* activas y el sistema al que pertenecen



**Consulta:**

Seleccionar un registro de la grilla, y presionar su respectivo botón “Vista Previa”:



**CIPOL**  soporta dos niveles de supervisión, dependiendo de la importancia de la operación, implementada a través de la requisitoria de uno o dos funcionarios autorizantes.

En la pantalla principal se disponen los botones **Nueva**, **Modificar** y **Eliminar** que operan las funciones de altas, bajas y modificaciones para este rubro.

**Botón Nuevo:**

Este botón permitirá registrar una nueva Tarea Autorizante. Al presionar este botón se abre una pantalla donde todos los campos se encuentran habilitados para ingresar los datos correspondientes en cada campo.

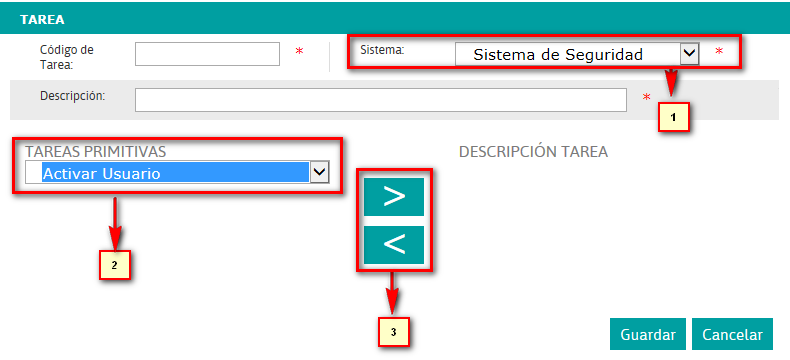
**Botón Modificar.**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema muestra una ventana con los campos habilitados en modo de edición para realizar las modificaciones necesarias.

**Botón Eliminar:**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema elimina la tarea autorizante.

La siguiente pantalla es la que se visualiza al presionar el **botón Nuevo** de la pantalla:



Descripción de los pasos para dar de Alta una nueva Tareas Autorizante:

A) Seleccionar el sistema de la lista desplegable, marcada con (1). Al seleccionar el sistema de esta lista, la lista con el nombre de Tareas Primitivas (2), se actualiza acorde a lo seleccionado en (1).

B) Seleccionar una Tareas Primitiva del combo marcado con (2).

C) Presionar el botón marcado con (3).

D) Para finalizar presionar el botón Guardar y los datos quedaran registrados.

Una vez efectuada el alta de una *Tarea Autorizante*,esta toma el mismo status que cualquier tarea. Esto significa que la Tarea Autorizante estará ahora disponible tanto para la generación de *Grupos* como para la de *Roles.*

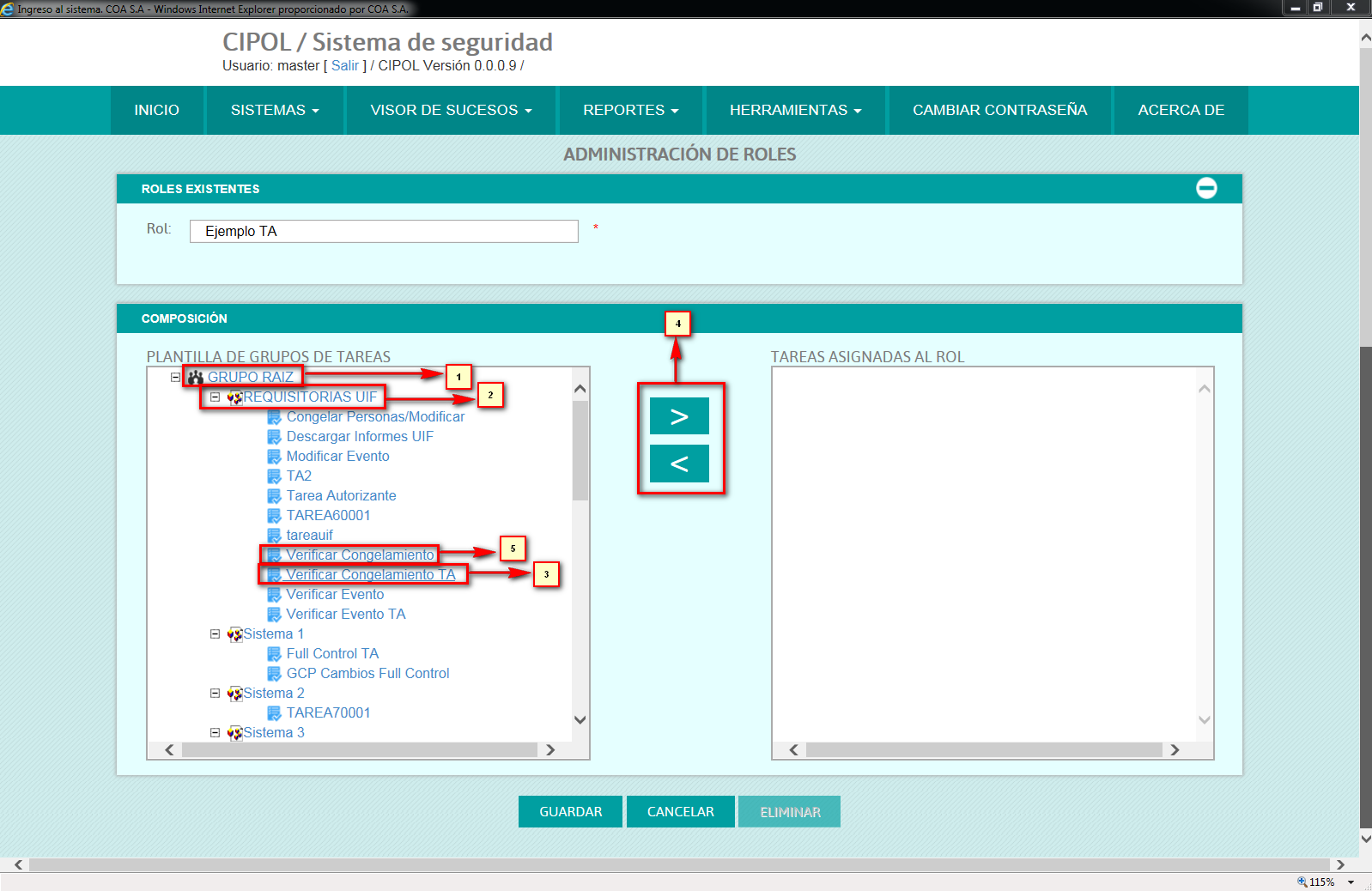
Ahora se detalla un ejemplo de los pasos a seguir para asignarle al usuario autorizante esta tarea:

A) En **tareas Autorizantes**: Presionar nuevo, ingresar los datos de la tarea que requiere autorización y presionar guardar, en la siguiente pantalla:



B) Ir a **Sistemas🡪 Administración de Roles** y crear un nuevo rol y asignarle la tarea Primitiva creada como indica la siguiente pantalla:

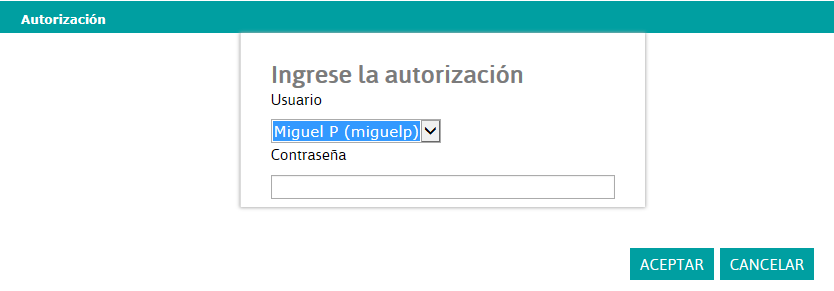
En esta instancia se debe asignar la tarea de supervisión a un Rol existente o crear uno nuevo que la contenga, optaremos por esto último:



La tareas se encuentra **seleccionando Grupo Raíz (1)🡪 Sistema de seguridad(2)🡪 Verificación Congelamiento TA (3)**, y luego presionar el botón de asignación (4) para asignar la tareas al Rol y para finalizar presionar Guardar.

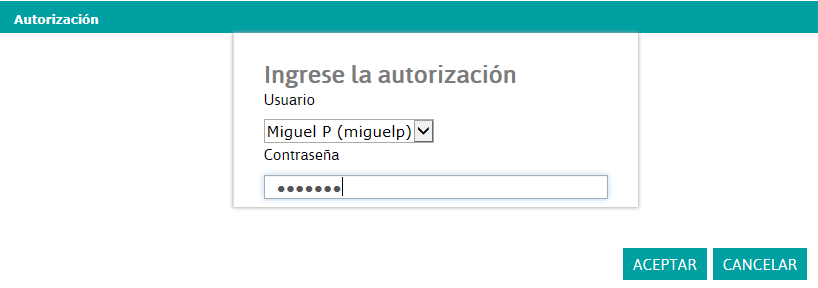
Verificar que dentro de la lista también se encuentra Administración de Usuarios marcado con (5), esta tarea es la tarea Primitiva, la misma se le debe asignar a todos los usuarios que tengan el rol de ingresar a la Administración de Usuario, pero que no sea usuario Autorizante.

C) Luego, cuando el usuario quiera realizar la tarea primitiva, se va a emitir un mensaje obligando a que un usuario, que tenga la tarea autorizante asignada, autorice la operación ingresando su contraseña:



En el cuadro se observa una lista desplegable con la identificación de los nombres de las cuentas de inicio de sesión, correspondientes a todos los usuarios que tienen asignado el *Rol Autorizante* sobre la actividad actual que se pretende realizar. Además se describe el nombre completo del usuario *Supervisor,* a los efectos de evitar confusiones.

🛈 *Un Usuario Supervisor será seleccionable siempre y cuando su cuenta está activa en el sistema, o sea no debe estar dado de baja ni bloqueado.*



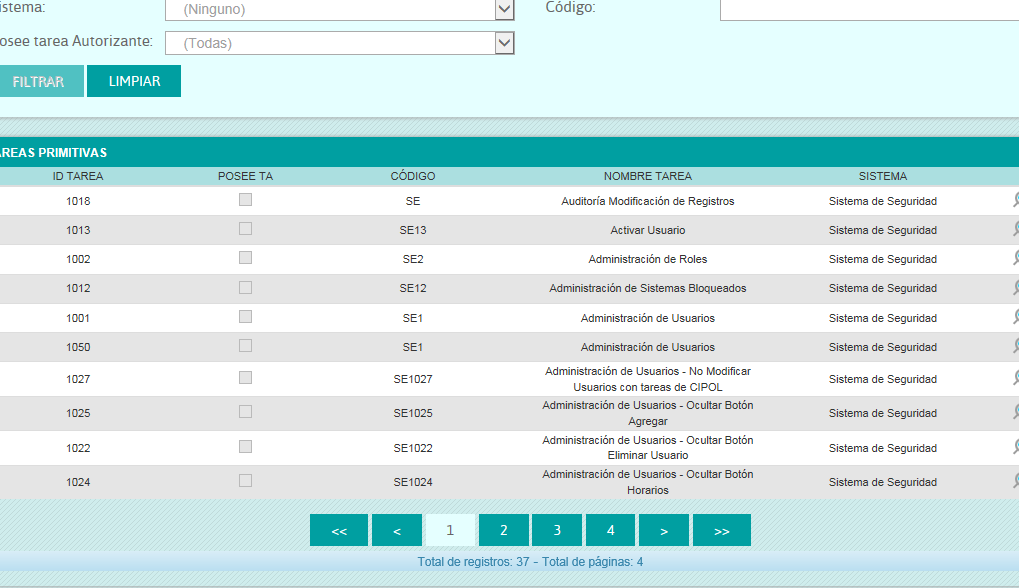
El usuario actual podrá seleccionar al Supervisor, tal como se muestra en la figura, y a continuación deberá solicitar la presencia del mismo para que ingrese su contraseña. Hecho esto, se presiona **Aceptar** y continuará normalmente.

🛈 *Un usuario puede tener asociado un Rol para efectuar una determinada Tarea, dentro de cualesquiera de los aplicativos gestionados por* ***CIPOL*** *, y a su vez poseer el Rol Autorizante relacionado.*

🛈 *Al igual que en caso de los Grupos, la implementación del esquema de supervisión a través de Tareas Autorizantes no es obligatoria. No obstante, es una herramienta útil en el sentido de que permite un mayor control sobre actividades sensitivas .*

#### ABM Tareas Primitivas

Al seleccionar del submenú Herramientas el ítem de menú **ABM Tareas Primitivas, CIPOL**  despliega una nueva ventanacon la lista de las tareas primitivas actuales de todos los sistemas integrados a **CIPOL**  actualmente y permite operar de la manera típica de un ABM, a los efectos de gestionar la habilitación de nuevas tareas, como muestra la siguiente pantalla:



**Filtros:**

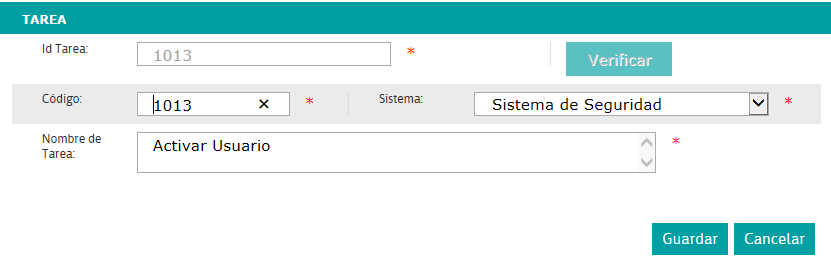
El filtrado actúa sobre los atributos: **ID Tareas, Nombre Tarea, Sistema, Cód. Tarea y Posee tarea autorizante**.

**Botón Limpiar:**

El botón **Limpiar** permite borrar las opciones de filtrado ingresadas hasta el momento. Además, si ya se realizó una consulta previa, este botón permitirá ingresar datos para realizar una nueva.

**Consulta:**

Al seleccionar un registro de la grilla y presionar el respectivo botón “Vista Previa”, se muestran todos los datos del registro seleccionado.



**Botón Nuevo:**

Este botón permitirá registrar una nueva Tarea Primitiva. Al presionar este botón se abre una pantalla donde todos los campos se encuentran habilitados para ingresar los datos correspondientes en cada campo.

**Botón Modificar.**

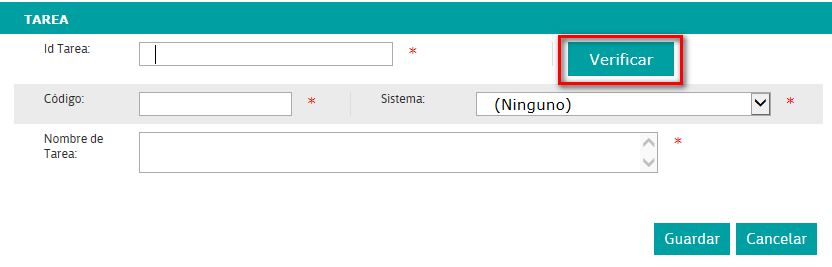
Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema muestra una ventana con los campos habilitados en modo de edición para realizar las modificaciones necesarias.

**Botón Eliminar:**

Se deberá presionar el botón Modificar del registro correspondiente, y así, el sistema elimina la Tarea Primitiva.

Al presionar el botón **Nuevo** se inicia la secuencia de alta de una nueva tarea primitiva, conmutando automáticamente desde la solapa **Tareas Primitivas** a la solapa **Detalle**.

La siguiente pantalla es la que se visualiza al presionar el **botón Nueva** de la pantalla:



**Botón Verificar:**

A presionar este botón, valida que el ID de Tarea no se encuentre ingresado en otra tarea existente.

En esta instancia se deberán ingresar los datos solicitados en las cajas de texto, procediendo a **Guardar** los mismos mediante el botón del mismo nombre.

#### Análisis de Auditoria

Al seleccionar del submenú Herramientas el ítem de menú **Análisis de Auditoria, CIPOL**  muestra la siguiente pantalla. Esta permite revisar las Auditorías de Eventos de actualización de datos del sistema a través de las opciones de filtrado disponibles.



Esta ventana consta de dos áreas:

* + - **Área de Filtros**: ubicada en la parte superior que permitirá establecer condiciones para refinar los criterios de selección de la información a consultar.
    - **Área de resultados:** en la parte inferior de la pantalla, donde se mostrará el resultado de la consulta.

Los filtros disponibles son:

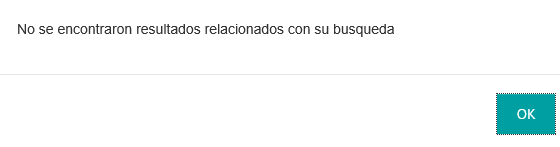
* **Fecha (Desde** y **Hasta):**  delimitadores para establecer el período a consultar (no podrá ser mayor a un mes calendario).
* **Tabla:** para elegir eventos de auditorías sobre una tabla en particular (o todas).
* **Usuario:** permitirá elegir eventos originados por un usuario determinado (o todos).
* **Operación:** permitirá elegir el tipo de operación de actualización de datos (o todos).
* **Nombre PC:** para cuando se desee revisar eventos originados en un puesto determinado (o todos).
* **Sistema:** habilita la posibilidad de consulta de eventos relacionado a uno (o todos) de los sistemas administrados por **CIPOL**.
* **Texto de Búsqueda:** permite ingresar un texto modelo para agregar como filtro a aplicar en la cadena SQL relacionada con la operación auditada.

Se recomienda la utilización de los filtros para acotar la cantidad de registros a recuperar. Son acumulativos, lo que facilita la refinación de la búsqueda.

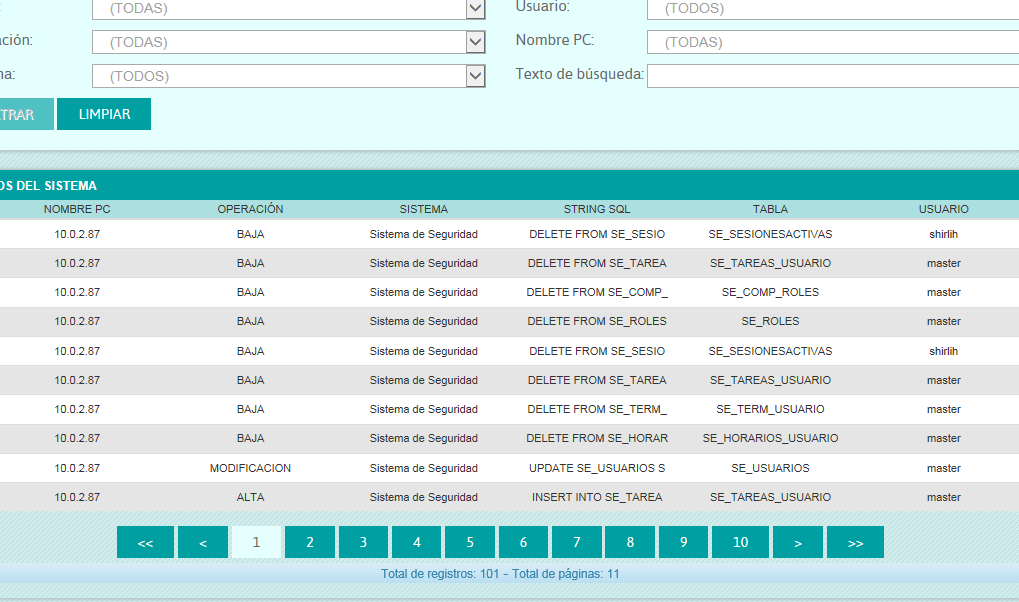
🛈 *Para colaborar con controlar el tráfico de red para que no atente contra los recursos de la red de la Organización, se exigirá que al menos haya una selección particular en los diferentes filtros exceptuando las Fechas (restringidas a no más de un mes) y el Texto genérico.*

La opción Limpiar, inicializa todos los filtros indicados, mientras que Filtrar, ordenará la ejecución de la consulta a la base de datos del sistema.

En caso de que el resultado no entregue registros que coincidan con las condiciones de la búsqueda, **CIPOL** mostrará un mensaje comunicando esto.



Caso contrario, desplegará los registros recuperados en el área de resultados.



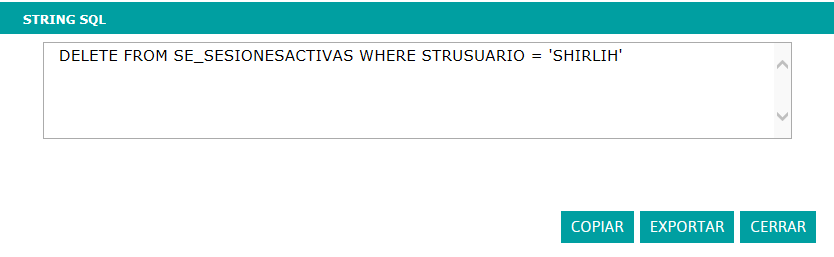
Por cuestiones de control de performance y posible impacto en los recursos de la red, si la cantidad de registros recuperados exceden un tope de control, el sistema advertirá la situación y permitiendo elegir entre visualizar solo lo recuperado hasta dicho tope o bien recargar todos los indicados como total de registros que se corresponden con los filtros indicados.



**Botón Exportar Excel:**

Cuando se hayan recuperado registros, se habilitará la opción Exportar a Excel para que se puedan exportar todos los registros recuperados (no solo los que se visualizan en pantalla) a un nuevo archivo Excel.

Por cada registro de la grilla podremos presionar la lupa al final del registro (Vista Previa) y de esta manera ampliar el contenido del valor String SQL que se utilizó en dicho evento.



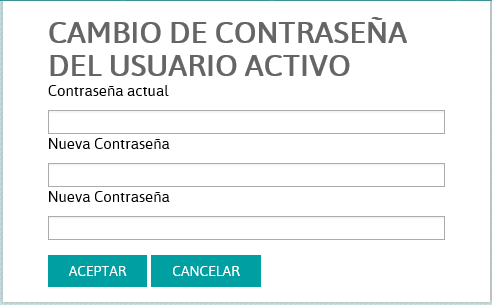
#### Cambiar nombre del Dominio.

Al seleccionar del submenú Herramientas el ítem de menú **Cambiar nombre del Dominio,** el sistema muestra la siguiente pantalla, en la misma



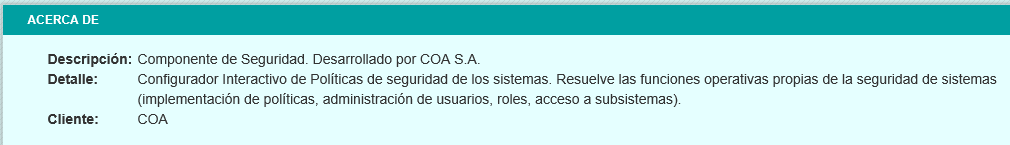
## Cambio de contraseña de usuario

La opción Cambiar contraseña permite al usuario cambiar su propia contraseña. Para conocer el procedimiento asociado a esta opción, remitirse a la explicación descripta en el capítulo anterior en el párrafo homónimo “Cambio de contraseña de usuario”. Esta opción solo estará habilitado cuando el sistema no se encuentra integrada al dominio o cuando la seguridad es mixta, para usuarios no integrados al dominio.



## Acerca de

La opción **Acerca de** presenta en una ventana con información del producto y del Cliente donde está instalado.



## Cerrar el Sistema

Para finalizar la sesión **CIPOL**  tiene 2 aternativa.

La primera será haciendo click sobre el link [Salir] o bien cerrando la pestaña del explorador, tal como se destaca en la figura siguiente.



**Apéndice A**

Revisiones del documento

|  |  |  |  |
| --- | --- | --- | --- |
| **Nº** | **Fecha** | **Autor** | **Corresponde a la versión** |
| 1 | 03/11/2014 | COA S.A. | 1.0.0 |
| 2 | 07/05/2107 | COA S.A: | 1.0.11 |