

# Enterprise - Especificación Funcional - Seguridad

---

## 1 Descripción

En el presente documento se detalla el esquema de seguridad para el sistema que se usa para modelar, las herramientas del mismo y los sistemas generados por él. En este documento no se analizarán esquemas de licenciamiento.

### 1.1 Definiciones y Acrónimos

Término	Definición
Elemento	Se refiere a todos aquellos elementos que se pueden definir en el sistema. Por ejemplo: entidad, proceso de negocio, desencadenante, transformación, etc.
Modelador/Programador	Se refiere al sistema formado por todas aquellas herramientas que se utilicen tanto para modelar y generar un sistema de información (por ejemplo: ERP, CRM, etc.), como para la inteligencia de negocios.
Objeto	Se refiere a todos aquellos elementos que se configuran desde el Dominio de Seguridad. Por ejemplo: usuario, grupo de usuarios, dispositivos, etc.
WS	Web Service

## 2 Introducción

La *seguridad* permitirá definir, tanto en tiempo de edición como en tiempo de ejecución del sistema generado, cuáles serán los diferentes permisos que podrán tener los usuarios del sistema, tanto del modelador como de los sistemas generados.

Esta funcionalidad será transversal a todo el sistema, de forma tal que toda operación que desee realizar una persona en el sistema pasará previamente por una verificación de seguridad. De no cumplir con dicha verificación, la acción no podrá ejecutarse, notificándose a quien corresponda.

A continuación, se presentan definiciones preliminares para comprender los conceptos de seguridad.

## 2.1 Definición de dominio de seguridad, modelo y ambiente.

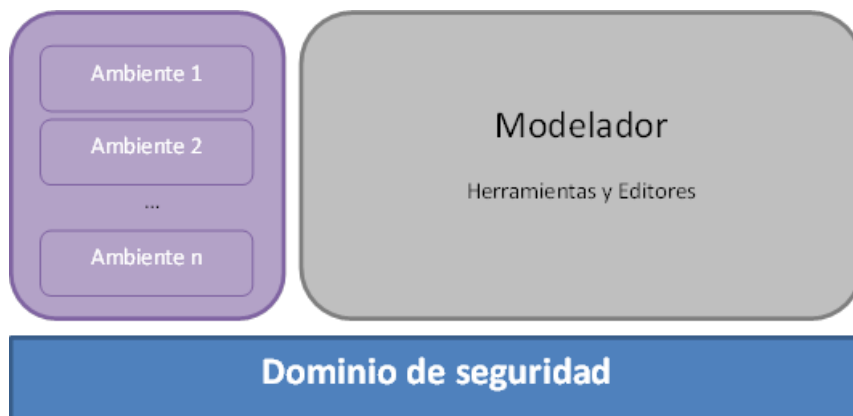
Un *dominio de seguridad* es una unidad única de administración de seguridad, y está compuesto por *objetos*, los cuales pueden ser unidades organizacionales, unidades organizacionales de sitios, grupos de sitios, sitios, grupos de usuarios, usuarios y dispositivos, y sus permisos, denegaciones y políticas. Un dominio tendrá al menos un usuario *administrador* de dominio.

Un *modelo* es un conjunto de definiciones que permitirán generar un sistema final (ERP, CRM, etc.) mediante el modelador y estará asociado a un único dominio de seguridad. *Un modelo se podrá replicar para generar otro modelo idéntico dentro de un dominio de seguridad diferente del original.* Además, un *dominio* podrá contener uno o varios *modelos*. Siempre existirá al menos un modelo en un dominio.

Un *ambiente* es el contexto en donde se ejecutarán los diferentes estados intermedios del sistema generado. Ejemplo: desarrollo, prueba, producción, etc. Se podrán generar vacíos, con datos de prueba o con acceso a los datos reales. *Ejemplo: un ambiente de prueba con datos reales de producción.* Existirá sólo una versión en producción del sistema y una o varias versiones en los demás ambientes.

Un *sistema generado o final* es una instancia de un modelo junto con su dominio de seguridad para un cliente en particular.

Se podrán definir permisos sobre los elementos del modelo, el sistema final, y los ambientes, a partir de los usuarios y grupos de usuarios de un dominio de seguridad.



El editor del dominio de seguridad tendrá la siguiente interfaz:

dominio.com

General Configuración regional Vínculos Historial de Versiones Seguridad Documentación

Nombre *dominio.com*

Descripción *30 licencias habilitadas.*

Calendario Calendario Predeterminado

**[-] Idiomas disponibles**

Seleccione los idiomas y dialectos que se utilizarán en todos los modelos.

Idiomas disponibles		Idiomas seleccionados
▼ Español	>	▼ Portugués
España	>>	Brasil
Uruguay	<<	Portugal
...	<	▼ Español
► Inglés		Argentina
► Francés		► Francés

Idioma predeterminado (\*) Portugués (Brasil)

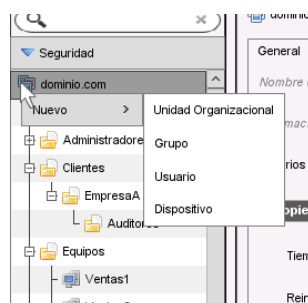
Idioma preferido de interfaz de usuario para autenticación de usuarios (\*) Español (Argentina)

Idioma preferido de datos para autenticación de usuarios (\*) Español (Argentina)

**Propiedades de las cuentas**

Tiempo máximo sin acceso antes de inhabilitar cuenta 60 días

Reintentos de acceso fallidos consecutivos 3 reintentos



Las propiedades de un *dominio* estarán divididas en cinco solapas:

✓ **General:** muestra información sobre el dominio:

- Nombre (no internacionalizable y no permite espacios porque se usa en la url).
- Descripción
- Logo: se tendrá la posibilidad de configurar en el Dominio el Logo de la empresa de manera que cada empresa y ISV tenga la posibilidad de personalizar su propio logo.  
Además, podrá visualizarse el mismo como fondo al ingresar al sistema antes de abrir cualquier actividad.
- ~~Identificador web del dominio: esta propiedad se usa dentro de la url de acceso a un dominio. Es un texto no internacionalizable que no podrá contener caracteres especiales ni espacios. Será de valor único entre los dominios de Fastprg (no se puede repetir). Si un usuario cambia esta propiedad, se aplicará a partir del próximo login de los usuarios, es decir, si hay algún usuario autenticado, no se actualizará la url hasta su próximo login.~~
- **Calendario asignado.** Inicialmente, el calendario asignado será el predeterminado, pudiendo asignar otro calendario al dominio o editar el

*calendario predeterminado desde el [Editor de Calendarios](#), accediendo desde el menú contextual sobre el nombre de dicho calendario.*

- Dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.)
  - idiomas disponibles: para todos los modelos en el dominio
  - idioma predeterminado
  - idiomas preferidos de datos y de UI para autenticación de usuarios
  - políticas de seguridad definidas.
- ✓ *Configuración regional:* en esta solapa se podrá definir la configuración regional por idioma.
- ✓ *Vínculos:* muestra los vínculos de seguridad y sus propiedades.
- ✓ *Licencias:* muestra información sobre la cantidad de licencias disponibles, asignadas y en uso, por cada tipo de licencia.
- ✓ *Historial de Versiones:* se podrá mantener un historial de versiones de la definición de la seguridad del dominio, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad:* muestra una lista de los permisos y denegaciones de cada usuario y grupos de usuarios.
- ✓ *Documentación:* contiene la documentación específica del dominio, de acuerdo a lo especificado en el documento de Estándares de Interfaz de Usuario.

Los *Idiomas disponibles* permitirán definir qué idiomas y qué dialectos de cada idioma se utilizarán en todos los modelos (incluyendo en qué idioma se usa el Administrador de Modelos y el Dominio). Será obligatorio indicar al menos un idioma. Es la lista de idiomas de interfaz de usuario en la que se podrán ver los editores, las aplicaciones finales e ingresar las instancias. Todos los modelos de dicho dominio van a estar en los idiomas elegidos. Para definir esta propiedad se utilizará una grilla. Para seleccionar cada idioma, se listarán todos los idiomas que se soporta NeuralSoft y para cada idioma se visualizarán todos los dialectos disponibles.

Luego de definir la lista de idiomas, se deberá elegir un *Idioma predeterminado* dentro de una lista desplegable de selección única donde se listarán los idiomas y dialectos seleccionados en la lista doble anterior y se deberá indicar cuál de ellos es el predeterminado. En caso de que el idioma presente algún dialecto, sólo se podrá indicar como predeterminado, a uno de los dialectos de dicho idioma. Por el contrario, si un idioma no presenta ningún dialecto, podrá seleccionarse al idioma como predeterminado. Este idioma servirá como base para las traducciones en los demás idiomas cuando se agrega un idioma.

A diferencia del idioma predeterminado, en el dominio también se deberá definir los idiomas preferidos para autenticación:

- *Idioma de interfaz de usuario preferido para autenticación:* lista desplegable de selección única para seleccionar en qué idioma de UI se autenticarán los usuarios, es decir, el idioma en el que se podrán ver los editores e ingresar las instancias del modelo (reglas de negocio, entidades, etc.). **Las OU y usuarios heredan esta configuración.** En esta lista sólo se mostrarán los idiomas disponibles seleccionados en la lista doble.
- *Idioma de datos preferido para autenticación:* lista desplegable de selección única para seleccionar en qué idioma de datos se autenticarán los usuarios, es decir, el idioma en el que se podrán ver e ingresar las instancias de usuario (cliente, factura, etc.). **Las OU**

y usuarios heredan esta configuración. En esta lista se mostrarán todos los idiomas de datos brindados por Neuralsoft.

Siempre se validará que el idioma predeterminado y los idiomas preferidos para autenticación sean uno de los que se encuentran seleccionados en la lista de idiomas disponibles.

Tanto la lista de los idiomas disponibles, como la configuración regional de cada idioma serán definidas por Neuralsoft. ~~Es importante aclarar que puedo comprar un modelo en un idioma que no esté dentro de los idiomas de mi dominio. En este caso, se traduce al vuelo el idioma predeterminado del modelo comprado a todos los idiomas de mi dominio. Por ejemplo, mi dominio tiene español e italiano, puedo comprar un modelo que sólo esté en ruso (predeterminado) y alemán y se va a traducir el modelo desde el ruso al español y al italiano. El modelo en ruso y alemán no se copian!~~

Se define que en los modelos vinculados, el dominio hijo tiene que tener al menos todos los idiomas que tiene el dominio padre. Por ejemplo, si el padre tiene español e inglés, el hijo tiene que tener si o si, español, inglés, y puede tener otros.

Si luego en el otro dominio se agrega el idioma español, se copia todo el modelo en español desde el padre y pisa todas mis traducciones y personalizaciones.

## 2.2 Configuración regional por idioma

Dentro de la configuración regional se puede definir:

- ✓ *Día inicial de la semana:* esta propiedad permite seleccionar el primer día de la semana para el idioma o dialecto que se esté definiendo. Las opciones disponibles son: lunes (opción predeterminada), martes, miércoles, jueves, viernes, sábado y domingo.
- ✓ *Semana inicial del año:* esta propiedad permite seleccionar la primera semana del año para el idioma o dialecto que se está definiendo. Las opciones que se pueden seleccionar son las siguientes: “Primera semana” (opción predeterminada), “Primer Semana Completa”, “Comienza el 1 de Enero”.
- ✓ *Separador decimal:* esta propiedad permite especificar para el idioma seleccionado cuál es el separador decimal de un número. **El valor definido en este campo no podrá ser igual que los valores definidos en los campos “Separador de lista” y “Separador de miles”.**
- ✓ *Separador de lista:* esta propiedad permite especificar para el idioma seleccionado cuál es el separador de elementos dentro de una lista, por ejemplo, para separar parámetros dentro de una función. **El valor definido en este campo no podrá ser igual que los valores definidos en los campos “Separador decimal” y “Separador de miles”.** Este separador de lista no se utiliza para separar ítems dentro de una colección, ya que, para esto se utiliza el separador de elementos definidos en la colección.
- ✓ *Separador de miles:* esta propiedad permite especificar para el idioma seleccionado cuál es el separador de miles a utilizar. **El valor definido en este campo no podrá ser igual que los valores definidos en los campos “Separador decimal” y “Separador de lista”.**
- ✓ *Formato de Fecha:* a través de este separador colapsable, el usuario puede definir para cada idioma, los diferentes formatos de fecha que estarán disponibles en la aplicación. Además, se debe indicar uno de los formatos

como valor predeterminado. Este se usará luego para visualizar los datos de tipo fecha.

- ✓ **Formato de Hora:** a través de este separador colapsable, el usuario puede definir para cada idioma, los diferentes formatos de hora que estarán disponibles en la aplicación. Además, se debe indicar uno de los formatos como valor predeterminado. Este se usará luego para visualizar los datos de tipo hora.
- ✓ **Formato Fecha y Hora:** a través de este separador colapsable, el usuario podrá definir para cada idioma, los diferentes formatos para los campos que son Fecha y Hora. Además, se debe indicar uno de los formatos como predeterminado. Este se usará luego para visualizar los datos de tipo fecha y hora.

✓

De forma predeterminada, existirá una configuración predeterminada por cada uno de los idiomas seleccionados en la solapa general, pudiendo los usuarios redefinirla.

La configuración regional aplica a todo el dominio, incluyendo los modelos contenidos en él.

En la sección Anexos, de este documento, se incluye una sección de Configuración regional por idioma ([11.2 Configuración regional por idioma](#)), donde se incluyen la configuración para los idiomas nuevos de8finidos en Fastprg.

dominio.com

General Configuración regional Vínculos Historial de Versiones Seguridad Documentación

**[ - ] Idioma Español**

Separador Decimal (\*)

Separador de lista (\*)

Separador de miles

**[ - ] Formato de fecha**

**Defina los formatos de fecha personalizados teniendo en cuenta los siguientes significados de las notaciones:**  
d, dd = número del día; ddd, dddd = día de la semana; m, mm = mes; mmm, mmmm = mes del año, aa, aaaa = año separadores= ./-b

Corto:  Ejemplo: 05 / 6 / 15

Medio:  Ejemplo: 05 - 07 - 2015

Largo:  Ejemplo: 30 de Julio de 2015

Completo:  Ejemplo: Jueves 30 de Julio de 2015

Formato de fecha Predeterminado (\*)

**[ - ] Formato de hora**

**Defina los formatos de hora personalizados teniendo en cuenta los siguientes significados de las notaciones:**  
h, hh = hora; mm = minuto; ss = segundo; t, tt = a.m. o p.m.; h/H = 12/24 horas

Corto:  Ejemplo: 2 :09 :08

Medio:  Ejemplo: 12.09.08 p

Largo:  Ejemplo: 15:09:57

Completo:  Ejemplo: 09 : 18 : 47 a.m.

Formato de hora Predeterminado (\*)

**[ - ] Formato de fecha y hora**

dominio.com

General Configuración regional Vínculos Historial de Versiones Seguridad Documentación

**[ - ] Idioma Español**

Separador Decimal (\*)

Separador de lista (\*)

Separador de miles

**[ + ] Formato de fecha**

**[ + ] Formato de hora**

**[ - ] Formato de fecha y hora**

**Defina los formatos de fecha y hora personalizados teniendo en cuentas los siguientes significados de notaciones:**

Para la fecha: D, DD = número del día; DDD, DDDD = día de la semana; M, MM = mes; MMM, MMMM mes del año; AA, AAAA = año  
 Para la hora: h, hh = hora; mm = minuto; ss = segundo; tt = agrega a.m./p.m.; z, zz = zona horaria  
 En los formatos corto y medio los posibles separadores para fecha son: - ./ y para la hora son: : |

Corto:  Ejemplo: 05 / 6 / 15 11:26

Medio:  Ejemplo: 05 - 07 - 2015 04:28

Largo:  Ejemplo: 30/07/2016 20:15:54 Argentina (Buenos Aires)

Completo:  Ejemplo: Jueves 30 de Julio de 2015 20:12:48

Formato de fecha y hora predeterminado (\*)

Las opciones de formato disponibles se representarán con distintas notaciones. Estas notaciones dependerán del idioma del usuario logueado (no importa el idioma en el cuál se está definiendo el formato, para todos los formatos usa el idioma en el que está el usuario).

Las notaciones definidas a continuación sólo se usan si el usuario está logueado en el idioma español:

Para la fecha:

Para los formatos corto y medio:

D = número del día sin mostrar 0 a la izquierda. Por ejemplo: 7 o 22

DD = número del día mostrando 0 a la izquierda. Por ejemplo: 07 o 31

M = número del mes sin mostrar 0 a la izquierda. Por ejemplo: 5 o 10

MM = número del mes mostrando 0 a la izquierda. Por ejemplo: 05 o 11

AA = año mostrando solo los dos últimos dígitos. Por ejemplo: 98 o 15

AAAA = año mostrando los cuatro dígitos. Por ejemplo: 1998 o 2015

Solo son posibles los siguientes separadores: "-", ".", "/" y ". ". Además todos los separadores utilizados en un formato corto y medio deben ser iguales, NO se podrá configurar por ejemplo 31-12/2017.

Para los formatos largo y completo se pueden utilizar todos los anteriores más:

DDD = día de la semana abreviado. Por ejemplo: Lun o Vie

DDDD = día de la semana escrito en forma completa. Por ejemplo: Lunes, Sábado

MMM = mes del año abreviado. Por ejemplo: Jun o Ene

MMMM = mes del año escrito en forma completa. Por ejemplo: Junio o Enero

Los separadores pueden ser distintos y no están acotados.

~~Todas las notaciones de fecha están en mayúsculas.~~ El separador de fecha no tiene una notación específica, sino que el usuario lo escribe directamente en la caja del formato que está configurando.

Por ejemplo para la fecha 07/12/2015 el usuario escribirá dd/mm/aaaa.

Todos los formatos siempre deben tener el día, mes y año.

Para la hora:

h = horas sin mostrar 0 a la izquierda. Por ejemplo: 5 o 11

hh = horas mostrando 0 a la izquierda. Por ejemplo: 05 o 11

mm = minutos (siempre muestra el 0 a la izquierda). Por ejemplo: 09 o 58

ss = segundos (siempre muestra el 0 a la izquierda). Por ejemplo: 06 o 47

**h/H = formato 12 o 24 horas.** Si el formato es 12 horas, deberá especificarse alguno de los siguientes:

t = "p" o "a". Por ejemplo: 04:32 p

tt = a.m. o p.m. Por ejemplo: 04:32 p.m.

~~Todas las notaciones de hora están en minúsculas.~~ En el caso de los formatos corto y medio solo son posibles los siguientes separadores: [":", "|"] y todos los separadores deberán ser iguales. Todos los formatos donde se configuren horas siempre deben tener la hora y los minutos.

Por ejemplo para la hora 07:15 a.m. el usuario escribirá hh:mm tt

Sólo en la configuración del formato Fecha y Hora, y para los formatos largo y completo se puede configurar la zona horaria:

z = zona horaria corta. Por ejemplo: UTC-03:00

zz = zona horaria larga. Por ejemplo: Argentina (Buenos Aires)

En los formatos largo y completo el separador de hora no tiene una notación específica, sino que el usuario lo escribe directamente en la caja del formato que está configurando.

Además, se presentará una lista de selección simple, para indicar cuál es el formato predeterminado de fecha y de hora (aquí se podrá seleccionar entre Formato Corto, Medio,



Largo o Completo), mediante la interfaz descrita en el documento de “Estándares de Interfaz de Usuario”.

The screenshot shows a web browser window with the address bar displaying 'dominio.com'. The application has a navigation bar with tabs: 'General', 'Configuración regional' (selected), 'Vínculos', 'Historial de Versiones', 'Seguridad', and 'Documentación'. The main content area is titled '[-] Idioma Español'. It contains several input fields for regional settings: 'Separador Decimal (\*)' with a period in the field, 'Separador de lista (\*)' with a comma in the field, and 'Separador de miles' which is empty. Below these are three expandable sections: '[+] Formato de fecha', '[+] Formato de hora', and '[-] Formato de fecha y hora'. The '[-] Formato de fecha y hora' section is expanded, showing a heading 'Defina los formatos de fecha y hora personalizados teniendo en cuenta los siguientes significados de notaciones:' followed by a legend for date and time notations. Below the legend are four rows of format examples: 'Corto' (DD / M / AA hh:mm, Ejemplo: 05 / 6 / 15 11:26), 'Medio' (DD - MM - AAAA hh:mm, Ejemplo: 05 - 07 - 2015 04:28), 'Largo' (DD/MM/AAAA hh:mm:ss zz, Ejemplo: 30/07/2016 20:15:54 Argentina (Buenos Aires)), and 'Completo' (DDDD DD de MMMM de AAAA hh:mm:ss, Ejemplo: Jueves 30 de Julio de 2015 20:12:48). At the bottom, there is a label 'Formato de fecha y hora predeterminado (\*)' and a dropdown menu currently showing 'Formato corto'.

Para el ingreso de cualquiera de estos tipos de datos se utiliza el formato medio, pudiendo el usuario usar cualquiera de los separadores disponibles.

La configuración definida para el idioma, aplicará a todos los dialectos del mismo. En caso de que se necesite definir una configuración particular para uno o más dialectos, el usuario deberá seleccionar el icono, situado al lado del texto “Excepciones de configuración regional por dialecto”. Al seleccionar el icono se presentará una lista desplegable de selección múltiple y las propiedades de configuración regional, de modo de que el usuario pueda definir la misma para ciertos dialectos del idioma. El usuario podrá seleccionar uno o más dialectos y definir la configuración regional para los mismos. Además, existirá la posibilidad de eliminar alguna configuración particular que se haya hecho para algún conjunto de dialectos. La interfaz para definir excepciones de dialectos será la siguiente:

## 2.3 Vínculos de seguridad

### 2.3.1 Introducción

Existen casos en donde los usuarios de un dominio necesitan acceder a los recursos de otro dominio. Para esto existen los *Vínculos de Seguridad*.

Un *Vínculo de Seguridad* es una relación entre dos dominios, en donde hay un Dominio Accesible y un Dominio de Autenticación, es decir una dirección de confianza.

El “**Dominio de autenticación**” es el dominio de origen de los usuarios y grupos compartidos. En este, se valida la correcta autenticación de los mismos.

El “**Dominio de Acceso**” es el dominio destino al cual los usuarios compartidos podrán acceder.

De esta manera, un mismo usuario podrá acceder a diferentes dominios.

### 2.3.2 Configuración

Para agregar un nuevo *Vínculo de Seguridad*, se deberá acceder a la configuración del dominio, dentro de la sección Dominio. Es importante destacar que esto se puede realizar dentro de cualquier ambiente, siempre que se cuente con los permisos necesarios.

Allí se deberá definir la siguiente información:

- **Dominios de autenticación:** dominios externos cuyos usuarios podrán acceder a nuestro dominio.
  - **Nombre del dominio:** nombre del dominio externo, por ejemplo neuralsoft. Atributo de valor único. Texto no internacionalizable requerido.
  - ~~URL: url del dominio externo.~~
  - **Descripción:** título o explicación para distinguir el elemento. Se usa como ayuda emergente del mismo. Texto internacionalizable opcional.
  - **Documentación:** información ampliada del vínculo. Texto enriquecido internacionalizable opcional.
  - **Estado del vínculo:** estado en el que se encuentra el vínculo actualmente. El estado de un vínculo siempre será el mismo en ambos dominios. Los estados de un vínculo podrán ser:

- **Pendiente de Aprobación:** indica que el vínculo ha sido solicitado y está a la espera de hacerse efectivo o ser rechazado por el otro dominio involucrado. Un dominio agrega a otro Dominio de autenticación o Dominio de acceso, y este último deberá aceptar/rechazar el vínculo. Un vínculo en estado pendiente podrá ser aprobado sólo por el dominio que no creó dicho vínculo, pero podrá ser rechazado por cualquiera de los dominios involucrados. Inicialmente el estado será Pendiente.
  - **Aprobado:** indica que el vínculo se ha hecho efectivo. Luego de aprobado, un vínculo podrá rechazarse por cualquier dominio que forme parte del mismo.
  - **Rechazado:** indica que se ha rechazado la vinculación. El vínculo se podrá rechazar desde el estado Pendiente. Una vez rechazado la única opción disponible será “eliminar”, de forma tal que ya no aparezca en la grilla.
- **Objetos externos:** los objetos externos de acceso podrán ser usuarios, grupos de usuarios, unidades organizacionales o dispositivos del dominio externo. Dichos objetos estarán disponibles si el vínculo está aprobado, y si el Dominio de autenticación los ha definido previamente, ~~o ha indicado que no existen restricciones (el dominio local puede visualizar todos los objetos del dominio externo).~~ En esta sección sólo se visualizan los objetos compartidos de manera directa, pero no los objetos contenidos dentro de los mismos. En el Panel de Navegación se visualizan los objetos compartidos de manera directa, y además, se pueden expandir los grupos ~~y OUs~~, y ver los objetos contenidos dentro de los mismos, es decir, los objetos compartidos de manera indirecta.
- **Dominios de Acceso:** dominios externos en donde nuestros usuarios podrán acceder. Tienen la misma configuración que los Dominios de autenticación, excepto la última:
  - ⊖ **Objetos locales:** podrán definirse usuarios, grupos de usuarios, ~~unidades organizacionales y dispositivos~~ de nuestro dominio que podrán acceder al dominio de autenticación. Podrán definirse tanto en el momento de la creación del vínculo con el dominio accesible, como luego de su aprobación. ~~Cuando el dominio que debe efectivizar dicho vínculo, lo aprueba,~~ si dichos objetos aún no han sido definidos, los mismos estarán pendientes de restricción y ningún usuario del Dominio de autenticación tendrá acceso al dominio accesible. Para que esto ocurra, se deberán seleccionar los objetos locales cuya seguridad de acceso al dominio accesible podrá ser administrada por dicho dominio. ~~Si los objetos del vínculo se definen sin restricciones, el dominio que confía podrá administrar la seguridad de acceso de todos los objetos locales.~~

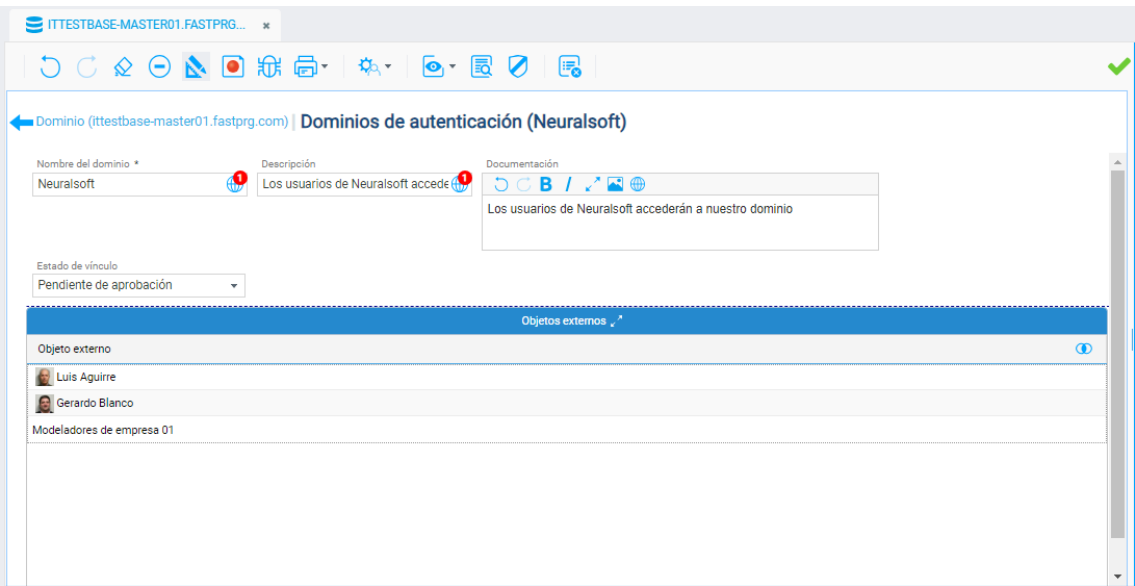
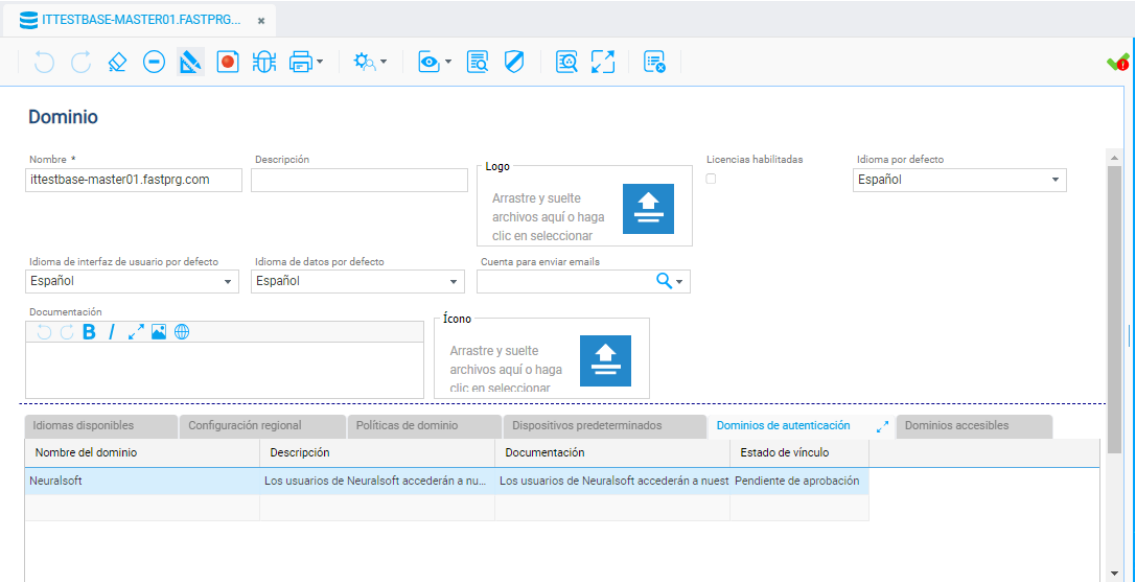
En el caso en que desde un dominio se creen dos vínculos con otro dominio, uno en cada dirección, el dominio al cual se le realiza la petición podrá aprobar o rechazar individualmente cada vínculo. Si aprueba o rechaza uno de los vínculos, el otro quedará pendiente hasta el momento en que realice una de las posibles acciones.

Sólo se podrá crear efectivamente un vínculo si no existe otro vínculo con el mismo dominio y dirección, o si existe y su estado es rechazado. Es decir, entre dos dominios no podrá haber más de un vínculo de seguridad en la misma dirección, con estado pendiente o aprobado. Si existe un vínculo entre dos dominios en una dirección, sólo se puede crear un nuevo vínculo en la misma dirección entre los mismos dominios, si el existente se encuentra rechazado. En este

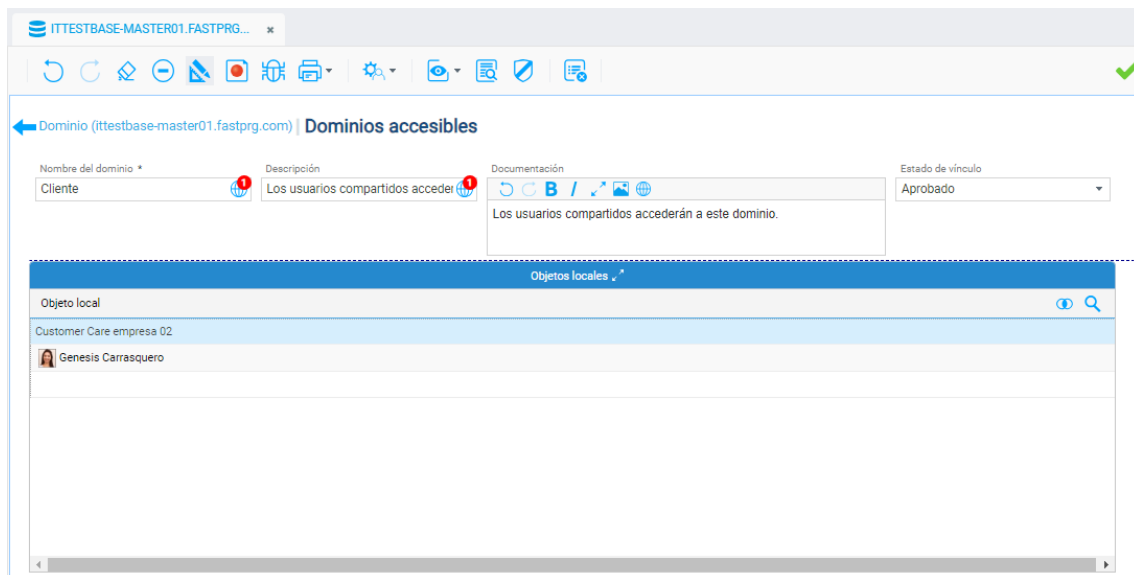
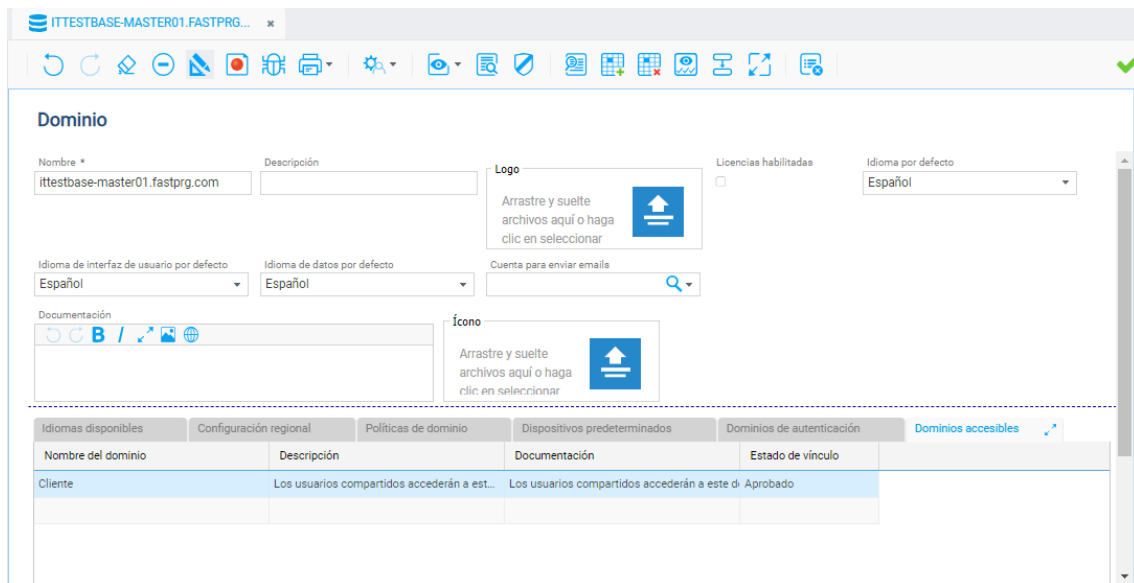
caso, se quitará automáticamente el vínculo rechazado de las interfaces de ambos dominios, y aparecerá el nuevo vínculo en estado pendiente.

Cuando se crea un dominio de autenticación, se crea una OU raíz que se visualiza en el panel de navegación y los objetos que se comparten se pueden visualizar dentro.

A continuación, un ejemplo de un dominio de autenticación:

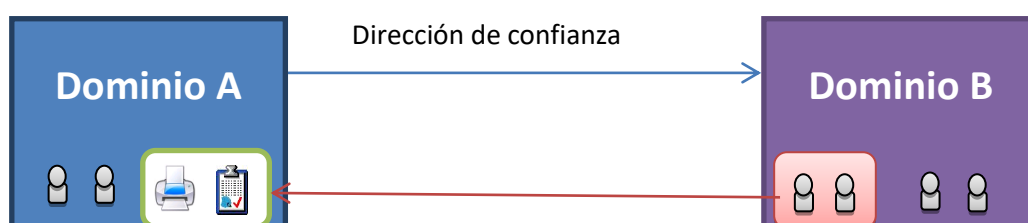


A continuación, un ejemplo de un dominio accesible:

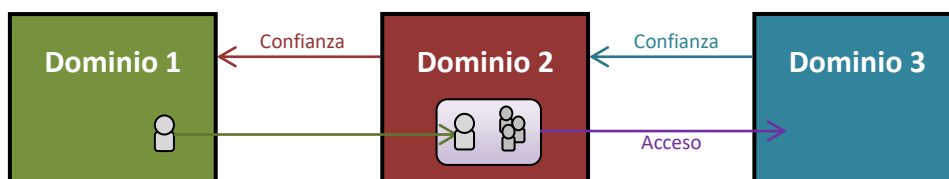


Si se establece un vínculo de confianza entre un dominio A (*dominio de acceso*) y un dominio B (*dominio de autenticación*), el administrador del dominio B deberá seleccionar los objetos que podrán tener acceso al dominio A. Los objetos de B podrán acceder a los elementos de A y el administrador de A podrá asignarles permisos a dichos objetos.

Por ejemplo, el dominio A establece un vínculo con el dominio B. Un usuario administrador de B acepta el vínculo y restringe el acceso a un grupo de usuarios. Para que estos usuarios puedan acceder al dominio A, un administrador de A deberá otorgarles permisos. En este ejemplo, el administrador de A le concede permisos al grupo de usuarios de B para acceder a la entidad Factura y a un dispositivo, ambos dentro de A. En consecuencia, los usuarios pertenecientes al grupo del dominio B podrán ingresar al dominio A y tendrán acceso a la entidad factura y al dispositivo en cuestión. Pero B no podrá acceder a las cuentas de usuarios de A; para que esto ocurra, se deberá generar otro vínculo de seguridad de la forma inversa. También, el usuario administrador del dominio B podrá administrar las políticas de acceso al dominio A de los usuarios de B, como por ejemplo, el rango horario en que podrán ingresar, si podrán delegar sus actividades, etc.



Además, si el dominio 3 confía en 2 y 2 confía en 1, se podrá dar el caso de que un usuario o grupo de 1 ingrese al dominio 3, ya que el dominio 2 puede administrar los usuarios externos en su dominio, como usuario de 1 y a su vez, puede administrar el grupo de usuarios que ingresan al dominio 3. Así, si ingresa un usuario de 1 a un grupo con acceso a 3, dicho usuario podrá acceder al dominio 3.



En este caso, Dominio 3 no sabe si los objetos que le comparte Dominio 2 son locales a este dominio, o se los comparte Dominio 1. En general, siempre que exista un vínculo de seguridad, el dominio accesible no sabrá en donde se originaron los objetos.

Un *vínculo de seguridad* entre dominios implicará la copia de objetos entre dominios, aunque los mismos permanecerán asociados a sus *dominios de origen* (en el cual se dieron de alta).

### 2.3.3 Objetos compartidos

Al establecer un *vínculo de seguridad* entre dos dominios, el mismo podrá aplicar tanto a todos los objetos como a un subconjunto de los mismos (por ejemplo, aquellos usuarios pertenecientes a un grupo determinado).

Se informará al dominio accesible los cambios en los objetos locales que forman parte de un vínculo de seguridad y que afecten al vínculo, ya sea de forma directa o indirecta.

En cualquier escenario en el cual se presente en un vínculo de seguridad, los objetos de acceso cumplirán las siguientes restricciones:

- **Usuarios:** se copiarán al principio, y estarán disponibles para asignarles permisos dentro del dominio accesible. Cuando se comparte el usuario, también se comparte el grupo personal.
  - Datos que se copian: foto, nombre de usuario (dominio/nombre de usuario), nombre, apellido. Estos datos no se pueden modificar en el dominio destino.
  - Al compartir un usuario, el tipo de usuario inicialmente es 'aplicación', pero se puede modificar a 'editor'.
  - Al compartir un usuario, el dominio externo se completa con el dominio de autenticación y no se puede modificar.
  - Datos que NO se copian: OU padre, contraseña, idioma de UI, idioma de datos, dominio local (pasa a ser el dominio actual), correo electrónico, teléfono, dirección, ciudad, provincia, país, descripción, y documentación. Todos estos datos quedarán vacíos en el dominio externo, heredando las configuraciones

de la OU raíz del dominio externo (o de la OU padre del usuario, si también se selecciona como objeto de acceso).

○ Políticas:

- Relacionadas a la autenticación: no se copian, no se pueden modificar en el dominio destino:
  - Métodos de autenticación
  - Forzar cambio de contraseña
  - Requiere completar datos personales en primer acceso
  - Habilitar cambio de contraseña
  - Rango horario permitido
  - Direcciones IP permitidas
- Relacionadas con la cuenta del usuario: no se copian, no se pueden modificar en el dominio destino:
  - Tiempo de expiración de la cuenta
  - Rango de fecha de validez de la cuenta
  - Cantidad de reintentos
  - Tiempo de bloqueo de cuenta
  - Cuenta bloqueada
- Relacionadas con la jerarquía en el organigrama: las opciones en las siguientes políticas son todos, pares y subordinados, subordinados o ninguno. No se copian, se heredan de la OU donde se agrega y se pueden modificar en el dominio destino. En el dominio destino deberán agregar el usuario en un organigrama para que tenga validez las opciones de pares y subordinados.
  - Delegación de actividades (inicialmente no definido en la ou)
  - Consulta de actividades delegadas (inicialmente no definido en la ou)
  - Delegación de hallazgos (inicialmente no definido en la ou)
  - Visualizar instancias en edición (inicialmente todos en la ou)
  - Permitir toma de sesión (inicialmente todos en la ou)
  - Permitir invitación a sesión (inicialmente todos en la ou)
  - Permitir monitoreo (inicialmente ninguno en la ou)
  - Permitir conferencia (inicialmente todos en la ou)
- Otros:
  - Cuenta inhabilitada: se copia, no se puede modificar.
  - Grupos de ejecución permitidos (colección de referencias a grupo). No se copia, se puede modificar.
  - Formato de página: no se copian, se pueden modificar.
  - Tiempo de expiración del token para servicio web: no se copia, no se comparten usuarios web service.

○ Opciones disponibles en dominios de acceso:

- Asignación de permisos.
  - Agregado a otros grupos de usuarios (locales, no externos)
  - Agregado a OU padre (local)
  - Agregado del usuario a los organigramas
  - Delegación de actividades y hallazgos
  - Cambio de algunas políticas
- *Grupos*: se copiarán al principio tanto el grupo como los usuarios y grupos contenidos en él. Sólo se podrá asignar permisos al grupo compartido y no a los objetos (usuarios y grupos) que se encuentren dentro. Los usuarios contenidos en el grupo compartido o

en algunos de los grupos que se encuentren dentro, heredarán estos permisos asignados al grupo compartido. No se podrán compartir roles.

- Datos que se copian: nombre. Estos datos no se pueden modificar en el dominio destino.
- Al compartir un grupo, el dominio externo se completa con el dominio de autenticación y no se puede modificar.
- Datos que NO se copian: OU padre, dominio local (pasa a ser el dominio actual), rol para dominios hijos, descripción, documentación. Todos estos datos quedarán vacíos en el dominio externo, heredando las configuraciones de la OU raíz del dominio externo.
- Opciones disponibles en dominios de acceso:
  - Asignación de permisos sólo al grupo compartido.
  - Agregado a otros grupos de usuarios padres (locales, no externos)
  - Agregado a OU padre (local)
  - No se puede agregar usuarios (externos o locales) al grupo compartido
- Si se comparten un usuario y un grupo a otro dominio, se mantendrá la relación entre estos en el dominio destino.
- No se podrá seleccionar un grupo externo dentro del modelo, por ejemplo en los permisos de ejecución de una RN, una TP o una TI.
- ~~OU: se copiarán al principio tanto la OU como los objetos contenidos, que pueden ser usuarios, grupos, dispositivos u otras OU. Para cada caso:~~
  - ~~○ Datos que se copian: nombre, descripción, documentación.~~
  - ~~○ Al compartir una OU, el dominio externo se completa con el dominio de autenticación y no se puede modificar.~~
  - ~~○ Datos que NO se copian: OU padre, versión y build del modelo, incluir nuevo dominio, dominio local (pasa a ser el dominio actual), dispositivos predeterminados.~~
  - ~~○ Políticas:~~
    - ~~▪ Relacionadas a la autenticación: no se copian, no se pueden modificar en el dominio destino:~~
      - ~~● Métodos de autenticación~~
      - ~~● Métodos de recuperación de contraseña~~
      - ~~● Forzar cambio de contraseña~~
      - ~~● Habilitar cambio de contraseña~~
      - ~~● Requiere completar datos personales en primer acceso~~
      - ~~● Tiempo de expiración de contraseña~~
      - ~~● Tiempo de validez del enlace para restablecer contraseña~~
      - ~~● Tiempo de validez de enlace para introducir contraseña~~
      - ~~● Rango horario permitido~~
      - ~~● Direcciones IP permitidas~~
      - ~~● Validación adicional ante autenticación para un nuevo dispositivo~~
    - ~~▪ Relacionadas con la cuenta del usuario: no se copian, no se pueden modificar en el dominio destino:~~
      - ~~● Tiempo de expiración de la cuenta~~
      - ~~● Tiempo sin acceso antes de deshabilitar la cuenta~~
      - ~~● Rango de fecha de validez de la cuenta~~
      - ~~● Cuenta inhabilitada~~
    - ~~▪ Relacionadas con la jerarquía en el organigrama: las opciones en las siguientes políticas son todos, pares y subordinados, subordinados o ninguno. Se copian y se pueden modificar.~~



- ~~Delegación de actividades~~
- ~~Consulta de actividades delegadas~~
- ~~Delegación de hallazgos~~
- ~~Visualizar instancias en edición~~
- ~~Permitir toma de sesión~~
- ~~Permitir invitación a sesión~~
- ~~Permitir monitoreo~~
- ~~Permitir conferencia~~
- \* ~~Otros:~~
  - ~~Notificación ante autenticación de un nuevo dispositivo (email, telegram). No se copia?, se puede modificar.~~
  - ~~Tiempo de inactividad para cierre automático de sesión. No se copia, se puede modificar.~~
  - ~~Tiempo de expiración del token para servicio web: no se copia, no se comparten usuarios web service.~~
- ~~Dudas:~~
  - \* ~~Estereotipo: OU u OU de sitios, se pueden compartir ou de sitios?~~
- ~~Opciones disponibles en dominios de acceso:~~
  - \* ~~Agregado a OU padre (externa o local)~~
  - \* ~~Agregado de otros objetos (externos o locales) a la OU compartida~~
  - \* ~~Cambio de algunas políticas~~
- *Dispositivos: se copiarán al principio y estarán disponibles para asignarles permisos dentro del dominio accesible.*
  - Datos que se copian: nombre, descripción, documentación,
  - Datos que NO se copian: OU padre, dominio local (pasa a ser el dominio actual), dominio externo (dominio origen), sitio local, sitio, dirección ip, puerto de comunicación.
  - Dudas:
    - Tipo de dispositivo: es una referencia a una entidad paramétrica (Impresora de documentos, Terminal punto de venta, Impresora fiscal, test. esa entidad dice si requiere controlador), el tipo de conexión (puerto serie, ethernet).
    - Colección de agentes: referencia a agente y a periférico. Qué pasa con el agente? Debe tenerlo instalado? Qué pasa sino?
    - Colección de controladores para modelo: referencia a modelo y a controlador.
  - Opciones disponibles en dominios de acceso:
    - Agregado a OU padre (local)
    - Consumo de dispositivo desde RN y funciones

No se podrán compartir agentes, controladores, protocolos, puestos de trabajo, sitios ni OU de sitios.

*Ejemplo:*

Dominio accesible: Dominio A.

Dominio de autenticación: Dominio B.

Objetos de acceso que comparte Dominio B:

- Usuarios: Jimena, Emmanuel.
- Grupos: Funcional (contiene a los usuarios Diego, Leandro y Jimena) y Desarrollo (contiene a usuario Emmanuel).

- Dispositivos: **Impresora4**.
- **OU Rosario** que contiene:
  - **Usuario Luis**.
  - **OU Administración**: contiene el usuario **Zulema**, el grupo **Jefas de administración** (que contiene los usuarios **Zulema** y **Cintia**) y el dispositivo **Impresora20**.
  - **Grupo Enterprise**: contiene grupo **Funcional** (contiene a los usuarios **Diego**, **Leandro** y **Jimena**) y al grupo **Arquitectos** (contiene los usuarios **Luis**, **Leandro** y **Diego**)

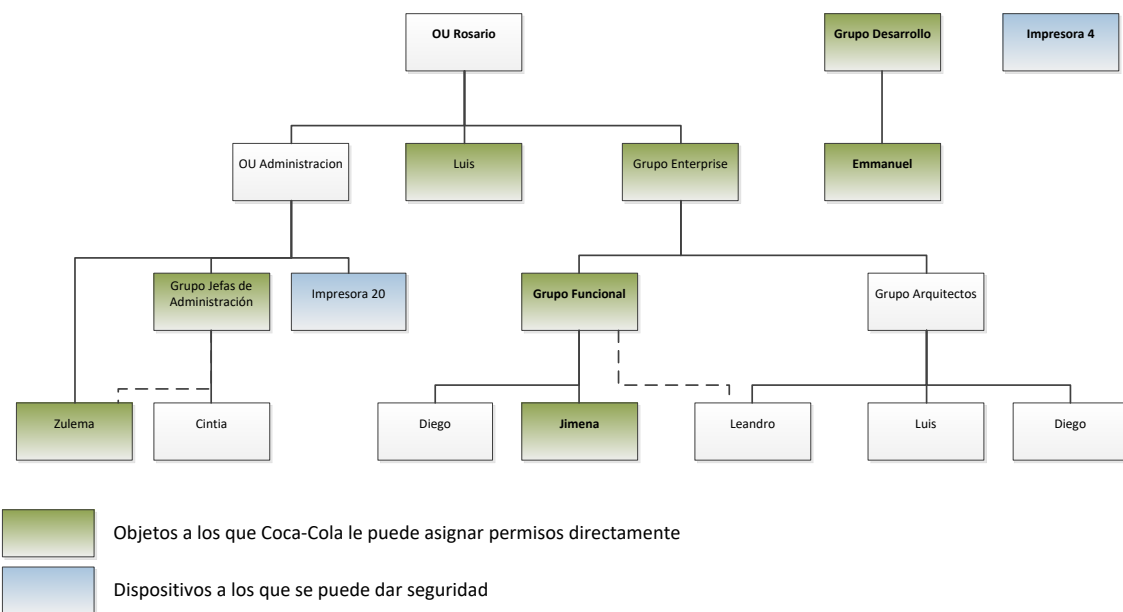
En **este** color: objetos a los que Dominio A le puede asignar permisos directamente.

En **este** color: dispositivos a los que se puede dar seguridad.

En **este** color: objetos que se copian en Dominio A pero no se les puede asignar permisos directamente.

En **este** color: OUs que se copian. No se asignan permisos a una OU.

En forma gráfica, el ejemplo sería:



En **negrita** los objetos que se establecieron a la hora de crear el vínculo de seguridad

### 2.3.4 Rechazo o eliminación de un vínculo y eliminación de objetos compartidos

Al rechazar un vínculo de seguridad, se eliminará toda la información referida a sus objetos de acceso y a la seguridad asignada a los mismos. De esta forma, si se crea un vínculo similar al rechazado, se deberán volver a definir los objetos de acceso. En el caso de que un objeto vuelva a ser definido como objeto de acceso, se deberán volver a otorgar los permisos correspondientes, quedando dichos permisos asociados al nuevo vínculo.

Eliminación de un usuario perteneciente a un vínculo de confianza: Si un usuario se inhabilita/elimina en el dominio de origen, se notifica a los dominios de acceso y se inhabilita/elimina en estos también, efectuando las acciones pertinentes (por ejemplo, dar de

baja los permisos específicos para dicho usuario o desconectarlo si se encuentra con una sesión activa). Si la referencia a un usuario se elimina en el dominio que validó el vínculo, entonces dicho usuario dejará de tener acceso a este dominio pero en el dominio de origen el usuario seguirá existiendo.

### 2.3.5 Eventos que se notifican entre dominios

- Alta, aprobación, rechazo y baja del vínculo
- Alta y baja de objetos compartidos, y modificación de una propiedad que se copia
- ~~Alta y baja de un objeto dentro de una OU compartida~~
- Alta y baja de un objeto dentro de un grupo compartido

### 2.3.6 Seguridad / Permisos necesarios para establecer un vínculo

Cada dominio podrá tener uno o varios usuarios *administradores de seguridad*, que gestionarán los usuarios dentro del dominio al cual pertenezcan y validarán los vínculos de seguridad con otros dominios. Cada *administrador* podrá otorgar a los usuarios del dominio los permisos que él posee, si cuenta con los derechos necesarios.

El permiso necesario para administrar los vínculos se llama “Administrar vínculo”.

#### Dominio (itmodeling01master.fastprg.com)

Grupo de usuarios		
quest		
Rol de administrador del dominio		
Rol de usuario final avanzado del dominio		
Rol de administrador de base de datos del do.		
Rol de editor del dominio		
Rol de usuario final del dominio		

Permiso	Entorno de desarrollo	
	Permitir	Den...
⊕ Administrar modelo	<input checked="" type="checkbox"/>	<input type="checkbox"/>
⊖ Administrar dominio	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Actualizar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Consultar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Administrar políticas	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Administrar vínculos	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Traducir	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input checked="" type="checkbox"/>	<input type="checkbox"/>

### 2.3.7 Historial de cambios

En la solapa *Historial de versiones* del dominio, se visualizarán todos los cambios realizados en cada vínculo.

### 2.3.8 Autenticación de un usuario externo

Los usuarios externos podrán acceder al *dominio vinculado*, realizando la autenticación en su dominio original, a través del vínculo en cuestión. Es decir, el usuario debe ingresar a la url del dominio de acceso y en el campo usuario debe especificar el dominio de autenticación de la siguiente manera: dominio\usuario. En este caso, no se visualizará la opción para restablecer la contraseña y en su lugar, se visualizará el dominio de autenticación.

## 2.4 Políticas de seguridad

Las *políticas de seguridad* podrán configurarse en un dominio, en las unidades organizacionales y en los usuarios, pero sólo se aplicarán a las cuentas de usuario (salvo en los últimos 6 ítems, en los cuales se aplicarán al dominio). A continuación, se detalla cada política, su valor predeterminado y desde dónde se podrá configurar.

Política	Descripción (tooltip)	Valores	Valor predeterminado	Dominio o Usuario		Usuario
Tiempo máximo sin acceso antes de inhabilitar cuenta	Define la cantidad de días (el 0 indicará nunca) luego de los cuales se inhabilitará una cuenta si el usuario no accede a la misma.	[0 - 999]	30	si	si	no
Tiempo de expiración de las cuentas	Define la cantidad de días (el 0 indicará nunca) luego de los cuales se inhabilitarán las cuentas de los usuarios, contando desde el día de la creación de la cuenta.	[0 - 999]	0	no	si	si
Rango de fecha de validez de la cuenta	Define el rango de fechas en el cual serán válidas las cuentas de usuario. Se podrá definir opcionalmente un rango de fechas no acotado, es decir, fecha de inicio pero no de fin o viceversa.	[siempre (las 2 fechas vacías), rango de fechas]	siempre	no	si	si

Reintentos de acceso fallidos consecutivos antes de bloquear cuenta	Define la cantidad de intentos fallidos luego de los cuales la cuenta de usuario se bloqueará, esto es independiente del dispositivo desde el cual intenta autenticarse el usuario e independientemente del tiempo transcurrido entre cada intento. Se contarán todos los intentos fallidos de acceso del usuario a partir de una autenticación correcta; es decir que cada vez que un usuario acceda correctamente, se volverá a iniciar la cuenta.	[1 - 9]	5	s i	n o	no
Tiempo de bloqueo de cuenta ante accesos fallidos consecutivos	Define la cantidad de minutos durante la cual se bloqueará una cuenta por primera vez luego de una cantidad de accesos fallidos consecutivos, a partir de esta cantidad se irá incrementando el tiempo de bloqueo, sumándose 5 minutos. Se volverá a iniciar la cuenta una vez que el usuario acceda correctamente. El 0 indica que no se establecerá una cantidad de minutos y que sólo el administrador podrá desbloquear la cuenta, habilitándola nuevamente.	[0 - 999]	10	s i	n o	no
Bloquear cuenta	Indica si la cuenta del usuario se encuentra bloqueada. De ser así, el mismo, no podrá ingresar al sistema o podrá restablecer su contraseña con algún método de recuperación de la misma. Solo cuando la cuenta esté bloqueada por el sistema un usuario con los derechos suficientes podrá desbloquearla. Esto significa que un administrador no podrá bloquear manualmente una cuenta.	[si, no]	no	n o	n o	si (menos el usuario admin)
Visualizar instancias en edición	Todo usuario podrá visualizar las instancias en edición creadas por él mismo. Esta política indica si puede ver los datos en edición de otros usuarios.	[todos, pares y subordinados, subordinados, no]	Todos	s i	s i	Si (menos usuarios de WS)

Delegación de actividades	Indica si un usuario puede delegar las actividades que le fueron concedidas, a todos los usuarios, a pares y subordinados, sólo a subordinados, o no puede delegar sus actividades.	[todos, pares y subordinados, subordinados, no delegar]	Todos	s i	s i	Si (menos usuarios de WS)
Consulta de actividades delegadas	Indica si un usuario puede consultar las actividades delegadas de todos los usuarios, de pares y subordinados, sólo a subordinados, o no puede consultar las actividades delegadas de los demás.	[todos, pares y subordinados, subordinados, no consulta ]	Todos	s i	s i	Si (menos usuarios de WS)
Delegación de hallazgos	Indica si un usuario puede delegar los hallazgos, a todos los usuarios, a pares y subordinados, sólo a subordinados, o no puede delegar los hallazgos.	[todos, pares y subordinados, subordinados, no delegar]	Ninguno	s i	s i	Si (menos usuarios de WS)
Grupos permitidos para ejecución	Indica los grupos de usuarios con cuyos permisos se podrán ejecutar las Reglas de Negocio, las Tareas y Planes de integración, y las Tareas Programadas.	Lista de selección múltiple de grupos	Ninguno	N o	N o	Si (menos usuarios de WS)
Inhabilitar cuentas	Indica si las cuentas de usuario se encuentran inhabilitadas. De ser así, dichos usuarios, no podrán ingresar al sistema.	[si , no]	no	n o	s i	si
Rango horario permitido	Define el horario en que los usuarios podrán utilizar el sistema. Al ingresar se valida que el horario se encuentre dentro de este rango y si se cumple el horario limite, se cierra la sesión del usuario. Si se configura como “horario acotado” se deberá definir una hora de inicio, una hora de fin y una zona horaria.	[sin restricciones , horario acotado ]	Sin restricciones	s i	s i	si

Direcciones IP permitidas <sup>1</sup>	Indica las direcciones IP desde las cuales los usuarios podrán ingresar.	Colección de direcciones IP o rangos	Sin restricciones	s i	s i	si
Permitir mantener sesión iniciada	Indica si en la pantalla de autenticación, los usuarios tendrán la opción para mantener la sesión iniciada o no. Mantener la sesión iniciada implica que cada vez que se ingrese al sistema, sin ingresar las credenciales, se abrirá la sesión del último usuario autenticado correctamente (un auto-login). Además, si un usuario activó esta opción, mientras esté conectado NO caducará su sesión. En cambio si no está conectado, si caducará la sesión en el servidor. Ahora bien, si el usuario no activó esta opción, al caducar su sesión, se redirigirá hacia la página de login (y si recordó sus credenciales, los valores de las mismas aparecerán auto-completados).	[si, no]	[no]	s i	n o	no
Tiempo de inactividad máximo para cierre automático de sesión	Indica la cantidad de minutos luego de la cual se cerrará una sesión en el servidor si no se detecta actividad del usuario dentro del sistema. Esta opción depende de si el usuario decidió mantener la sesión activa en cuyo caso no se cerrará su sesión, aunque haya sobrepasado el tiempo de inactividad.	[1 - 999]	15	s i	s i	no
Tiempo de inactividad máximo para cierre automático de autenticación	Indica la cantidad de minutos luego de la cual se descartarán todos los datos ingresados en la pantalla de autenticación si no se detecta actividad del usuario (inclusive si ya ingresó algunas	[1 – 9]	1	s i	n o	no

<sup>1</sup> Tener en cuenta IPv4, IPv6.

	credenciales y se piden métodos extras de autenticación). Se redirige a la primera pantalla de login con los campos de las credenciales vacíos.					
Métodos de autenticación adicionales	Un usuario se podrá autenticar utilizando uno de varios métodos. El ingreso de contraseña, siempre es requerido como mínimo pero se pueden requerir adicionalmente dispositivos de autenticación tales como verificación de código enviado por email, aplicación OTP, Telegram, verificación biométrica, certificado digital. Será requerido como mínimo siempre autenticarse con contraseña.	Lista de métodos de autenticación, con selección múltiple.	-	s	s	Si (los usuarios de WS tienen solo otp)

La política “Métodos de autenticación permitidos” tiene como particularidad que en las OU y en los usuarios no se puede redefinir los métodos seleccionados en el dominio, pero sí se pueden agregar más métodos.

Forzar cambio de contraseña en el próximo acceso	Define si los usuarios deberán cambiar su contraseña al acceder al sistema la próxima vez por pantalla. Esta opción se inhabilitará automáticamente en el usuario cuando el mismo realice el cambio correctamente.	[si, no]	No / Si para usuarios WS	s	s	si
Forzar carga de datos personales en primer acceso	Indica si los usuarios deberán ingresar sus datos personales en el primer acceso. Luego del primer login correcto, se abrirá el formulario de las preferencias del usuario, donde el mismo deberá ingresar sus datos personales, inicialmente los datos solicitados serán teléfono y dirección.	[si, no]	si	s	s	no
Habilitar cambio de contraseña	Define si los usuarios podrán cambiar su contraseña. El cambio de contraseña de un usuario sólo se realizará a través del envío de email, no se realizará directamente en las preferencias del usuario.	[si, no]	si	s	s	si
Longitud mínima de contraseña	Indica la longitud mínima que deberán tener las contraseñas de los usuarios. Cuando un	[6 - 99]	6	s	n	no



	usuario genere o modifique su contraseña de acceso, el sistema validará que la cantidad de caracteres definidos no sea mayor al valor definido para ésta política en el dominio al cual pertenece.					
Tiempo de expiración de la contraseña	Indica la cantidad de días luego de los cuales dejará de tener validez la contraseña de cada usuario desde la última fecha de cambio de la misma. El valor 0 indica que no se tomará en cuenta esta directiva. Durante los siete días anteriores (como máximo) a la expiración de la contraseña, se avisará al usuario que debe cambiarla mediante una notificación que se mostrará en cada acceso. Cuando la contraseña expire, el usuario deberá ingresar una nueva por pantalla.	[0 - 999]	0	s i	s i	no
Cantidad de contraseñas anteriores que no podrán reutilizarse	Indica la cantidad de contraseñas anteriores que no podrán volver a utilizar los usuarios.	[1 - 99]	3	s i	n o	no
Métodos de restablecimiento de contraseña	<p>Permite establecer el o los métodos de recuperación de contraseña. Un usuario podrá recuperar su contraseña, indicando los métodos: dirección de e-mail, <del>envío de SMS</del>, Telegram.</p> <p>En el caso de seleccionar más de una opción, el link se manda por varios medios, pero sólo será válido una vez.</p> <p>Es importante aclarar que si se define un método de restablecimiento, éste se sumará a los métodos de autenticación adicionales definidos para el usuario. Por ejemplo, si en los métodos de autenticación adicionales se configura OTP y el método de recuperación de contraseña es Email, se deberán</p>	Lista de métodos de recuperación de contraseñas, con selección múltiple.	e-mail	s i	s i	no

	<p>ingresar correctamente ambos códigos para poder restablecer la contraseña. Si en ambas políticas está definido el mismo método, ejemplo email, sólo se solicitará una vez.</p> <p><del>Esta política sólo se visualizará en el caso de que “contraseña” sea un método de autenticación permitido.</del></p>					
Tiempo de validez del enlace para restablecer la contraseña	<p>Permite establecer el tiempo en horas en el cual es válido el link para restablecer la contraseña.</p> <p>Si este tiempo caduca, se podrá utilizar el comando “restablecer contraseña” sobre el usuario para reenviar el link o que el usuario vuelva a indicar que olvidó su contraseña.</p> <p><del>Esta política sólo se visualizará en el caso de que haya un método de restablecimiento de contraseña definido.</del></p>	[1-999] horas	1 hora	s i	s i	no
Tiempo de validez del link para ingresar la primera contraseña	<p>Permite establecer el tiempo en horas en el cual es válido el link para ingresar por primera vez la contraseña.</p> <p>Si este tiempo caduca, se podrá utilizar el comando “restablecer contraseña” sobre el usuario para reenviar el link.</p> <p><del>Esta política sólo se visualizará en el caso de que “contraseña” sea un método de autenticación permitido.</del></p>	[1-999] horas	48 horas	s i	s i	no
Validación adicional ante una autenticación en un nuevo dispositivo	<p>Permite establecer el o los métodos de validación extra, ante una autenticación en un nuevo dispositivo. Las opciones disponibles serán: dirección de e-mail, aplicación OTP, Telegram, <del>dispositivo OTP.</del></p>	Lista de métodos de validación extra, con selección múltiple.	e-mail	s i	s i	no

Notificación ante una autenticación en un nuevo dispositivo	Permite establecer el o los métodos de notificación al usuario, ante una autenticación en un nuevo dispositivo. Las opciones disponibles serán: envío de e-mail, Telegram. El contenido de la notificación tendrá un link para bloquear la cuenta en ese dispositivo.	Lista de métodos de notificación, con selección múltiple.	e-mail	si	si	no
Toma de sesión	Indica si se permitirá la toma de sesión, mediante la cual un usuario podrá ver la pantalla de otro, previa confirmación.	[todos, pares y subordinados, subordinados, no permitir]	todos	si	si	Si (menos usuarios de WS)
Invitación a sesión	Indica si se permitirá la invitación a tomar la sesión propia, mediante la cual un usuario podrá ver la pantalla de otro, previa confirmación.	[todos, pares y subordinados, subordinados, no permitir]	todos	si	si	Si (menos usuarios de WS)
Monitorización	Indica si se permitirá la monitorización, mediante el cual un usuario podrá ver la pantalla de otros, sin que éstos sepan que están siendo supervisados.	[todos, pares y subordinados, subordinados, no permitir]	subordinados	si	si	Si (menos usuarios de WS)
Coaching	Indica si se permitirá el coaching, mediante el cual un usuario podrá seleccionar otros usuarios y darles la posibilidad de ver lo que él realiza.	[todos, pares y subordinados, subordinados, no permitir]	todos	si	si	Si (menos usuarios de WS)
Dominios externos que pueden tomar	Indica los dominios que pueden tomar sesión a los usuarios del dominio local,	Colección de dominio	Ninguno	Si	No	No

sesión	independientemente de los vínculos de confianza.	s				
Dominios externos que pueden invitar a sesión	Indica los dominios que pueden invitar a tomar sesión a los usuarios del dominio local, independientemente de los vínculos de confianza.	Colección de dominios	Ninguno	S	N	No
Dominios externos que pueden invitar a coaching	Indica los dominios que pueden invitar a una sesión de coaching a los usuarios del dominio local, independientemente de los vínculos de confianza.	Colección de dominios	Ninguno	S	N	No
Dominios externos que pueden utilizar modelos del dominio local	Indica los dominios externos que podrán usar los modelos del dominio local como modelos padres de sus modelos, sin necesidad de comprarlos mediante el Market Place. Es decir, al crear un modelo en alguno de los dominios externos indicado en esta política, podrán elegir como modelo padre a un modelo de mi dominio.	Colección de dominios	Ninguno	S	N	No
Políticas de actualización de Modelos Padres	Un <i>Modelo Hijo</i> podrá recibir actualizaciones desde el Modelo padre, es decir si el Modelo Padre hace cambios en el Modelo Padre las mismas podrán ser implementadas en el Modelo Hijo. Estas actualizaciones sólo aplican a los <i>Builds</i> que están en Estado Aprobado y el Modelador indicó que están disponibles para que se instale en los Modelos Hijos. Para más información, ver el documento <a href="#">Versionado</a> .	[ Automática por <i>builds</i> , automática versiones y <i>builds</i> , Manual ]	Automática por <i>builds</i>	S	N	No
Tiempo de expiración del token para web service	Indica la cantidad de horas luego de las cuales dejará de tener validez el token otorgado a un usuario WS para ejecutar actividades en una aplicación.	[1 - 24]	24	S	S	Si (solo para usuarios ws)

Geolocalización	Se podrá elegir entre 3 valores, y según el valor elegido, se completará el registro de aplicación. Mas info en: <a href="http://innovacion:26607/EnterpriseFuncional/Seguridad/Pol%C3%ADtica%20de%20georeferenciaci%C3%B3n.docx">http://innovacion:26607/EnterpriseFuncional/Seguridad/Pol%C3%ADtica%20de%20georeferenciaci%C3%B3n.docx</a>				
-----------------	--	--	--	--	--

Por lo tanto, las cuentas de los usuarios pueden estar en uno de los siguientes estados:

- ✓ Activa.
- ✓ Inhabilitada.
- ✓ Bloqueada.

Si deja de ser válida la sesión de un usuario en el sistema, tanto por un cambio en la configuración de una política de seguridad (por ejemplo, se inhabilita el usuario), como porque la política lo establece (por ejemplo, finaliza el rango de horas permitido), entonces se cerrará automáticamente su sesión.

Si el usuario no cierra su sesión, sólo cierra el browser o apaga la PC, la sesión seguirá activa durante el tiempo de inactividad máximo configurado en sus políticas.

Las políticas de las cuentas y contraseñas de los *usuarios de WS* detallados en la sección [Usuarios y grupos de usuarios](#), aplicarán cuando dichos usuarios se autentifiquen en el sistema. Por ejemplo: permitir cambio de contraseña, sólo estará disponible desde el sistema, y no mediante un método de WS.

El *tooltip* de cada política de seguridad se visualizará de acuerdo al documento de [Estándares de interfaz de usuario](#), por ejemplo:

La *contraseña* deberá contener como mínimo tres de las cuatro categorías siguientes: minúsculas, mayúsculas, números y símbolos. Además, no deberán contener el nombre del usuario de la cuenta o parte del nombre completo del usuario que exceda de dos caracteres consecutivos. Por ejemplo, la contraseña del usuario juliamartinez no podrá contener "juli".

Si se establece un vínculo de seguridad con un Dominio de autenticación, automáticamente se agregará dicho dominio a la colección de dominios con permiso para tomar sesión, invitar a la toma de sesión, e invitar a coaching. Para que un dominio externo pueda realizar una monitorización sobre usuarios del dominio local, se deberá establecer obligatoriamente un vínculo de confianza.

Una vez establecido un vínculo de confianza o una política de seguridad que indique que los usuarios de un dominio externo podrán supervisar a los usuarios del dominio local, se deberán especificar los permisos correspondientes en la seguridad de los usuarios externos para concretar dicha supervisión.

Se tendrá en cuenta el documento de Estándares de interfaz de usuario para diferenciar los permisos de usuarios y grupos de usuarios -hijos- diferentes de aquellos definidos para el grupo al que pertenecen -padre- y para distinguir los permisos de los grupos de usuarios -padres- que contengan un objeto -hijo- con dicho permiso definido de otra manera. La interfaz para definir *Políticas de Seguridad* del Dominio será:

dominio.com

General | Vínculos | Historial de Versiones | Seguridad | Documentación

Nombre del dominio: dominio.com

Información: 30 licencias habilitadas.

### Propiedades de las cuentas

Tiempo máximo sin acceso antes de inhabilitar cuenta: 60 días

Reintentos de acceso fallidos consecutivos: 3 reintentos

Tiempo de bloqueo de cuenta: 5 minutos

Delegación de permisos: Todos los usuarios

### Propiedades de los accesos

Rango horario permitido: De lunes a domingo, de 0 a 24 hs

Direcciones IP permitidas: Sin restricciones

Permitir recordar último usuario identificado en equipo: Recordar sólo usuario

Tiempo de inactividad máximo: 2 minutos

Métodos de autenticación permitidos:

- Requerir usuario y contraseña: ☒
- Requerir dispositivo de autenticación: ☒

dominio.com

General | Vínculos | Historial de Versiones | Seguridad | Documentación

### Propiedades de las contraseñas

Forzar cambio de contraseña en el próximo acceso: ☐

Forzar carga de datos personales en primer acceso: ☒

Permitir cambio de contraseña: ☒

Longitud mínima de contraseña: 8 caracteres

Tiempo de expiración de la contraseña: 0 días

Cantidad de contraseñas anteriores que no podrán reutilizarse: 3 contraseñas

Métodos de recuperación de contraseñas:

- Dirección e-mail: ☒
- Enviar SMS: ☐
- Requerir dispositivo OTP: ☐

### Propiedades de supervisión

Toma de sesión: Todos los usuarios

Invitación a sesión: Todos los usuarios

Monitorización: Sólo a subordinados

Coaching: Todos los usuarios

dominio.com

General Vínculos Historial de Versiones Seguridad Documentación

Permitir cambio de contraseña ☒

Longitud mínima de contraseña 8 caracteres

Tiempo de expiración de la contraseña 0 días

Cantidad de contraseñas anteriores que no podrán reutilizarse 3 contraseñas

Métodos de recuperación de contraseñas

Dirección e-mail ☒

Enviar SMS ☐

Requerir dispositivo OTP ☐

**Propiedades de supervisión**

Toma de sesión Todos los usuarios

Invitación a sesión Todos los usuarios


Monitorización Sólo a subordinados

Coaching Todos los usuarios

Dominios externos que pueden tomar sesión

Dominios externos que pueden invitar a sesión

Dominios externos que pueden invitar a coaching



El rango horario será por defecto de lunes a domingo en cualquier horario. Para restringirlo, se deberá hacer clic en , seleccionar la/s celda/s y definir si el acceso en ese rango estará permitido o denegado. La selección podrá realizarse mediante *drag & drop* o clic (o su equivalente en otras interfaces). Cada vez que se realice una selección, se invertirá el estado de la celda seleccionada. Además, desde el menú contextual sobre la grilla se presentará la opción "Configurar horario" para establecer un horario específico. Esta restricción se aplicará por defecto a todos los usuarios del dominio, así como a los usuarios de los dominios que hayan establecido un vínculo de seguridad. Cuando un usuario realice una correcta autenticación, se validará el rango horario permitido, junto con las demás políticas de seguridad, tomando como referencia la zona horaria del sitio al cual el usuario desee acceder.

Horario de Acceso

**Definir el horario de acceso al sistema:**

Haqa clic en el/los día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lunes																								
Martes																								
Miércoles																								
Jueves																								
Viernes																								
Sábado																								
Domingo																								

 Acceso Permitido  Acceso No Permitido

De lunes a domingo, de 0 a 24 hs

Horario de Acceso

**Definir el horario de acceso al sistema:**  
Haga clic en el/los día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lunes																								
Martes																								
Miércoles																								
Jueves																								
Viernes																								
Sábado																								
Domingo																								

Acceso Permitido
Acceso No Permitido

De lunes a domingo, de 0 a 24 hs

Horario de Acceso

**Definir el horario de acceso al sistema:**  
Haga clic en el/los día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lunes																								
Martes																								
Miércoles																								
Jueves																								
Viernes																								
Sábado																								
Domingo																								

Acceso Permitido
Acceso No Permitido

De lunes a domingo, de 0 a 15 hs

Horario de Acceso

**Definir el horario de acceso al sistema:**  
Haga clic en el/los día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lunes																								
Martes																								
Miércoles																								
Jueves																								
Viernes																								
Sábado																								
Domingo																								

Acceso Permitido
Acceso No Permitido

De lunes a domingo, de 0 a 15 hs



**Horario de Acceso**

**Definir el horario de acceso al sistema:**

Haga clic en el/dos día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Lunes																
Martes																
Miércoles																
Jueves																
Viernes																
Sábado																
Domingo																

☐ Acceso Permitido
 ☐ Acceso No Permitido

De lunes a domingo, de 0 a 15 hs

**Configurar horario**

**Definir el rango horario específico permitido:**

Completar el horario de comienzo y fin.

Hora Inicio: 17:15 Hora Fin: 19:00

Martes de 19:15 hs a 19:00 hs

23

Las *políticas de seguridad* se podrán redefinir por unidad organizacional, y por usuario. Por ejemplo, si el rango horario definido en el dominio es de lunes a viernes de 9 a 18 hs, podrá redefinirse para una OU o para un usuario, otro rango.

Cuando existan usuarios y OUs configurados con políticas diferentes a las definidas en el dominio y se modifique una política de seguridad en dicho dominio, esto no afectará a las políticas definidas individualmente en los usuarios y OUs, sino sólo a los nuevos objetos y a aquellos que no hayan cambiado dicha política. Se podrá restablecer una política a los objetos del dominio (usuarios y OUs), de acuerdo a lo definido en el documento de Estándares de interfaz de usuario. Esto también aplicará para restablecer políticas en los objetos que pertenezcan a una OU. En este caso, los hijos serán los objetos contenidos (OUs y usuarios) y el padre será el objeto que contiene dichos hijos (podrá ser una OU o el dominio). A su vez, un objeto (OU) podrá ser padre e hijo al mismo tiempo. Si cambia una política en el padre, se restablecerá sólo en los hijos que no hayan modificado esta política. Los formatos de visualización de las políticas en cada caso, serán los detallados en Estándares de interfaz de usuario.

Cuando en un dominio se realice un cambio con respecto a las políticas de seguridad, por ejemplo, un cambio de la complejidad de la contraseña se presentará el siguiente comportamiento:

- 1) Todas las contraseñas de los usuarios almacenadas pasarán a ser consideradas como inválidas. Forzando al usuario a modificarla.
- 2) Se enviará un email de recuperación de contraseña al buzón de correo de los usuarios informando que deben realizar el cambio de contraseña.
- 3) El email enviado contendrá un link que al seleccionarlo re-direccionará al usuario a la ventana de login donde se mostrará el nombre del usuario en sólo lectura y los campos para ingresar la contraseña dos veces: uno para la nueva contraseña y otro para confirmarla.
- 4) En caso de realizar el cambio exitosamente se mostrará un mensaje al usuario indicando que el cambio fue realizado exitosamente y deberá autenticarse nuevamente introduciendo el usuario y la nueva contraseña. No se realizará el ingreso automáticamente.

## 2.5 Seguridad del Dominio

En la solapa *Seguridad* del dominio se asignarán permisos y denegaciones a todos los usuarios y grupos de usuarios del dominio con una *Lista de Control de Acceso (ACL)*. Esta ACL tendrá los permisos generales que harán referencia a las acciones disponibles en el dominio (crear usuarios, dispositivos, etc.) como así también a las acciones disponibles en el administrador de modelos (crear, modificar modelos, etc.):

- ✓ *Administrar dominio:*
  - consultar/modificar/administrar políticas de seguridad/administrar vínculos/traducir/administrar permisos.
- ✓ *Administrar modelos:*  
crear/consultar/modificar/eliminar/restaurar/ejecutar/publicar/desvincular de padre/modificar modelos de dispositivos disponibles/traducir/administrar permisos (consultar y modificar).
- ✓ *Administrar cuentas de notificaciones:*  
crear/consultar/modificar/eliminar/restaurar/traducir/consultar seguridad/actualizar seguridad
- ✓ *Administrar empresas:*  
crear/consultar/modificar/eliminar/restaurar/consultar/consultar seguridad/actualizar seguridad
- ✓ *Administrar agentes:*  
crear/consultar/modificar/eliminar/restaurar/consultar/consultar seguridad/actualizar seguridad
- ✓ *Administrar controladores y protocolos:*  
crear/consultar/modificar/eliminar/restaurar/consultar/consultar seguridad/actualizar seguridad

El detalle de los permisos en cada objeto de seguridad se encuentra en la sección “Seguridad de objetos”.

dominio.com

General Vínculos Historial de Versiones Seguridad Documentación

**Definir la seguridad para los usuarios y grupos de usuarios:**

Haga clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Usuario/Grupo
administradores
admin
ivasco

Permiso	Permitir	Denegar
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Modificar	<input type="checkbox"/>	<input type="checkbox"/>
Administrar políticas de seguridad	<input type="checkbox"/>	<input type="checkbox"/>
Administrar vínculos	<input type="checkbox"/>	<input type="checkbox"/>
Traducir	<input type="checkbox"/>	<input type="checkbox"/>
▶ Administrar permisos	<input type="checkbox"/>	<input type="checkbox"/>
▼ Administrar Modelos	<input type="checkbox"/>	<input type="checkbox"/>
Crear	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Modificar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>
Restaurar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ejecutar	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Aclaración: dentro del permiso “Administrar permisos” de cada elemento existirá la posibilidad de consultar, y la de modificar.

Los usuarios que tengan el permiso “*Administrar permisos*” de una sección, podrán tanto otorgar como denegar los permisos de esa sección a otros usuarios. Sin embargo, esto no implica que el usuario *Administrador* cuente con los permisos que otorgue o deniegue. Por ejemplo, si un usuario admin tiene habilitada la modificación de permisos pero tiene denegado Administrar vínculos, de todas formas admin podrá otorgar permisos a otros usuarios para Administrar vínculos, aunque no tenga ese permiso habilitado. También podrá permitir administrar permisos de dicha sección a otros usuarios.

## 2.6 Federación<sup>2</sup>

Una *federación* es una colección de dominios que han establecido confianza. Uno de estos dominios será el administrador de la federación. El nivel de confianza puede incluir sólo autenticación, incluir autenticación y autorización, etc.

Mediante soluciones de *Identidad Federada*<sup>3</sup>, un usuario puede utilizar la misma identificación personal (típicamente usuario y contraseña) para identificarse en redes de diferentes sectores o incluso empresas. De este modo las empresas pueden compartir información sin tener que compartir tecnologías de directorio, seguridad y autenticación.

El sistema deberá estar preparado para formar parte de una *federación*.

<sup>2</sup> Esta funcionalidad se describirá en detalle para incorporar en el Release 2 de la aplicación.

<sup>3</sup> Tener en cuenta productos como Microsoft Active Directory Federation Services 2.0

## 2.7 Integración con servicios de directorio<sup>4</sup>

Un *servicio de directorio* es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Por ejemplo, en entornos Microsoft, Active Directory.

El sistema deberá estar preparado para interactuar con un *servicio de directorio*. La administración de usuarios y recursos podrá realizarse desde el servicio de directorio replicándose en el sistema, y viceversa.

## 3 Administración de objetos

Los *objetos* podrán ser:

- ✓ *Unidades organizacionales de sitios*
- ✓ *Grupos de sitios*
- ✓ *Sitios*
- ✓ *Unidades organizacionales*
- ✓ *Grupos de usuarios*
- ✓ *Usuarios*
- ✓ *Dispositivos*

El dominio contendrá los objetos. Cada objeto pertenece a un sólo dominio (que será su dominio local).

Las OU sirven para organizar los objetos. Una OU puede contener usuarios, grupos de usuarios, dispositivos y otras OU. Cada uno de estos objetos podrá pertenecer a una sola OU.

Lo mismo ocurre para la OU de sitios con los sitios y grupos de sitios.

En lo que respecta a los grupos, un grupo de usuarios (o de sitios) puede contener varios usuarios (o sitios) y grupos de usuarios (o de sitios), y a su vez, un usuario (o sitio) puede estar en varios grupos.

Un usuario o grupo de usuarios podrá tener los siguientes *privilegios* sobre una acción:

- ✓ *Permiso*: indica que una acción podrá realizarse.
- ✓ *Permiso no definido*: indica aquellas acciones de las cuales no se especifica si se podrán realizar o no.
- ✓ *Denegación*: indica que una acción no podrá realizarse.

Las *denegaciones* siempre tendrán prioridad frente a los *permisos* y a los *permisos no definidos*. Si un permiso no está definido, la acción no podrá realizarse, a menos que el objeto herede dicho permiso de algún grupo que lo contiene.

Si un usuario no tiene permiso sobre un componente, el mismo no podrá ser visualizado por dicho usuario. Adicionalmente, si un usuario no tiene permiso o tiene denegada una acción (ya sea heredada de un grupo o definida en forma particular), no podrá visualizarla en ningún lugar donde esté definida.

La creación de un nuevo objeto podrá hacerse directamente en el dominio, desde el panel de navegación, dentro de la sección 'Dominio', haciendo clic alternativo e indicando el nuevo objeto.

---

<sup>4</sup> Esta funcionalidad se describirá en detalle para incorporar en el Release 2 de la aplicación.

### 3.1 Unidades organizacionales (OU)

Las *unidades organizacionales (OU)* son contenedores que se utilizan para organizar *objetos* dentro de un dominio. Podrán contener cuentas de usuarios, grupos de usuarios, dispositivos y otras OU. Esto permitirá administrar las *políticas de seguridad*. Una OU podrá contener referencias a usuarios y grupos de usuarios de otros dominios. Se podrán definir OU por departamentos jerárquicos, por zonas geográficas, etc.

- ✓ Un *dominio de seguridad* se podrá dividir en n *unidades organizacionales*.
- ✓ Una *unidad organizacional* podrá tener ninguno, uno o varios usuarios *administradores de seguridad*.
- ✓ Un *administrador de seguridad* podrá administrar una o varias *unidades organizacionales*.
- ✓ Una *unidad organizacional* podrá contener n *objetos*.
- ✓ Una *unidad organizacional* podrá contener n *unidades organizacionales*.
- ✓ Un *objeto* podrá pertenecer a una única *unidad organizacional*.

El *administrador de seguridad* podrá administrar las *políticas de seguridad* de una o varias OU (dar de alta usuarios, definir la contraseña, etc.), y además podrá configurar los permisos y denegaciones de los objetos dentro de estas OU. Esto se especificará en la solapa Seguridad de las mismas. Dicho usuario sólo podrá ver las OU que administra.

Al crear un usuario dentro de una OU, el mismo heredará las políticas de seguridad de dicha OU. ~~También se podrán crear usuarios dentro del dominio. En este caso, los usuarios obtendrán las políticas configuradas en el mismo. Luego se podrán redefinir las políticas para cada usuario.~~

Cada vez que se cree un dominio, AI creará la OU raíz y la OU raíz de sitios. La primera contendrá usuarios, grupos de usuarios, dispositivos, puestos de trabajo y otras OU; y la segunda contendrá sitios, grupos de sitios y otras OU de sitios. Ambas OU tendrán ciertas limitaciones, como por ejemplo, no se podrán eliminar ni que hereden de otra OU (siempre serán padres de otros objetos, nunca hijos).

Cada *Unidad Organizacional* tendrá las siguientes propiedades:

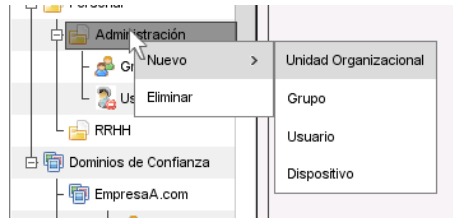
- ✓ *General*: ubicación, nombre, descripción, **calendario**, los dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.), **idiomas preferidos de UI y de datos para autenticación de usuarios (hereda del dominio)** y políticas de seguridad (ver [tabla](#) de políticas de seguridad). **Inicialmente, cada OU heredará el calendario, los dispositivos, los idiomas y las políticas de seguridad de la OU padre.** Estas propiedades **podrán redefinirse, respetando lo detallado para herencia en el documento [Estándares de interfaz de usuario](#).**
- ✓ *Historial de Versiones*: se podrá mantener un historial de versiones de cada OU, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contiene la lista de permisos y denegaciones de los usuarios y grupos de usuarios sobre la OU (ver [tabla](#) de solapa "Seguridad").
- ✓ *Documentación*: contendrá la documentación específica de la OU.

Siempre se validará que el idioma preferido sea uno de los que se encuentran seleccionados en la lista de idiomas disponibles en el dominio.

La única propiedad obligatoria será nombre. ~~Las OU podrán tener el mismo nombre si se encuentran en diferentes ubicaciones. No se podrá crear ni arrastrar una OU en una ubicación, si existe otra OU con el mismo nombre.~~

La administración de usuarios y grupos de usuarios hará referencia tanto a los que se encuentren localizados en dicha OU, como así también a los localizados en las OUs que contenga la misma.

A continuación, se muestra la creación de la OU “Zona Norte” y las diferentes propiedades de dicha OU ubicadas en solapas.



**Nueva OU** ✕

General | Historial de Versiones | Seguridad | Documentación

Ubicación: dominio.com > Personal > Administración

Nombre (\*) Zona Nor

Descripción

Calendario Calendario Predeterminado

Idioma preferido para autenticación de usuarios (\*) Español (Argentina)

---

**Propiedades de las cuentas**

Tiempo máximo sin acceso antes de inhabilitar cuenta 60 días

Tiempo de expiración de las cuentas 0 días

Rango de fechas de validez de las cuentas desde hasta

Delegación de permisos Todos los usuarios

Inhabilitar cuentas

---

**Propiedades de los accesos**

Rango horario permitido De lunes a domingo, de 0 a 24 hs

Direcciones IP permitidas Sin restricciones

Permitir recordar último usuario identificado en equipo Recordar sólo usuario

Tiempo de inactividad máximo para cierre automático de sesión 2 minutos

Métodos de autenticación permitidos

- ✓ Un *dominio* podrá contener n *sitios*.
- ✓ Un *dominio* podrá contener n *grupos de sitios*.
- ✓ Un *usuario* podrá acceder a n *sitios* o *grupos de sitios*.
- ✓ Un *grupo de usuarios* podrá acceder a n *sitios* o *grupos de sitios*.
- ✓ Un *dispositivo* deberá estar localizado en un único *sitio*.
- ✓ Un *dispositivo* podrá ser accedido desde n *sitios* o *grupos de sitios*.
- ✓ Un *grupo de sitios* podrá contener n *sitios* o *grupos de sitios*.
- ✓ Un *sitio* o *grupo de sitios* podrá pertenecer a n *grupos de sitios*.

Cada *sitio* tendrá las siguientes propiedades:

- ✓ *General*: ubicación (dentro del dominio), nombre, descripción, país, provincia/estado, ciudad, domicilio, teléfono, zona horaria, empresa, los dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.). ~~objetos que tienen acceso a dicho sitio, grupos de sitios a los que pertenece.~~
- ✓ *Historial de Versiones*: se podrá mantener un historial de versiones de cada sitio, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contiene la ACL (Lista de Control de Accesos) sobre el sitio. Se podrá definir cuáles usuarios/grupos de usuarios podrán administrar el sitio y cuáles podrán administrar accesos de usuarios o grupos de usuarios dentro del mismo (ver [tabla](#) de solapa “Seguridad”).
- ✓ *Documentación*: contendrá la documentación específica del sitio.

Cada *grupo de sitios* tendrá las siguientes propiedades:

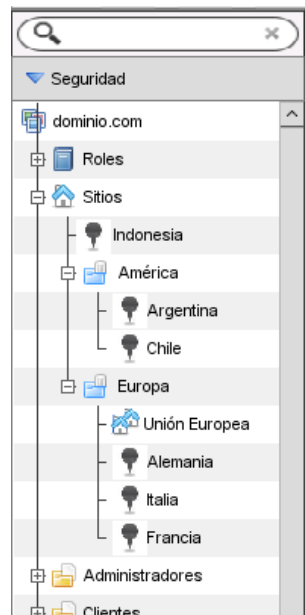
- ✓ *General*: ubicación, nombre, descripción, [país](#), [provincia/estado/región](#), [ciudad](#), ~~objetos que tienen acceso a los sitios de dicho grupo~~, grupos de sitios a los que pertenece y sitios/grupos contenidos.
- ✓ *Historial de Versiones*: se podrá mantener un historial de versiones de cada grupo de sitios, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contiene la ACL (Lista de Control de Accesos) sobre el grupo de sitios. Se podrá definir cuáles usuarios/grupos de usuarios podrán administrar el grupo y cuáles podrán administrar accesos de usuarios o grupos de usuarios dentro del mismo (ver [tabla](#) de solapa “Seguridad”).
- ✓ *Documentación*: contendrá la documentación específica del grupo.

Las propiedades obligatorias de cada sitio son: nombre, [zona horaria](#), [domicilio](#), [provincia/estado/región](#) y [país](#). La propiedad obligatoria de un grupo de sitios es el nombre. No podrá existir más de un sitio o grupo de sitios con el mismo nombre. **Adicionalmente, un sitio no podrá tener el mismo nombre que un grupo de sitios y viceversa.**

Se podrán agrupar los sitios y grupos en *unidades organizacionales de sitios* para mejor visualización. Estas OU sólo contendrán sitios y grupos de sitios, y sus propiedades serán:

- ✓ *General*: ubicación, nombre, descripción y los dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.).
- ✓ *Historial de Versiones*: se podrá mantener un historial de versiones de cada OU de sitios, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contiene la lista de permisos y denegaciones de los usuarios y grupos de usuarios sobre la OU de sitios (ver [tabla](#) de solapa “Seguridad”).
- ✓ *Documentación*: contendrá la documentación específica de la OU de sitios.





Argentina

GeneralHistorial de VersionesSeguridadDocumentación

Ubicación:

dominio.com > Sitios > América

Nombre (\*)

Argentina

Zona horaria (\*)

(GMT-03:00) Buenos Aires

Descripción

Objetos que pueden acceder

Grupos a los que pertenece

Propiedades geográficas

Pais

Argentina

Provincia / Estado

Ciudad

Domicilio

Teléfono

### 3.3 Usuarios y grupos de usuarios

Los *usuarios* y *grupos de usuarios* podrán darse de alta en el dominio. En el alta de usuarios, no se validará que la cantidad de usuarios no supere el límite de la licencia. Los usuarios externos habilitados para ingresar al dominio se tendrán en cuenta para el licenciamiento.

Un *usuario* es un individuo -dentro de la organización- que accederá al sistema a través de autenticación. Cada *usuario* será único.

Un usuario sólo podrá tener activa una sesión a la vez. Si un usuario se encuentra activo, al acceder desde otra ubicación o navegador se cerrará automáticamente la sesión anterior (Tal como funciona Windows Terminal server).

En caso de producirse un cierre de sesión, ya sea automático o manual, cuando un usuario vuelva a iniciar sesión, el sistema presentará el contenido de pantalla existente al momento previo al cierre de sesión.

Cada *usuario* tendrá las siguientes propiedades:

- ✓ *General:* ubicación, nombre de usuario, tipo de usuario, nombre, apellido, foto, descripción, contraseña, correo electrónico, cuenta predeterminada para envío de correo electrónico, **cuentas de MI**, cuenta telegram, teléfono, teléfono celular, domicilio, provincia/estado/región, código postal, ciudad, país, **puestos, departamentos, jefes, subordinados, grupos de usuarios a los que pertenece, ~~sitios y grupos de sitios a los que puede acceder~~, calendario, los dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.),** idiomas preferidos de UI y de datos para autenticación de usuarios (hereda de la OU donde se encuentre el usuario) y políticas de seguridad (ver tabla de políticas de seguridad). **El calendario y las políticas de seguridad se heredarán de la OU que contenga al usuario.** Para el caso de Telegram se podrá tener una única cuenta asociada.
- ✓ *Limitar sitios y Limitar empresas:* permite definir que el usuario solo tiene acceso a los sitios/empresas seleccionadas y en consecuencia las instancias visualizadas dentro del sistema sobre las cuales tenga permisos de consultar, son sólo las correspondientes a dichos sitios o empresas según sea el caso.
- ✓ *Limitar empresas:* permite definir que el usuario solo tiene acceso a las empresas seleccionadas y en consecuencia las instancias visualizadas dentro del sistema sobre las cuales tenga permisos de consultar, son sólo
- ✓ *Licencias:* contiene las licencias asignadas al usuario. Desde aquí, se pueden asignar licencias disponibles y también desasignarlas. Si no hay licencias disponibles, la opción para asignar licencia se mostrará en sólo lectura. Además, se visualizará un botón para acceder a comprar licencias en el Market Place.
- ✓ *Historial de Versiones:* se podrá mantener un historial de versiones de cada usuario, de acuerdo a lo definido en el documento Estándares de interfaz de usuario.
- ✓ *Seguridad:* contiene la ACL (Lista de Control de Accesos) sobre el usuario (ver tabla de solapa "Seguridad").
- ✓ *Documentación:* contendrá la documentación específica del usuario.

Las propiedades que deberán definirse obligatoriamente al momento de la creación de un usuario serán: nombre de usuario, ubicación, nombre, apellido, tipo de usuario, idioma de datos y de ui. **Además, contraseña, e-mail y celular, en caso en que la política efectiva lo requiera.** Distintos usuarios activos no podrán tener el mismo nombre de usuario, dirección de e-mail, ~~ni número de teléfono celular.~~

Siempre se validará que el idioma preferido sea uno de los que se encuentran seleccionados en la lista de idiomas disponibles en el dominio.

Los *tipos de usuario* disponibles serán:

- ✓ *Usuario de Aplicación:* podrá acceder a la Aplicación, es decir, al Sistema en tiempo de ejecución.
- ✓ *Usuario Editor:* podrá acceder a la Aplicación, y a los Editores.
- ✓ *Usuario de Web Service:* solamente podrá ejecutar las Actividades de WS. **Podrá acceder a la Aplicación pero solamente podrá acceder a sus preferencias de usuario y consultar los logs de las actividades realizadas.**

Tipo de usuario (*)	<div>▼</div> <div>         Usuario de Aplicación          Usuario Editor          Usuario de Web Service       </div>
Nombre (*)	
Apellido (*)	
Foto	

Un *Usuario de Web Service* es un individuo que podrá acceder a ciertas actividades por medio de un Web Service. Para realizar las actividades, deberá ingresar a un determinado link previamente configurado. Además, podrá ingresar a la aplicación, autenticándose al igual que el resto de los usuarios, y realizar ciertas operaciones de manera limitada; como por ejemplo, cambiar su contraseña, sus datos personales, idioma preferido de datos y de UI y las demás preferencias de usuario, visualizar los logs de las actividades realizadas, etc.

Las propiedades del usuario: puestos, departamentos, jefes y subordinados servirán para automatizar y mantener la definición del organigrama con seguridad, además de definir la jerarquía en la seguridad de delegación de actividades y supervisión (toma de sesión, iniciar toma de sesión, coaching y monitorización). Estas propiedades no estarán disponibles para los Usuarios de WS.

Un usuario podrá tener un puesto por departamento. Las propiedades jefes y subordinados serán del tipo colección de usuarios. Para seleccionar la jerarquía del usuario dentro de la organización se utilizará una grilla. En la misma se deberá elegir primero el departamento y luego el puesto dentro de ese departamento, ambos en listas descolgables. Automáticamente se visualizarán los jefes y subordinados del usuario para el departamento y puesto seleccionados, en la fila correspondiente de la grilla. Esto quedará reflejado en el organigrama predeterminado para la seguridad.

Al inhabilitar o eliminar un usuario, se eliminarán sus referencias jerárquicas asociadas. Esto se reflejará instantáneamente en el organigrama de seguridad.

Además, al eliminar un usuario, se eliminarán todos los permisos que el mismo posee en los distintos elementos, pero no se eliminarán los logs que se generaron asociados al usuario. Ahora bien, cuando se restaura un usuario, los permisos NO se restaurarán, es decir, cuando se restaura un usuario, se debe volver a configurar sus permisos.

Las propiedades país, puestos y departamentos deberán pertenecer a entidades paramétricas que puedan accederse desde los editores o desde el sistema generado. Además, deberán permitir la internacionalización. Estas entidades internas serán listas predefinidas modificables. Desde la interfaz se realizará una búsqueda incremental cada vez que se invoque dichas propiedades.

Los *grupos permitidos para ejecución de reglas de negocio y tareas programadas* serán los grupos de usuarios con cuyos permisos se podrán ejecutar las RN y tareas programadas en los PN. Cuando un usuario configure una RN o una TP, podrá elegir con los permisos de qué grupo se va a ejecutar dicha RN o TP. Estos grupos de ejecución se acotarán en las políticas de seguridad del usuario.

**Propiedades de la cuenta**

Tiempo de expiración de la cuenta: 0 días

Rango de fechas de validez de la cuenta: desde [ ] hasta [ ]

Delegación de permisos: Todos los usuarios

Grupos permitidos para ejecución:

- ☐ Grupo 1
- ☒ Grupo 2
- ☐ Grupo 3
- ☒ Grupo 3

Bloquear cuenta

Inhabilitar cuenta

---

**Propiedades de los accesos**

Rango horario permitido: De lunes a domingo, de 0 a 24 hs

Cada vez que se visualice un usuario en el sistema, se presentará el nombre y apellido de dicho usuario precedido de su foto o de una imagen genérica ( ) en caso de no haber cargado una foto. Además se indicará con un marco o un icono visible en distintos colores, los diferentes estados de un usuario.

~~Inicialmente, se visualizarán de una manera diferente tanto la foto o imagen genérica, como el nombre de aquellos usuarios que todavía no se hayan autenticado al sistema.~~

Luego de la primera autenticación, un *usuario* tendrá uno de los siguientes *estados*:

- ✓ **Disponible:** el usuario se encuentra autenticado en el sistema y puede ser contactado para iniciar un chat o una supervisión. Este estado se indicará de la siguiente manera:
- ✓ **Ausente:** el usuario se encuentra autenticado en el sistema, pero ha permanecido inactivo durante un cierto tiempo. Este estado se indicará de la siguiente manera:
- ✓ **No disponible:** el usuario se encuentra autenticado en el sistema y ha indicado que no desea ser molestado. Este estado se indicará de la siguiente manera:
- ✓ **No conectado:** el usuario no se encuentra autenticado en el sistema. Este estado se indicará de la siguiente manera:

La lista de estados posibles irá incrementándose a medida que se agregue funcionalidad.

En cualquier lugar donde se visualice un usuario, se tienen las mismas opciones (por ejemplo, chatear, monitorizar, etc.). En cualquier lugar donde se visualice el usuario autenticado se tienen las mismas opciones que son distintas a las primeras (por ejemplo, cerrar sesión, cambiar datos personales, etc.)

Un usuario administrador que tenga permiso para cambiar la contraseña de un usuario, podrá además restablecerla haciendo clic en el ícono . En este caso, la contraseña generada se informará al e-mail del usuario, o en su defecto a su teléfono. En caso de no poseer e-mail ni celular, no se podrá restablecer la misma, notificándose al administrador, debiendo este cambiarla manualmente.

Una vez que haya accedido, un usuario podrá cambiar algunas de sus propiedades desde *Preferencias de Usuario*. Dichas propiedades serán: ~~contraseña~~, foto, domicilio, localidad/provincia/estado, código postal, país, e-mail y teléfono, entre otras, siempre que tenga los derechos necesarios. Si un usuario puede realizar cambios en sus preferencias, deberá validarse nuevamente por el sistema de autenticación que tenga definido para poder concretarlo.

Se define como *grupo de usuarios* a un objeto que contiene usuarios y/o otros grupos de usuarios, de acuerdo a las siguientes reglas:

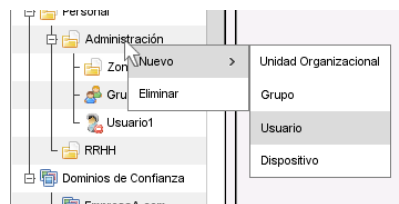
- ✓ Un *grupo de usuarios* podrá contener  $n^5$  *usuarios*.
- ✓ Un *grupo de usuarios* podrá contener  $n$  *grupos de usuarios*.
- ✓ Un *usuario* podrá pertenecer a  $n$  *grupos de usuarios*.
- ✓ Un *grupo de usuarios* podrá pertenecer a  $n$  *grupos de usuarios*.

Cada *grupo* tendrá las siguientes propiedades:

- ✓ *General*: ubicación, nombre, descripción, imagen, grupos de usuarios en los que está incluido, objetos contenidos ~~y sitios y grupos de sitios a los que puede acceder~~ y establecer como rol en modelo hijo.
- ✓ *Historial de Versiones*: se podrá mantener un historial de versiones de cada grupo de usuarios, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contiene la ACL con los permisos y denegaciones sobre el grupo (ver [tabla](#) de solapa “Seguridad”).
- ✓ *Documentación*: contendrá la documentación específica del grupo.

Al momento de la creación de un grupo, será obligatorio definir el nombre del mismo. No podrá existir más de un usuario o grupo de usuarios con el mismo nombre. Adicionalmente, un usuario no podrá tener el mismo nombre que un grupo de usuarios y viceversa. Se podrá agregar una imagen identificativa a cada grupo, de manera similar a la descripta para la foto de los usuarios.

A continuación se detalla un ejemplo de la creación de un usuario dentro de la OU Administración.



---

<sup>5</sup> El valor de  $n$  va de 0 a  $\infty$ , a menos que se indique lo contrario.

Nuevo usuario

General | Historial de Versiones | Seguridad | Documentación

Ubicación: dominio.com > Personal > Administración

Usuario (\*)

Tipo de usuario (\*)

Nombre (\*)

Apellido (\*)

Foto

Descripción

Contraseña

E-mail

Teléfono celular

Domicilio

Localidad/Estado/Provincia

Código Postal

País

Departamentos	Departamento	Puesto	Jefes	Subordinados

Nuevo usuario

General | Historial de Versiones | Seguridad | Documentación

Calendario

Cuenta predeterminada para envío de email

Dispositivos predeterminados

Idioma preferido

**Propiedades de la cuenta**

Tiempo de expiración de la cuenta  días

Rango de fechas de validez de la cuenta desde  hasta

Delegación de permisos

Grupos permitidos para ejecución

Bloquear cuenta ☐

Inhabilitar cuenta ☐

**Propiedades de los accesos**

Rango horario permitido

Direcciones IPs permitidas

Permitir recordar último usuario identificado en equipo ☐

**Métodos de autenticación permitidos**

Requerir usuario y contraseña ☒

Nuevo usuario ✕

General
 Historial de Versiones
 Seguridad
 Documentación

Métodos de autenticación permitidos
 

Requerir usuario y contraseña ☒
 Requerir dispositivo de autenticación ☐
 Validar con SMS ☐
 Validar con OTP ☐
 Requerir verificación biométrica ☐
 Requerir certificado digital ☐

**Propiedades de la contraseña**

Forzar cambio de contraseña en el próximo acceso ☐
 Permitir cambio de contraseña ☒

**Propiedades del control remoto**

Toma de sesión 

Todos los usuarios ▾

 Invitación a sesión 

Todos los usuarios ▾

 Monitorización 

Sólo a subordinados ▾

 Coaching 

Todos los usuarios ▾

Rango de fechas de validez de la cuenta
 desde 17 JUL 2012
 hasta

Delegación de permisos
 Todos

Cuenta bloqueada
 ☐

2012
 1 2 3 4 5 6 7
 8 9 10 11 12 13 14
 15 16 17 18 19 20 21
 22 23 24 25 26 27 28
 29 30 31

Horario de Acceso
 ✕

**Definir el horario de acceso al sistema para el usuario:**

Haga clic en el/los día/s de la semana y en el horario para permitir/denegar el acceso.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lunes																								
Martes																								
Miércoles																								
Jueves																								
Viernes																								
Sábado																								
Domingo																								

☒ Acceso Permitido
 ☐ Acceso No Permitido

De lunes a domingo, de 0 a 24 hs

**Usuario2**

General | **Licencias** | Historial de Versiones | Seguridad | Documentación

### Asignar las licencias al usuario para acceder a las aplicaciones:

A continuación, se pueden ver los modelos a los que el usuario podría acceder. Para que pueda ingresar, debe asignarle la licencia correspondiente.


Plataforma	
Plataforma de Desarrollo	<input type="checkbox"/>
Plataforma de ejecución	<input type="checkbox"/>
Licencia de Web Service	<input type="checkbox"/>

Aplicaciones	
<b>[ - ] Modelo:</b> CRM Finanzas	
Licencia de aplicación	<input type="checkbox"/>
Licencia de edición	<input type="checkbox"/>
Licencia de Web Service	<input type="checkbox"/>
<b>[ - ] Modelo:</b> Busintelligence	
Licencia de aplicación	<input type="checkbox"/>
Licencia de edición	<input type="checkbox"/>

[Comprar más licencias](#)



Usuario2 

General | Historial de Versiones | Seguridad | Documentación

**Definir la seguridad para los usuarios y grupos de usuarios:**

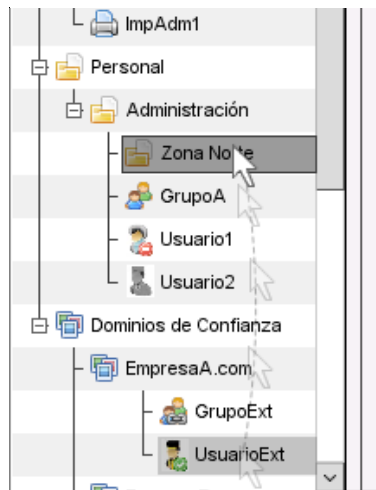
Haqa clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Usuario/Grupo

Permiso	Permitir	Denegar
Administrar usuario	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Consultar permisos efectivos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar ubicación	<input type="checkbox"/>	<input type="checkbox"/>
Modificar datos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar foto	<input type="checkbox"/>	<input type="checkbox"/>
Modificar contraseña	<input type="checkbox"/>	<input type="checkbox"/>
Modificar e-mail	<input type="checkbox"/>	<input type="checkbox"/>
Modificar teléfono celular	<input type="checkbox"/>	<input type="checkbox"/>
Modificar domicilio	<input type="checkbox"/>	<input type="checkbox"/>
Modificar permisos y grupos a los que pertenece	<input type="checkbox"/>	<input type="checkbox"/>

Los *usuarios y grupos de usuarios externos* (de otros dominios) tendrán las mismas propiedades y posibilidades de acceso que los del dominio original, salvo que los datos de las políticas de acceso de un usuario serán locales al dominio. Se podrá definir como usuarios externos cualquier tipo de usuarios (de Aplicación, Editores y de Web Service). Además, no se visualizarán los datos personales de los usuarios externos (teléfono, dirección, etc.) y no podrán modificarse las propiedades generales ni las propiedades de la contraseña. Los datos que se podrán modificar harán referencia al dominio local y serán: puestos, departamentos, jefes, subordinados, grupos a los que pertenece, tiempo de expiración de acceso al dominio local, rango de validez del mismo, delegación de Actividades, bloquear cuenta (se habilitará si el usuario intenta acceder al dominio local luego de una cantidad de accesos fallidos consecutivos, y se podrá inhabilitar), inhabilitar cuenta (si se activa esta directiva, la cuenta no podrá acceder al dominio local pero sí al de origen), rango horario, direcciones IP permitidas, permitir mantener sesión iniciada, métodos de autenticación adicionales, toma de sesión, invitación a sesión, monitorización y coaching, e idioma preferido.

Se presenta a continuación un ejemplo en el cual se muestra cómo se “arrastra” un usuario externo del dominio EmpresaA a la OU Zona Norte:



UsuarioExt

General | Historial de Versiones | Seguridad | Documentación

Ubicación: dominio.com > Personal > Administración > Zona Norte

Usuario (\*)

Nombre (\*)

Apellido (\*)

Foto

Descripción

Departamentos

Departamento	Puesto	Jefes	Subordinados

Calendario: Calendario Predeterminado

Cuenta predeterminada para envío de email

Dispositivos predeterminados: impresora HP Adm, Fiscal Hassar pc4

Idioma preferido: Español

**Propiedades de la cuenta en el dominio local**

Tiempo de expiración de la cuenta: 0 días

UsuarioExt

General Historial de Versiones Seguridad Documentación

**Propiedades de la cuenta en el dominio local**

Tiempo de expiración de la cuenta 0 días

Rango de fechas de validez de la cuenta desde hasta

Delegación de permisos Todos los usuarios

Bloquear cuenta

Inhabilitar cuenta

**Propiedades de los accesos al dominio local**

Rango horario permitido De lunes a domingo, de 0 a 24 hs

Direcciones IP permitidas Sin restricciones

Permitir recordar último usuario identificado en equipo

**Métodos de autenticación permitidos**

Requerir usuario y contraseña

Requerir dispositivo de autenticación

Validar con SMS

Validar con OTP

UsuarioExt

General Historial de Versiones Seguridad Documentación

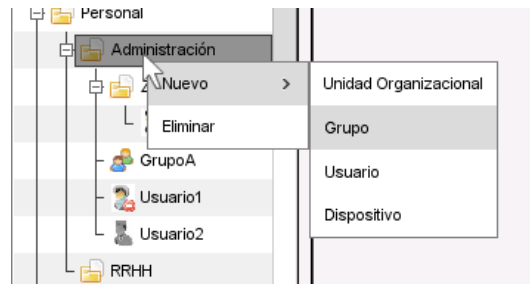
**Definir la seguridad para los usuarios y grupos de usuarios:**

Haga clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Usuario/Grupo

Permiso	Permitir	Denegar
Administrar usuario		
Consultar		
Consultar permisos efectivos		
Modificar ubicación		
Modificar datos		
Modificar permisos y grupos a los que pertenece		
Modificar sitios a los que puede acceder		
Modificar políticas de seguridad locales		
Modificar documentación		
Eliminar		
Traducir		


Ahora se muestra un ejemplo de la creación de un grupo de usuarios desde el acordeón de Seguridad, también en la OU Administración:




**Nuevo Grupo** ✕

General | Historial de Versiones | Seguridad | Documentación

Ubicación: dominio.com > Personal > Administración

Nombre (\*)  

Descripción

Imagen 

Grupos a los que pertenece  ▼

Objetos contenidos  ▼

Sitios a los que puede acceder  ▼

Grupos de sitios a los que puede acceder  ▼

Modelos a los que puede acceder  ▼

Establecer como rol en modelos hijos ☐

**Como son calculados, se muestran en sólo lectura**

Marketing

General Historial de Versiones Seguridad Documentación

**Definir la seguridad para los usuarios y grupos de usuarios:**

Haga clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Usuario/Grupo

- Todos
- Administrador de RN

Permiso	Permitir	Denegar
Administrar grupo	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Consultar permisos efectivos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar ubicación	<input type="checkbox"/>	<input type="checkbox"/>
Modificar datos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar permisos y grupos a los que pertenece	<input type="checkbox"/>	<input type="checkbox"/>
Modificar objetos contenidos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar sitios/grupos de sitios de acceso	<input type="checkbox"/>	<input type="checkbox"/>
Modificar documentación	<input type="checkbox"/>	<input type="checkbox"/>
Utilizar como grupo de ejecución	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>

Los *permisos* y *denegaciones* se podrán otorgar por grupos de usuarios<sup>6</sup> o individualmente por usuario.

Los *usuarios* obtendrán los permisos de los *grupos de usuarios* a los que pertenezcan (y a su vez de los *grupos de usuarios* a los que pertenezca cada grupo, recursivamente), además de los permisos asignados individualmente al *usuario*. De la misma manera se asignarán las *denegaciones*.

Las *denegaciones* siempre tendrán prioridad sobre los *permisos* y las *propiedades no definidas*, aún si estos son heredados de un grupo. Por ejemplo, si un grupo tiene denegado el acceso a un elemento, aunque se especifique el permiso a un usuario de ese grupo, dicho usuario no podrá acceder al elemento.

En cualquier momento, a un usuario se le podrán asignar los permisos y denegaciones predeterminados de los grupos de usuarios a los que pertenece.

### 3.4 Usuarios y grupos de usuarios predefinidos del sistema (roles)

Existirán -conjuntamente con los grupos de usuarios y usuarios definidos por los usuarios- *grupos de usuarios* y *usuarios* definidos en el sistema.

Un rol definido por el usuario es un grupo de usuarios con la propiedad *Rol para dominios hijos*. Los roles definidos por el usuario se crean en los dominios nuevos (donde haya algún modelo hijo del modelo actual).

La funcionalidad de estos roles, es que al crear un usuario o grupo, tan sólo agregándolo a uno de estos roles, ya podrá realizar todas las operaciones que el rol tiene permisos para realizar, sin la necesidad de dar los permisos uno por uno.

<sup>6</sup> De acuerdo a las mejores prácticas, se recomienda no usar la denegación en los grupos.

El único *usuario predefinido* será el administrador del dominio o “*administrador*”. Se podrán modificar sus datos como nombre, apellido, usuario, contraseña, etc. para mayor seguridad.

A continuación, se detalla los roles predefinido del sistema y los permisos predeterminados en todos los elementos: ~~se encuentra en el siguiente documento~~

- **Usuario final del dominio:** el objetivo es que ingrese a todos los modelos de un dominio, en el ambiente de producción, sin configurar nada extra. Sólo tiene permiso de acceder a producción.
- **Usuario avanzado del dominio:** el objetivo es que use todos los modelos de un dominio y realice configuraciones mínimas, en los ambientes de producción y prueba, sin configurar nada extra. Tiene permiso de acceder a producción y prueba, ejecutar las actividades, realizar todas las operaciones en las instancias de entidades y en todas las herramientas dinámicas.
- **Editor del dominio:** el objetivo es que programe dentro de los modelos de un dominio, en los ambientes desarrollo, prueba y producción. Tiene permiso de acceder a todos los ambientes, realizar todas las operaciones en las instancias de entidades, en todas las herramientas dinámicas y los editores.
- **Administrador del dominio:** el objetivo es que administre los permisos sobre todos los elementos de los modelos de un dominio, en todos los ambientes. Tiene permiso de acceder a todos los ambientes, realizar todas las operaciones en las instancias de entidades, herramientas dinámicas, editores y en el dominio (usuario, grupo, etc). Además, tiene habilitada la opción para [restablecer credenciales](#) en el usuario.
- **Administrador de dispositivos:** el objetivo es que administre los dispositivos en todos los modelos de un dominio, en todos los ambientes. Tiene permiso de acceder a todos los ambientes y todos los permisos en dispositivo, agente, controlador, protocolo y tipo de dispositivo.

Al crear un usuario, se configura su tipo: Editor, Aplicación o WS.

- Si se crea un usuario editor, se agrega al rol Editores del dominio.
- Si se crea un usuario de aplicación, se agrega al rol Usuarios finales del dominio.

Esta pertenencia se podrá modificar.


Administradores de Seguridad

General
Historial de Versiones
Seguridad
Documentación

Ubicación: dominio.com > Roles

Nombre (\*) Administradores de Seguridad

Descripción Grupo predefinido de los administradores de seguridad de dominio

Imagen


Objetos contenidos

Administradores de Seguridad

General
Historial de Versiones
Seguridad
Documentación

**Definir la seguridad para los usuarios y grupos de usuarios:**

Haga clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Usuario/Grupo

Permiso	Permitir	Denegar
Administrar grupo predefinido	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Consultar permisos efectivos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar documentación	<input type="checkbox"/>	<input type="checkbox"/>
Modificar objetos contenidos	<input type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input type="checkbox"/>	<input type="checkbox"/>
Administrar grupos de usuarios contenidos	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Consultar permisos efectivos	<input type="checkbox"/>	<input type="checkbox"/>
Administrar usuarios contenidos	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>

### 3.5 Usuarios de Web Service

Un Usuario de Web Service es un individuo que podrá acceder a ciertas actividades por medio de un Web Service. Para realizar las actividades, deberá ingresar a un determinado link previamente configurado y autenticarse correctamente.

La seguridad configurada en los Procesos de Negocio y la seguridad de instancias en las Entidades, definirán lo que cada usuario de WS podrá realizar.

Además, se podrá autenticar al sistema de la misma manera que el resto de los usuarios y cambiar sus preferencias de usuario y entre ellas, su contraseña.

Dentro de las políticas de seguridad configurables para un usuario WS, se encuentra la opción "Métodos de autenticación adicionales", cuya única opción disponible es OTP (One-Time Password) para usuarios WS. Si se configura un usuario WS con este método, es necesario vincular al usuario con la aplicación OTP. Para ello, se debe obtener la clave secreta a través de la opción del menú contextual "Vincular con aplicación OTP", que muestra dicha clave en una ventana modal. Esta clave puede ser copiada y enviada a la persona correspondiente para completar la vinculación. En el caso de que el usuario tenga una cuenta otp ya asociada, el menú contextual muestra ventana modal advirtiendo esta situación ("Si obtiene una nueva clave, la cuenta anterior quedará sin validez"). Si el usuario acepta, se muestra la nueva clave secreta, invalidando la anterior desde el momento en que se muestra la nueva clave. Es importante aclarar que esta opción de menú contextual solo estará disponible para quienes posean permisos de edición del usuario en cuestión.

### 3.6 Dispositivos

Los *dispositivos* podrán ser cualquier periférico para el cual se necesite administrar la seguridad, por ejemplo, impresoras, scanners, tickeadoras, impresoras fiscales, etc.

El *tipo de dispositivo* deberá especificarse en el momento de la creación del dispositivo.

El formulario del objeto *Dispositivo* tendrá las siguientes solapas con sus respectivas propiedades:

- ✓ **General:** en esta solapa se especifican las propiedades principales. Las mismas son:
  - Nombre: permite ingresar un nombre representativo del dispositivo, el mismo es un texto internacionalizable de valor único y obligatorio.
  - Descripción: permite ingresar una descripción para el dispositivo, el mismo es un texto internacionalizable.
  - Tipo de dispositivo: valor obligatorio que permite elegir el tipo correspondiente para el dispositivo a crear. Es un combo de selección única que lista los valores posibles proporcionados por el sistema. Algunos de los *tipos de dispositivos* predefinidos inicialmente serán:
    - Impresora de documentos
    - **Dispositivos Multifunción**
    - **Scanner**
    - Impresora fiscal
    - **Tickeadora**
    - **Impresora de código de barra**
    - **Balanza**
    - **Dispositivo biométrico**
    - **Puerto**



- Terminal punto de venta

- ~~Modelo de dispositivo: valor obligatorio a elegir desde un combo de selección única que lista los modelos de dispositivos (drivers) que corresponda con el dispositivo a crear. Los modelos de dispositivos disponibles estarán definidos en el Administrador de Modelos y deberán ser compatibles con el tipo de dispositivo. Por ejemplo, para el tipo de dispositivo impresoras fiscales, los modelos podrán ser: HASAR SMH/P P441 f, SMHP 330 f, etc. La selección del modelo será obligatoria.~~

~~Si el tipo de dispositivo es "Impresora" no se visualiza la propiedad "Modelo de dispositivo".~~

- ~~Tipo de configuración: valor obligatorio a elegir desde un combo de selección única donde las opciones disponibles son "Automático" o "Manual". La opción "Automático" indica que se seleccionará un dispositivo detectado automáticamente por uno o más de los agentes dados de alta en el sistema. En cambio, la opción "Manual" indica que ningún agente disponible lo puede detectar automáticamente, por lo que al elegir esta opción para asociar el dispositivo con alguno de los agentes del sistema se deben configurar propiedades adicionales que permitirán luego acceder al mismo.~~
- Sitio: se debe indicar el sitio en donde se encuentra localizado el dispositivo. Opcional.
- Calendario: El calendario se hereda de la OU donde se encuentra, pudiendo redefinirse el calendario a utilizar por el dispositivo. Esta opción es un combo de selección única, donde los valores disponibles son aquellos calendarios creados en el sistema.
- Agentes: En la sección a continuación se define el o los agentes correspondientes al dispositivo actual, por cada agente que se agrega se muestra un combo de selección única donde los valores posibles son los agentes definidos en el dominio y que se encuentran vinculados. Será obligatorio al menos agregar un agente.

~~Si el tipo de configuración es automática,~~ una vez seleccionado el agente se debe elegir el periférico detectado. Las opciones son todos aquellos dispositivos que detecta el agente en el host donde se instaló. En este combo el usuario debe elegir la opción que corresponde al dispositivo que se está creando.

~~Si la identificación del dispositivo es "Manual", debajo del agente seleccionado en vez de listarse los dispositivos físicos detectados se visualizan las propiedades necesarias para configurar el dispositivo físico, las propiedades son las que se detallan a continuación:~~

- ~~Tipo de conexión: tipo de puerto en donde se encuentra conectado el dispositivo físico. Combo de selección única donde las opciones son "Puerto serie" o "Ethernet".~~

~~Si se elige la opción "Puerto serie" se deben configurar también las siguientes opciones:~~

- Puerto: es un combo de selección única, por ejemplo, COM3
- Velocidad: es un valor de enumerado selección simple
- Longitud de palabra de datos: es un enumerado selección simple
- Paridad: es un enumerado selección simple
- Cantidad de bits de parada: es un enumerado selección simple
- Control de flujo: es un enumerado selección simple

~~Si se elige la opción "Ethernet" se debe completar el valor "IP" con la IP correspondiente.~~

Poder agregar más de un agente permite poder agregar distintos agentes que detectan el mismo dispositivo físico, entonces si ocurre que un agente no responde el otro agente agregado permite usar el dispositivo. También se pueden elegir distintos dispositivos detectados por un mismo agente, permitiendo balancear carga entre los distintos dispositivos físicos vinculados.

Si el agente vinculado se vuelve a instalar y el nombre del dispositivo detectado por la nueva instalación del agente coincide con el configurado en el dispositivo, la configuración realizada sigue siendo válida. Si no coincide el nombre del dispositivo, o el agente quedó desvinculado, el dispositivo definido en el dominio queda inválido y se notificará el error en ejecución cuando se quiera consumir.

- ✓ *Historial de Versiones*: se puede mantener un historial de versiones de cada dispositivo, de acuerdo a lo definido en el documento [Estándares de interfaz de usuario](#).
- ✓ *Seguridad*: contendrá una lista usuarios y grupos de usuarios que podrán acceder al dispositivo y los permisos de cada uno sobre el mismo (los permisos dependerán del tipo de dispositivo).
- ✓ *Documentación*: contendrá la documentación específica del dispositivo.

En la siguiente imagen se muestra el alta de un dispositivo:

The screenshot shows a web-based configuration interface for a device. The main window is titled 'Dispositivo' and has a tabbed interface with 'General', 'Historial de Versiones', 'Seguridad', and 'Documentación'. The 'General' tab is active. The form contains the following fields:

- Ubicación:** Text input with 'Dominio.com / Equipos'.
- Nombre \*:** Text input with 'Impresora de código de barras'.
- Descripción:** Text input with 'Impresora del sector despacho mercaderíaadministrativo'.
- Tipo de dispositivo:** Dropdown menu with 'Impresora de código de barras' selected.
- Modelo de dispositivo:** Dropdown menu with 'HP P1102W' selected.
- Tipo de configuración:** Dropdown menu with 'Manual' selected.
- Sitio de localización:** Dropdown menu with 'Rosario' selected.
- Calendario:** Dropdown menu with 'Calendario predeterminado' selected.

Below the main form is a section titled 'Agentes' with a plus icon. It contains two entries, each with a minus icon, a plus icon, and a dropdown arrow:

- Agente:** 'Agente de Área Administración' (dropdown)
- Dispositivo detectado:** 'Impresora Laser HP 5698' (dropdown)

The second entry is identical, with 'Dispositivo detectado' set to 'Impresora Laser HP 6001'. A vertical sidebar on the right is labeled 'Propiedades'.

~~En la siguiente imagen se muestra la configuración en caso que se haya elegido la opción Manual en Identificación dispositivo.~~

Dispositivo

General
Historial de Versiones
Seguridad
Documentación

Ubicación

Dominio.com / Equipos

Nombre \*

Impresora de código de barras

Descripción

Impresora del sector despacho mercaderíaadministrativo

Tipo de dispositivo

Impresora de código de barras

Modelo de dispositivo

HP P1102W

Tipo de configuración

Manual

Sitio de localización

Rosario

Calendario

Calendario predeterminado

+ Agentes

- Agente:
Agente de Área Administración

Tipo de conexión

Puerto Serie

Puerto

Velocidad

Longitud

Paridad

Propiedades

¿Con qué orden de prioridad se consumen los agentes? ¿Con qué algoritmo resolvemos la asignación de trabajos?

Primero, el primero definido en dispositivo y luego los siguientes, esto es funcionalmente como en las acciones de las RN pero para los dispositivos igualmente hay que tener una lógica interna, por ejemplo se van asignando trabajos en cada dispositivo, dependiendo la carga.

¿Lo podría configurar el usuario o es interno? Por ejemplo, si en todos los dispositivos hay trabajos, pero en el 1ro hay un trabajo que se reconoce puede demorar más, cuando se enconle una nueva petición se asignará al 2do dispositivo o al menos cargado.

~~Ver excepciones al querer consumir un dispositivo, y qué hacer en cada caso, no hay papel en un agente, no está conectada la impresora, da error el dispositivo, etc. Se manejan las excepciones como Windows.~~

**Definir la seguridad para los usuarios y grupos de usuarios:**

Haga clic en la lista o arrastre usuarios/grupos desde el panel de navegación a la lista siguiente.

Permiso	Permitir	Denegar
Administrar dispositivo	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Modificar	<input type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>
Traducir	<input type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Modificar	<input type="checkbox"/>	<input type="checkbox"/>

*Aclaración: los dispositivos no poseen dentro de su configuración acciones, comandos ni parámetros ya que las expresiones en cada parámetro no podrían configurarse porque los dispositivos no están dentro de ningún modelo (están dentro del dominio). Por este motivo, las expresiones en cada parámetro de entrada y salida se configuran dentro de los “Controladores de Dispositivo” que se encuentran dentro de cada Modelo.*

Luego de configurado el dispositivo, se puede usar en acciones de RN para dispositivos.

En caso de copiarse el dispositivo en otros modelos vinculados, distintos de donde se creó el mismo, se copiará las propiedades Nombre, Descripción, Documentación y Tipo dispositivo, el resto de las propiedades específicas del dispositivo físico quedan en blanco en el modelo vinculado teniendo que especificarse luego. Por otra parte, el atributo Unidad organizacional al copiarse el dispositivo se completará en el hijo con una referencia a la OU general.

Si el dispositivo es invocado faltando definir propiedades obligatorias, dará una excepción en tiempo de ejecución en la cola de consumo de dispositivos mostrando al usuario un mensaje y logueando el error en el log correspondiente.

### 3.7 Puestos de trabajo

Para el caso en que el dispositivo sea una computadora (de escritorio, notebook, etc.) el tipo de objeto debe ser *Puesto de Trabajo*.

Un *Puesto de Trabajo* tendrá las siguientes propiedades:

- ✓ *General:* ubicación, nombre, descripción, sitio en donde se encuentra localizado, sitios/grupos de sitios desde donde se puede acceder al puesto de trabajo, calendario ~~y dispositivos predeterminados (para imprimir, para numerar, para escanear, etc.).~~ El

calendario y los dispositivos lo heredarán de la OU donde se encuentra, o del dominio en el caso de que el puesto de trabajo no se encuentre dentro de ninguna OU.

- ✓ *Propiedades específicas del puesto de trabajo:* dentro de las mismas se encuentra la ubicación en tcp/ip, ya sea con hostname o dirección IP.
- ✓ *Historial de Versiones:* se podrá mantener un historial de versiones de cada puesto de trabajo, de acuerdo a lo definido en el documento Estándares de interfaz de usuario.
- ✓ *Seguridad:* contendrá una lista usuarios y grupos de usuarios que podrán acceder al puesto de trabajo y los permisos de cada uno sobre el mismo.
- ✓ *Documentación:* contendrá la documentación específica del dispositivo.

Las propiedades obligatorias serán el nombre y la ubicación hostname/ip.

### 3.8 Cuentas de notificación

Se definen en una misma entidad las cuentas para notificaciones mediante envío de correo electrónico o mensajería instantánea.

En la seguridad de las cuentas se podrán configurar los siguientes permisos:

- Crear
- Consultar
- Modificar
- Eliminar
- Restaurar
- Traducir
- Administrar permisos (consultar, modificar).

Adicionalmente, se cuenta con un ABM Cuentas de notificación, al cuál puede accederse desde el acordeón, mediante la sección de Dominio.

#### 3.8.1 Cuentas de notificación personales.

Al realizar la administración de usuarios o incluso en el momento que un usuario pueda acceder a sus preferencias, se permite configurar las cuentas de notificación personales que deben utilizarse para cada uno de ellos. Es decir, se permite ingresar la configuración de cada uno de los medios por los cuales Fastprg puede emitir una notificación en nombre de un usuario.

Para esto, cuando accedemos al mantenimiento de un usuario, el formulario presenta una solapa por cada tipo de cuenta de notificación, por ejemplo, una solapa para configurar el correo electrónico otra solapa para configurar los datos de la cuenta de Telegram.

Luego, este tipo de cuentas no podrán seleccionarse en forma explícita al enviar un correo electrónico o al notificar por telegram, sino que estas cuentas solo serán utilizadas cuando se indique que debe utilizarse la cuenta del usuario autenticado.

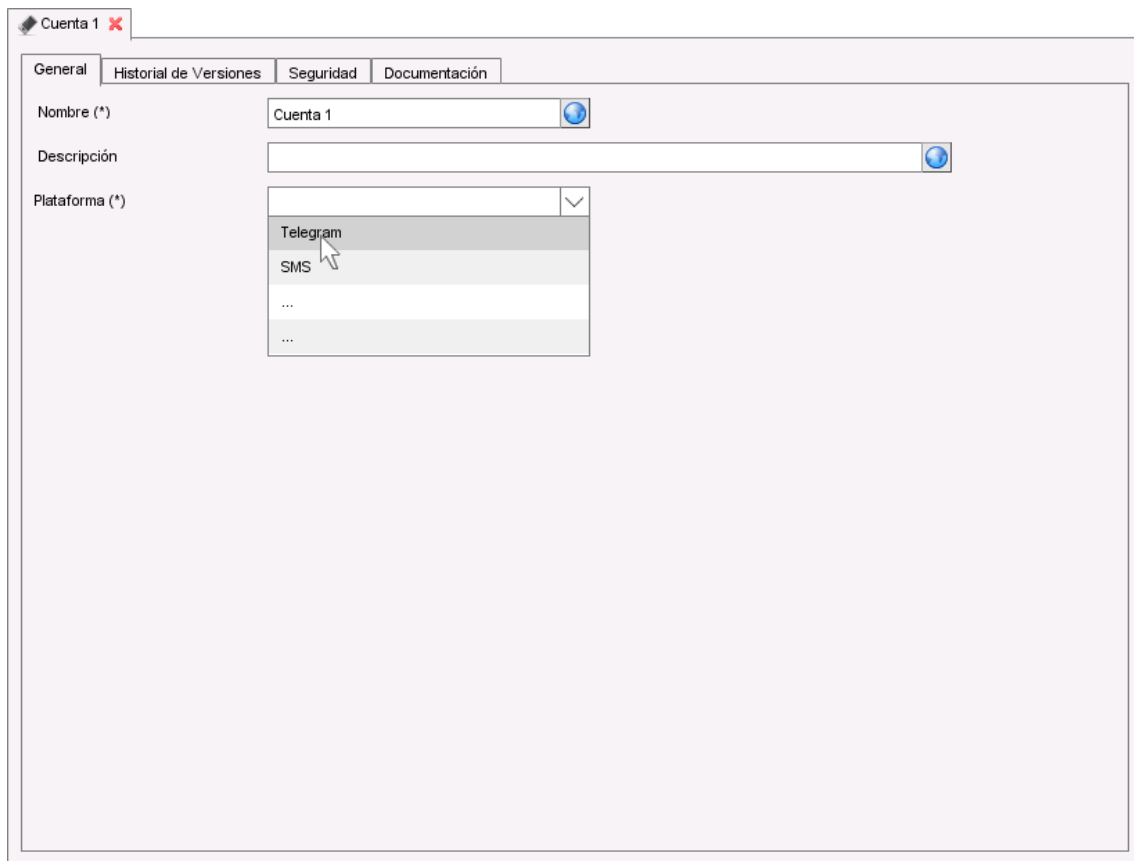
Para más detalles de como completar la información según el tipo de cuenta, acceder en este mismo documento a la sección correspondiente al tipo de cuenta que desea configurar.

### 3.8.1.1 Cuentas para envío de mensajería instantánea

En el dominio se podrán definir cuentas para el envío de mensajería instantánea en diferentes plataformas, cada una exige diferentes datos.

Lo primero que se deberá definir en cada cuenta es:

- Nombre, obligatorio.
- Descripción, opcional.
- Tipo de cuenta. En este caso se darán las opciones de seleccionar si la cuenta será utilizada para correo electrónico, telegram, IM, etc. Dato obligatorio.



Luego de definir la plataforma, se presentarán las configuraciones de acuerdo a la misma.

#### 3.8.1.1.1 Telegram

Telegram es una de las plataformas permitidas para envío de IM dentro de FastPrg. En el dominio se podrán dar de alta muchas cuentas Telegram para enviar mensajes. Para llevar a cabo la configuración de la cuenta de notificación antes debemos registrarnos en Telegram utilizando cualquier aplicación por ejemplo descargando la aplicación en nuestro teléfono celular y luego registrarnos en la API de Telegram.

##### 3.8.1.1.1.1 Registro en la API de Telegram

La API permite crear clientes propios de Telegram de manera personalizada.

Cada cuenta de notificación debe crear una aplicación de Telegram, es decir, registrar una nueva sesión de tu cuenta. Al registrarnos en la API obtenemos un **API ID** que es la puerta de entrada para la comunicación por este medio. Cada número de teléfono registrado puede tener un **API ID** conectado.

A continuación, el paso a paso de este proceso:

1. Iniciar sesión en <https://my.telegram.org>
2. Acceder a Herramientas de desarrollo y completar el formulario.

Una vez realizado este paso obtendremos el **API\_ID** y **API\_HASH** que serán los datos necesarios para la autorización del usuario y el registro de la cuenta de notificación en FastPrg.

##### 3.8.1.1.1.2 Registro de cuenta de notificación en FastPrg

Cada cuenta de Telegram tendrá su configuración detallada y contará con los siguientes atributos:

- ✓ Número de teléfono: Atributo del tipo "Teléfono celular". El número tiene que estar en formato internacional de celular. (Por ejemplo +543413722918)
- ✓ Identificador de aplicación: Atributo tipo "Entero 9". Número de identificación brindado por la aplicación. (API\_ID)
- ✓ Hash de aplicación: Algoritmo matemático brindado por la aplicación. Es un atributo del tipo "texto medio". (API\_HASH)
- ✓ Hash de autorización del teléfono: Algoritmo matemático de autorización brindado por la aplicación. También es un atributo del tipo "texto medio".
- ✓ Código de autorización del teléfono: Código de autorización brindado por la aplicación y emitido al número de teléfono celular. Es un atributo del tipo "Texto 100"
- ✓ Data center de telegram: Tipo de atributo "Texto 100". Es visible solo en el modelo Editores, aquí se almacena el código provisto por Telegram mediante el mismo permite conectarse a los servidores de Telegram.
- ✓ Clave de autorización: Tipo de atributo "Texto 500". Es visible solo en el modelo Editores, aquí se almacena el código provisto por Telegram mediante el cual se posibilita la conexión a los servidores.
- ✓ Respuesta de Telegram: Json de respuesta de Telegram, almacena la información necesaria al momento de iniciar sesión por cada cuenta de notificación para el servicio de Telegram. El valor de este campo es modificado a través de las funciones (Solicita código de autorización de Telegram, Inicia sesión en Telegram). Tipo de atributo Texto "10000". Este campo es visible únicamente en el modelo editores.

Para poder realizar la validación de la cuenta, primero se deberán ingresar el número de teléfono, el ID de aplicación y hash de aplicación. En este momento se habilitará un botón denominado "Solicitar código" que completará automáticamente el hash de aplicación y enviará un código por Telegram que deberá ingresarse en el campo Código de autorización.

Finalmente, veremos otro botón "Validar código" que al presionarlo concluirá la autorización, se guardará la cuenta y se habrá realizado el Sign In.

### Cuenta de mensajería instantánea

Tipo de mensajería  
 Telegram

---

Cuenta de Telegram
 

Número de teléfono \*

Identificador de aplicación

Hash de aplicación

Hash de autorización del teléfono

Código de autorización del teléfono

El código una vez validado muestra el textbox deshabilitado y con: \*\*\*\*\*

Si se cambia algún dato (por ejemplo, hash de autorización) y se blanquea el código recibido por SMS, el usuario deberá volver a enviar el código y luego validarlo para que la cuenta sea válida nuevamente.



Cuenta 1 ✕

General Historial de Versiones Seguridad Documentación

Nombre (\*) Cuenta 1

Descripción

Plataforma (\*) Telegram

Id (\*) 79536

Hash (\*) 781046f35895a4b6d935479dd8ea1712

Configuración de producción (\*) 149.154.167.50:443

Clave pública (\*)  
DONS789sVoD/xCS9Y0hk9kwd9P0NsZRPsmoqVwMbMu7mStFai6alh3n  
Slv8kg9qv1m6XH/VQY3PnEw+QQtqStXklHwID+RwFMOOul9lcixlEKzwkENj1Yz/s7daS  
an9tqw3bfUv/hqgbhGx8kC3gtL1tSTlTgCbCVfaigxX0CDqVVeR1yFL1v/+7RF AEddlLm  
AjnK7a+XY19sluzHRyVvaTTveB2GazMITwEfkz2DVgkBlumI8OREmvfraX3bkHZJTKX  
4EQSjBbbdJ2ZxIsRrYOXfaA+xayEGB+  
8hBCgKCAAwVACQEPi9w23mF3tBkdZz+zwzKOaaQdr01vAbU4E1pvkfj4sqDsm6  
lyAQAB

Enviar código

Clave recibida por SMS (\*) \*\*\*\* Validar cuenta ✓

Para el caso de que el tipo de cuenta sea SMS, se presentarán las siguientes configuraciones:

- ✓ Tipo de Gateway: existen 2 formas de mandar SMS: por medio de un Gateway propio o por medio del Gateway de Neuralsoft. Si se elige el Gateway de Neuralsoft, se deberá abonar un costo. En el caso de querer usar su propio Gateway, se deberá configurar:
  - Forma de envío. El SMS se puede enviar por medio de un web service o por medio de un email.
    - Si la forma de envío es WS, se deberá configurar mediante qué cuenta de WS se realizará y qué método del mismo se invocará. Además, en la cuenta de WS se configuran los parámetros de cada método, por lo tanto, en la cuenta IM de SMS se debe elegir qué parámetro se usa para número destinatario y qué parámetro se usa para mensaje. El valor del número de teléfono y el valor del mensaje sólo se configuran en la RN y son obligatorios.
    - Si la forma de envío es Email, se deberá configurar mediante qué cuenta de Email se realizará (antes era más usado este tipo de envío de SMS, se puede poner el número en el asunto o en el “para”, y el mensaje en el cuerpo de email).

Cuenta 1 ✖

General | Historial de Versiones | Seguridad | Documentación

Nombre (\*)

Descripción

Plataforma (\*)

Tipo de gateway (\*)

Forma de envío (\*)

Web service (\*)

Método (\*)

Parámetro del número destinatario (\*)

Parámetro del mensaje (\*)

Validar cuenta ✓

Luego de validada la cuenta, se podrá usar en acciones de RN para IM.

En caso de copiarse la cuenta de mensajería instantánea en otros modelos vinculados, distintos de donde se creó la misma, se copiará sólo las propiedades Nombre y Descripción, el resto de las propiedades quedan en blanco en el modelo vinculado teniendo que especificarse luego.

Si la cuenta es utilizada faltando definir propiedades obligatorias, dará una excepción en tiempo de ejecución en la cola de mensajería instantánea mostrando al usuario un mensaje y logueando el error en el log correspondiente.

### 3.8.1.2 Cuentas para envío de email

En el dominio se podrán definir cuentas para el envío correos electrónicos de diferentes proveedores. Se deberá tener en cuenta que según el Proveedor de email que se seleccione, la configuración a definir puede presentar variaciones.

Para todas las cuentas se definen las siguientes propiedades:

- ✓ **Nombre:** Permite definir un nombre de la cuenta de email a crear. El mismo debe ser único en el sistema y para el idioma en que se está modelando, además, será pasible de internacionalización. Este dato es obligatorio.
- ✓ **Descripción:** Permite ingresar un texto donde se describe más en detalle la cuenta a crear. Este campo será pasible de internacionalización.
- ✓ **Proveedor de e-mail:** Combo de selección única donde se permite elegir el proveedor de e-mail de la cuenta. Las opciones disponibles son: Gmail, Outlook, Exchange u Otro.
- ✓ **Nombre de usuario:** Permite ingresar el nombre de usuario que se presentará como remitente del e-mail enviado. Este dato es obligatorio.

- ✓ **Contraseña:** permite ingresar la contraseña de la cuenta de email que se configura. Este dato es obligatorio.
- ✓ **Dirección de correo:** permite ingresar la dirección de correo desde la cual se enviará el e-mail y en la cual recibirá las respuestas. Este dato es obligatorio.
- ✓ **Validar cuenta:** Este botón permite validar los datos de la cuenta que se crea. Esta acción envía un correo de verificación a la cuenta configurada.

En las cuentas de los proveedores **Gmail, Outlook y Otras** además se deben configurar las siguientes propiedades:

- ✓ **Seguridad de la conexión:** Combo de selección única donde se permite elegir el protocolo criptográfico que se utilizará para lograr una comunicación segura a través de la red. Las opciones son: SSL-TLS, STARTTLS o Ninguno.
- ✓ **Host:** Permite ingresar el nombre de servidor de la cuenta que se configura.
- ✓ **Puerto:** Permite especificar el punto de acceso por el cual se transferirán los e-mails.

En las cuentas de Exchange además se deben configurar las siguientes propiedades:

- ✓ **URL EWS:** Permite ingresar la URL para conectar con el servidor de Exchange
- ✓ **Dominio EWS:** Permite ingresar el dominio de la cuenta Exchange que se crea.

Luego de validada la cuenta, se podrá usar en acciones de RN para envío de email, para asociar a un usuario, enviar GDI, etc.

En caso de copiarse la cuenta de email en otros modelos vinculados, distintos de donde se creó la misma, se copiará las propiedades Nombre y Descripción, el resto de las propiedades quedan en blanco en el modelo vinculado teniendo que especificarse luego.

Si la cuenta es utilizada faltando definir propiedades obligatorias, dará una excepción en tiempo de ejecución en la cola de envío de emails mostrando al usuario un mensaje y logueando el error en el log correspondiente.

### 3.9 Agentes

En el dominio pueden crearse agentes, estos generan instaladores que vinculan el agente al host donde se instala y permiten el uso de impresoras u otros dispositivos.

En la solapa General se definen las siguientes propiedades:

- ✓ Nombre: Permite definir un nombre del agente a crear. El mismo debe ser único en el sistema, en cada idioma, además, será pasible de internacionalización. Este dato es obligatorio.
- ✓ Descripción: Permite ingresar un texto donde se describe más en detalle el agente la cuenta a crear. Este campo será pasible de internacionalización.

Una vez completas las propiedades requeridas anteriores y confirmada la instancia, se habilita el botón “Descargar”, esta acción genera el agente correspondiente e inicia la descarga del mismo para que el usuario pueda instalarlo.

Cuando se genera el agente se incluyen las credenciales (token, certificado, o las que correspondan) en el instalador que luego descarga el usuario.

La instalación del agente permite vincular el host donde se instala con el agente dado de alta. Una vez que se encuentra vinculado el agente, se visualizan otros campos informativos en solo lectura: estado, fecha instalación, [última fecha de conexión](#).

También se visualiza una grilla con todos los periféricos (dispositivos) detectados que reconoce el agente. Por cada uno se visualiza:

- Nombre detectado: es el nombre del dispositivo que reconoce el agente.
- [Nombre en el dominio: se completa con el nombre de dispositivo vinculado, en caso que se corresponda con alguno de los dispositivos agregados al dominio.](#)
- Estado: es “Habilitado” si el agente está vinculado y se detecta el dispositivo o “Inhabilitado”, si el agente ya no está vinculado, y se dejó de detectar el dispositivo.

En caso que el agente haya sido descargado e instalado, en el botón en vez de la opción “Descargar” se visualiza la opción “Desvincular agente”, si se selecciona esta opción se notifica al usuario con una advertencia que se anulará el agente instalado y que los dispositivos vinculados a ese agente dejarán de prestar servicios no quedando disponibles. Se vuelve a visualizar la opción “Descargar” y en la grilla se visualizan los dispositivos detectados pero ahora con estado “Inhabilitado”.

Cuando se vuelve a vincular el agente (descargar e instalar), se actualiza la grilla con la lista de dispositivos nuevos detectados, si tienen igual nombre que los anteriores detectados tendrá estado “Habilitado” y si además corresponde con uno de los dispositivos vinculados del dominio, el mismo ya disponible para su uso, sino puede ocurrir que alguno de los dispositivos vinculados del dominio quede inválido porque cambiaron los dispositivos detectados, en este caso se notificará el error en tiempo de ejecución cuando se quiera consumir el dispositivo.

Por ejemplo, se creó y configuró el Agente X, que reconoce a los dispositivos: HP LaserJet Pro MFP M127fn, HP Color Laser Jet CP2025dn, Lector Código Barras Dynapos Laser Usb Syn-hh10b. También se configuraron los dispositivos en el dominio, visualizándose en el Agente X la siguiente grilla de dispositivos.

Dispositivos detectados		
Nombre detectado	Nombre en el dominio	Estado
HP LaserJet Pro MFP M127fn	Impresora Administración	Habilitado
HP Color LaserJet CP2025dn	Impresora Remitos	Habilitado
Lector Código De Barras Dynapos Laser Usb Dyn-hh10b	Lectora Despacho	Habilitado

Luego se vuelve a instalar el Agente X anulando el anterior y cuando vuelve a detectar los dispositivos conectado reconoce los siguientes: HP LaserJet Pro MFP M127fn e Impresora Multifunción Epson L220.

**Pudiéndose mostrar una de las siguientes opciones:**

1)

Dispositivos detectados		
Nombre detectado	Nombre en el dominio	Estado
HP LaserJet Pro MFP M127fn	Impresora Administración	Habilitado
HP Color LaserJet CP2025dn	Impresora Remitos	Inhabilitado
Lector Código De Barras Dynapos Laser Usb Dyn-hh10b	Lectora Despacho	Inhabilitado
Impresora Multifuncion Epson L220		Habilitado

2)

Dispositivos detectados		
Nombre detectado	Nombre en el dominio	Estado
HP LaserJet Pro MFP M127fn	Impresora Administración	Habilitado
Impresora Multifuncion Epson L220		Habilitado

El dispositivo Impresora Administración definido en el dominio podrá seguir utilizándose sin inconvenientes.

Pero los dispositivos Impresora Remitos y Lectora Despacho (los inhabilitados) dejarán de ser válidos y si por ejemplo se elige la impresora Remitos para enviar a imprimir un comprobante se notificará el error al usuario.

El sistema registra la fecha y hora en que el usuario realiza las acciones anteriores, descarga, vinculación o desvinculación del agente para auditorias futuras.

A continuación se visualiza el caso en que el agente ya se encuentra instalado:

Enterprise Neuralsoft v1 Producción Argentina

09:30:24 Cecilia López

↶ ↷ 📄 📄 📄 📄 📄

Dominio

Administrador de Modelos

Versionado

Tipos de atributo

Entidades

Nombre

Procesos de negocio

Reglas de negocio

Secuenciadores

Gestor dinámico de información

Programador de tareas

Modelos de dispositivo

Integración con Fuentes de Datos Externas

Funciones

Organigramas

Calendarios

Colas de Inbox

Inbox

Mapas estratégicos

Inteligencia estratégica

Market Place

Carpetas personales

Agente

General

Historial de Versiones

Seguridad

Documentación

Ubicación

dominio.com / Equipos

Nombre \*

Agente área administración

Descripción

Agente de impresión que se utiliza en el área de administración

Desvincular agente

Dispositivos detectados

Nombre detectado	Nombre en el dominio	Estado
HP LaserJet Pro MFP M127fn	Impresora Administración	Habilitado
Microsoft Print to PDF		Habilitado
Fax		Habilitado
Teclado		Habilitado
HP Color LaserJet CP2025dn	Impresora Marketing	Habilitado

Ítem de solapa "Seguridad"	Usuario		Sitio	Dispositivo	Grupo			De usuarios
	Local	Externo			De usuarios	Predefinido (Rol)	De sitios	
<b>Administrar usuarios</b>	✓	✓			✗	✗		✓
Crear					✗	✗		✓
Consultar	✓	✓			✗	✗		✓
Modificar	✓	✓			✗	✗		✓
Modificar foto	✓							✓
Modificar contraseña	✓							✓
Modificar e-mail	✓							✓
Modificar teléfono celular	✓							✓
Modificar domicilio	✓							✓
Eliminar	✓	✓			✗	✗		✓
Restaurar	✓	✓			✗	✗		✓
Traducir	✓	✓			✗	✗		✓
Administrar permisos (consultar y modificar)	✓	✓			✗	✗		✓
<b>Administrar grupos de usuarios</b>					✓	✓		✓
Crear (sólo para grupos contenidos)					✓	✓		✓
Consultar					✓	✓		✓
Modificar (sólo para grupos contenidos)					✓			✓
Eliminar (sólo para grupos contenidos)					✓	✓		✓
Restaurar (sólo para grupos contenidos)					✓	✓		✓
Traducir (sólo para grupos contenidos)					✓	✓		✓
Administrar permisos (consultar y modificar)					✓	✓		✓
<b>Administrar unidades organizacionales</b>								✓
Crear (sólo para OU contenidas)								✓
Consultar								✓
Modificar								✓
Eliminar								✓
Restaurar								✓
Traducir								✓
Administrar permisos (consultar y modificar)								✓
<b>Administrar dispositivos</b>				✓				✓
Crear								✓
Consultar				✓				✓
Modificar				✓				✓
Utilizar dispositivo				✓				✓



Ítem de solapa "Seguridad"	Usuario		Sitio	Dispositivo	Grupo			De usuarios
	Local	Externo			De usuarios	Predefinido (Rol)	De sitios	
Eliminar				✓				✓
Restaurar				✓				✓
Traducir				✓				✓
Administrar permisos (consultar y modificar)				✓				✓
<b>Administrar sitios</b>			✓				✗	
Crear							✗	
Consultar			✓				✗	
Modificar			✓					
Acceder			✓				✗	
Eliminar			✓				✗	
Restaurar			✓				✗	
Traducir			✓				✗	
Administrar permisos (consultar y modificar)			✓				✗	
<b>Administrar grupos de sitios</b>							✓	
Crear <i>(sólo para grupos contenidos)</i>							✓	
Consultar							✓	
Modificar <i>(sólo para grupo editado)</i>							✓	
Eliminar							✓	
Restaurar							✓	
Traducir							✓	
Administrar permisos (consultar y modificar)							✓	
<b>Administrar OU de sitios</b>								
Crear <i>(sólo para OU contenidas)</i>								
Consultar								
Modificar								
Eliminar								
Restaurar								
Traducir								
Administrar permisos (consultar y modificar)								

Se deberá tener en cuenta que si un usuario cuenta con permiso de modificación sobre un objeto, también tendrá permiso de consulta sobre el mismo. Por ejemplo, si un usuario cuenta con permiso de modificación de un sitio, podrá visualizar los datos del sitio.

### 3.11 Panel de Navegación

La sección del panel de navegación (acordeón) llamada “*Dominio*” contendrá:

- <Nombre Dominio Principal>
  - <Agentes>
  - “Dominios de autenticación”
    - <Nombre Dominio A>
      - <Nombre Objetos compartidos>
    - <Nombre Dominio B>
    - ...
- <Nombre OU raíz>
  - <Usuarios>
  - <Grupos de usuarios> (incluye roles)
  - <Dispositivos>
  - <Puestos de trabajo>
  - <OU>
    - <Usuarios>
    - <Grupos de usuarios>
    - ...
- <Nombre OU raíz de sitios> (el nombre puede ser “Sitios”)
  - <Sitios>
  - <Grupos de sitios>
  - <OU de sitios>
    - <Sitios>
    - <Grupos de sitios>
    - <OU de sitios>
- “Cuentas”
  - “Cuentas para envío de email”
    - <Cuenta 1>
    - <Cuenta 2>
  - “Cuentas para envío de mensajería instantánea”
    - <Cuenta 1>
    - <Cuenta 2>
  - “Grupos de servicios web”
    - <Cuenta 1>
    - <Cuenta 2>

### 3.12 Políticas para Solicitar pantalla y Compartir Pantalla

Políticas de seguridad relacionadas con la funcionalidad de Solicitar pantalla y Compartir pantalla.

- Solicitar pantalla al dominio propio: permite al usuario solicitante tener el permiso para pedir acceso a la sesión de los usuarios del dominio actual.

- Solicitar pantalla a otros dominios externos: (permite al usuario solicitante tener el permiso para pedir acceso a la sesión de los usuarios de los dominios externos que tenga confianza otorgada.

- Compartir pantalla al dominio propio: permite al usuario solicitante tener el permiso para compartir la sesión propia a los usuarios del dominio actual

- Compartir pantalla para otros dominios externos: permite al usuario solicitante tener el

permiso para compartir la sesión propia a los usuarios de los dominios externos que tenga confianza otorgada.

- Solicitar control: permite al usuario solicitante, toma el control de la sesión a la cual se encuentra participando para poder manejar el cursor y realizar cambios.

- Ceder el control: permite al usuario asistido, otorgarle al otro usuario el control de la sesión a la cual se encuentra participando para poder manejar el cursor y realizar cambios.

Las políticas de seguridad se deben definir a nivel Marketplace, para que se pueda decidir qué dominios pueden solicitar control. Esta configuración se realiza en la instancia de Dominio de implementación teniendo en cuenta los dominios a los que se tiene confianza.

Cuando se desee otorgar la política de solicitud y compartición de pantalla para dominios externos, sólo se debe permitir para aquellos dominio de implementación que tengan otorgados dominios. Por ejemplo:

ISV 'Irontech' sólo posee permisos para solicitar pantalla a los usuario del dominio propio. Fastprg posee permisos para solicitar pantalla a los usuarios del dominio propio y adicionalmente a ISV 'Irontech'.

## 4 Herramientas dinámicas

Al crear una herramienta dinámica en algún ambiente que no sea el de desarrollo, el usuario "creador" de esta herramienta tendrá todos los permisos sobre la misma en ese ambiente. Esto aplicará a todas las herramientas dinámicas, como por ejemplo:

- Reglas de negocio
- GDI
- Tareas programada
- Tareas de integración
- Planes de integración
- Web services
- Conexiones
- Reportes por banda
- Funciones

El comportamiento esperado es:

Si un usuario crea uno de los elementos mencionados anteriormente en un ambiente que no sea desarrollo, el sistema automáticamente le brindará al usuario todos los accesos al elemento.

Si un usuario se está agregando a sí mismo a la grilla de seguridad de alguno de los elementos de arriba, se le marcarán todos los permisos como permitido en el ambiente actual. Esto aplica a los ambientes de producción y prueba.

## 5 Delegación de Actividades

Tanto desde el *ribbon*, como desde el panel de navegación en la sección “Procesos de Negocio”, se podrá acceder a la consulta de *Actividades Delegadas*, desde la cual se podrá administrar de una forma centralizada las actividades que un usuario delega. Su funcionalidad es que un usuario pueda conceder a otros usuarios la autorización de ejecutar actividades en nombre del primero.

Se denomina usuario *delegador* a aquel usuario que delega una o varias actividades, es decir, el usuario que con sus permisos puede realizar la actividad. Por otro lado, se denomina usuario *delegado* al usuario a quien le delegan actividades. Un usuario delegador podrá delegar una o más actividades a cada usuario delegado. Un usuario puede ser delegador y delegado a la vez.

Además, desde el menú contextual sobre un usuario existirá la opción “*Delegar actividades*” y la opción “*Consultar Actividades Delegadas*”. La primera opción abrirá la consulta de Actividades Delegadas con el usuario seleccionado como usuario delegado y con el usuario autenticado como usuario delegador. La segunda opción abrirá la consulta de Actividades Delegadas con el usuario seleccionado como usuario delegador, es decir, las actividades delegadas del usuario seleccionado. En este último caso, la consulta será de sólo lectura.

Un usuario delegador deberá tener activa la política “Delegación de actividades” y sólo podrá delegar actividades a los usuarios que autorice la política (a todos, a sus pares y subordinados o sólo a sus subordinados). De la misma manera, para que un usuario pueda consultar actividades delegadas de otros usuarios, debe tener activa la política “Consulta de actividades delegadas” y sólo podrá consultar actividades delegadas de los usuarios autorizados por la política (a todos, a sus pares y subordinados o sólo a sus subordinados).

Aclaración: los pares y los subordinados de cada usuario se definen en el organigrama de seguridad.

Las actividades se podrán delegar de manera permanente o de manera transitoria. Por lo tanto, a cada usuario se le pueden delegar distintas actividades en distintos tiempos.

La interfaz de las Actividades Delegadas será:

Actividades Delegadas ✖

**Definir los usuarios a los cuales desea delegar actividades:**  
Haga clic en la lista o arrastre usuarios desde el panel de navegación a la lista siguiente.

Usuario

Jack Martel

Lucy Hale

Mike Anderson

**Definir las actividades delegadas para cada usuario:**  
Configure el período de delegación y las actividades que desea delegar por cada período. Luego presione el botón confirmar.

[ - ] Inicio (\*) Hoy 00:00:00

Frecuencia (\*) Siempre

Definir franja horaria ☐

Desde 00:00:00 Hasta 23:59:59

Activar expiración ☐

Expira el  a las 00:00:00

**Actividades a delegar**

Actividad	Actividad Delegada	Usuario delegador	Período delegado	Delegar
Realizar Pedido de Venta				<input checked="" type="checkbox"/>
Remitir por Mayor				<input type="checkbox"/>
Facturar por Mayor				<input checked="" type="checkbox"/>


En la sección superior, se podrán agregar o quitar usuarios a los cuales se les delega actividades.

En la sección inferior, al seleccionar un usuario se podrá configurar tanto el período de delegación (permanente o transitorio) como las actividades delegadas por cada período. Además, contará con un botón que servirá para confirmar lo que se está editando. Este botón se encuentra dentro de una barra de Navegación de Instancias, tal como se detalla en el documento [Formularios](#), pero a diferencia de los Formularios, no hay otras opciones dentro de esta barra.

El período hará referencia a la hora y fecha de la zona horaria del sitio donde el usuario delegador se autenticó. En este período se puede definir:

- ✓ Inicio: es obligatorio definir la fecha y el horario de comienzo de delegación, es decir, desde cuando el usuario delegado podrá ejecutar la/s actividad/es delegadas. De manera predeterminada, este valor estará vacío para que el usuario lo complete obligatoriamente.
- ✓ Frecuencia: es obligatorio definir la frecuencia o repetición de delegación. Las opciones de este combo son: siempre, semanal, mensual y anual. La opción predeterminada es “siempre”, la cual permitirá definir una actividad delegada que se pueda ejecutar en todo momento dentro de las fechas y horas de inicio y expiración. Las particularidades de cada opción se definen en el documento [Reglas de Negocio](#).
- ✓ Definir franja horaria: al activar este *checkbox*, el usuario podrá definir una hora de inicio y de fin para que la actividad delegada puede ser ejecutada por el usuario delegado, dentro de cada día que se defina a partir del campo “Frecuencia”. De manera predeterminada, la franja horaria no estará activa, y al activarla, sus valores iniciales son: Desde 00:00:00 Hasta 23:59:59.
- ✓ Activar expiración: al activar este *checkbox*, el usuario podrá definir una fecha y hora de expiración, luego de la cual, el usuario delegado no podrá ejecutar la actividad

delegada. De manera predeterminada, la expiración no estará activa, al activarse, la fecha y el horario estarán vacíos inicialmente.

Se podrán agregar otros períodos con , y dentro del nuevo período se podrán delegar las mismas u otras actividades pero al mismo usuario (el usuario seleccionado en la grilla de la sección superior).

Si el período de delegación termina, el usuario delegado no podrá ejecutar las actividades delegadas, pero esta delegación seguirá visualizándose en la consulta de Actividades Delegadas.

Si un usuario posee una actividad delegada por un determinado período y este, a su vez, desea delegarla a otro usuario por otro período, el período efectivo o período resultante será aquel que esté incluido en ambos períodos (la intersección). Por ejemplo: si la actividad está delegada desde el 04/05 al 10/06/2016 y el usuario delegado decide delegarla desde el 01/06/2016 con una frecuencia semanal de días lunes de 9 a 15:30 hs, entonces el período efectivo será los días lunes de 9 a 15:30 hs desde el 01/06 al 10/06/2016. Esto se visualizará en un *tooltip* dentro de un icono representativo en dicha actividad.

**Definir las actividades delegadas para cada usuario:**  
Configure el período de delegación y las actividades que desea delegar por cada período. Luego presione el botón confirmar.

[.] Inicio (\*) 01/06/2016 07:00:00

Frecuencia (\*) Semanal

Días (\*) Lunes

Definir franja horaria ☒

Desde 09:00:00 Hasta 15:30:00

Activar expiración ☐

Expira el a las 00:00:00

**Actividades a delegar**

Actividad	Actividad Delegada	Usuario delegador	Período delegado	Delegar
Realizar Pedido de Venta				<input checked="" type="checkbox"/>
Transformar Pedido de Ventas en Orden de Despacho Pendiente				<input type="checkbox"/>
Remitir por Mayor				<input checked="" type="checkbox"/>
Facturar por Mayor				<input type="checkbox"/>
	Facturar por menor	Mary Johnson	Desde 04/05/2016 hasta 10/06/2016	<input checked="" type="checkbox"/>
	Facturar por menor	Adam Williams	Siempre	<input type="checkbox"/>

El período efectivo de delegación será: los días lunes de 9:00 a 15:30 hs, desde el 01/06/2016 hasta el 10/06/2016.

Las actividades que se podrán delegar serán las que pueda ejecutar el usuario delegador en el ambiente en que se encuentra autenticado. Estas actividades se visualizarán en sólo lectura, en una grilla dentro del período de delegación. Los datos que se visualizarán de las Actividades son: el nombre de cada Actividad y si es delegada, el usuario delegador y el período.

Al activar el *checkbox* de la columna Delegar sobre un Proceso de Negocio, se seleccionarán automáticamente las actividades de dicho PN en ese momento. En caso de que luego de delegar el Proceso de Negocio, el usuario delegador puede ejecutar más actividades dentro de dicho PN, automáticamente las podrá ejecutar el usuario delegado.

La delegación de actividades se podrá realizar:

- ✓ Entre usuarios del mismo dominio.
- ✓ Desde usuarios locales a los usuarios externos que hayan previamente establecido un vínculo de seguridad con el dominio local.

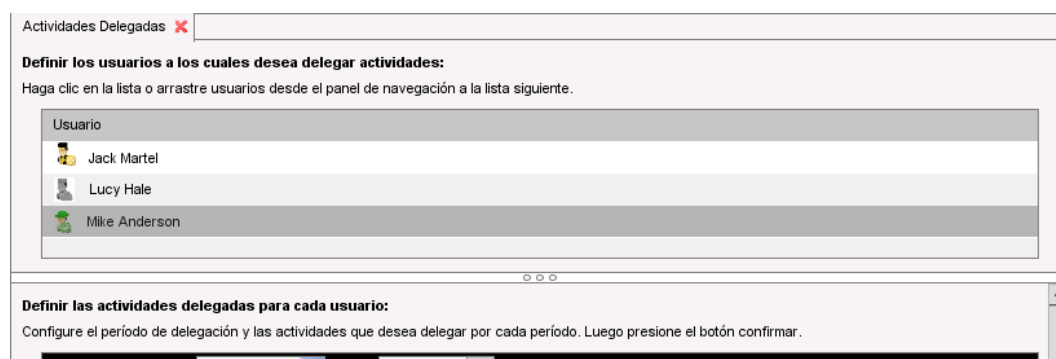
- ✓ Desde usuarios externos a los usuarios locales.
- ✓ Entre usuarios externos que hayan previamente establecido un vínculo de seguridad con el dominio local.

A continuación se detalla un ejemplo de delegación de un usuario a otro.

En este ejemplo, el usuario autenticado es Jack Collins. Dicho usuario tiene la política que le permite delegar actividades a sus subordinados. Por lo tanto, al ingresar al menú contextual sobre el usuario Mike Anderson, que es uno de sus usuarios subordinados, podrá acceder a la opción “Delegar Actividades”.



A diferencia de acceder a la consulta de Actividades Delegadas desde el *ribbon* o desde el panel de navegación, cuando se ingresa desde el menú contextual de un usuario, dicho usuario se agregará a la grilla de usuarios delegados, o aparecerá seleccionado si el mismo ya se encuentra entre los usuarios delegados.



Se inicializará el período con las configuraciones predeterminadas.

Luego, el usuario delegador podrá configurar los períodos que desee y por cada uno de estos periodos, deberá seleccionar una o más actividades para delegar. Por ejemplo:

Actividades Delegadas ✕

**Definir los usuarios a los cuales desea delegar actividades:**  
Haga clic en la lista o arrastre usuarios desde el panel de navegación a la lista siguiente.

Usuario
Jack Martel
Lucy Hale
Mike Anderson

**Definir las actividades delegadas para cada usuario:**  
Configure el período de delegación y las actividades que desea delegar por cada período. Luego presione el botón confirmar.

**Inicio (\*)** Hoy 00:00:00

Frecuencia (\*) Siempre

Definir franja horaria ☐

Desde 00:00:00 Hasta 23:59:59

Activar expiración ☐

Expira el a las 00:00:00

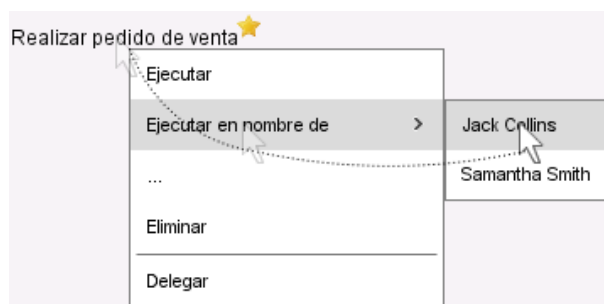
**Actividades a delegar**

Actividad	Actividad Delegada	Usuario delegador	Período delegado	Delegar
Realizar Pedido de Venta				<input checked="" type="checkbox"/>
Remitir por Mayor				<input type="checkbox"/>
Facturar por Mayor				<input checked="" type="checkbox"/>

Confirmar

Por último, el usuario delegador deberá confirmar la delegación presionando el botón confirmar.

En el momento en que el usuario delegador confirma la delegación, el usuario delegado tendrá disponible la ejecución de las actividades delegadas (siempre que se esté dentro del periodo de delegación de la actividad). Es importante aclarar, que si el usuario delegado se encuentra ejecutando la actividad cuando termina el período de delegación, entonces no podrá confirmar la misma. Las mismas tendrán un icono particular para indicar que son delegadas y podrán ser ejecutadas desde la opción "Ejecutar en nombre del usuario delegador" en el menú contextual de dichas actividades:



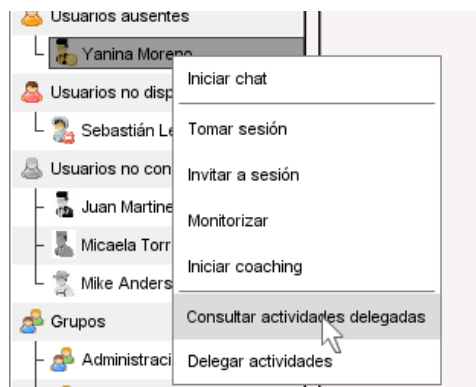
Si un usuario sólo puede ejecutar una actividad con permisos delegados de un solo usuario, entonces no será necesario ejecutar la actividad desde el menú contextual, se podrá ejecutar con permisos del otro usuario al hacer clic.

Así como desde cualquier lugar donde se acceda al menú contextual de una instancia se puede ejecutar las actividades permitidas por el usuario, también se podrán ejecutar las actividades



delegadas. Por ejemplo, dentro de una grilla, al ver una factura pendiente de transformar, se podrá invocar a la actividad para transformar la factura con los permisos propios o de otro usuario, si la actividad se encuentra delegada.

Por último, si el usuario autenticado tiene activa la política para consultar actividades delegadas de otro usuario, podrá hacerlo desde el menú contextual sobre el usuario y presionando la opción “Consultar Actividades Delegadas”



En este caso se visualizará la consulta de Actividades Delegadas con las actividades de usuario consultado y en solo lectura.

Actividades Delegadas de Yanina Moreno ✕

**Definir los usuarios a los cuales desea delegar actividades:**  
Haga clic en la lista o arrastre usuarios desde el panel de navegación a la lista siguiente.

Usuario

- Jack Martel
- Lucy Hale
- Mike Anderson

**Definir las actividades delegadas para cada usuario:**  
Configure el período de delegación y las actividades que desea delegar por cada período. Luego presione el botón confirmar.

**Inicio (\*)** 09/09/2015 00:00:00

Frecuencia (\*) Siempre

Definir franja horaria ☐

Desde 00:00:00 Hasta 23:59:59

Activar expiración ☐

Expira el a las 00:00:00

**Actividades a delegar**

Actividad	Actividad Delegada	Usuario delegador	Período delegado	Delegar
Realizar Pedido de Venta				<input type="checkbox"/>
Remitir por Mayor				<input type="checkbox"/>
Facturar por Mayor				<input checked="" type="checkbox"/>

## 6 Organigramas

Un *organigrama* es la representación gráfica de la estructura de una empresa u organización. Se podrá definir tanto en tiempo de edición como de ejecución. Una organización podrá definir uno o varios *organigramas*. Por ejemplo, un organigrama por zona geográfica y otro jerárquico. Habrá un organigrama predeterminado de toda la organización, que será el utilizado en seguridad por organigrama.

Un *departamento* es un contenedor de integrantes de la organización.

Dentro de un *organigrama*, los integrantes pueden ser *pares*, *jefes* y/o *subordinados* de otros integrantes. A su vez, el jefe de un departamento podrá ser subordinado de otro. Un integrante corresponderá a un usuario. El organigrama podrá mostrar los datos de cada integrante, por ejemplo la foto.

- Un *departamento* podrá contener n *departamentos*.
- Un *departamento* podrá pertenecer a n *departamentos*.
- Un *subordinado* podrá tener n *jefes*.
- Un *jefe* podrá tener n *subordinados*.
- Un *integrante* podrá estar en n *departamentos*.
- Un *integrante* podrá tener n *puestos*, uno por *departamento*.

### 6.1 Seguridad por Organigrama

Cada organización podrá definir si tendrá *seguridad por organigrama*.

Se tomará como referencia al *organigrama predeterminado*, tanto para supervisión como para delegación de actividades a pares y subordinados. Dicho organigrama se verá reflejado en los datos generales de cada usuario: puestos, departamentos, jefes, pares y subordinados.

Se entenderá por *pares* a aquellos usuarios que se encuentren en el mismo departamento, y que no tengan entre ellos relación jefe/subordinado. Por otro lado, se entenderá por *subordinados* a aquellos usuarios dentro del mismo departamento que tengan dependencia del usuario jefe, así como a los usuarios de otros departamentos que tengan dependencia del departamento en cuestión. En el organigrama, se diferenciarán visualmente con una flecha que indicará dependencia, independientemente del departamento. Las relaciones no serán transitivas; por ejemplo al eliminar un usuario, su jefe y su subordinado no pasarán a estar vinculados de manera directa.

De acuerdo a la política de delegación de actividades, un usuario dado podrá delegar sus permisos a todos, a sus pares y a sus subordinados, sólo a sus subordinados o a nadie. En este contexto, será válido el concepto de *grant option*, por el cual un jefe podrá otorgar los permisos que posea -ya sea en forma temporal o permanente- a sus subordinados, de manera recursiva (esto es, a los subordinados de sus subordinados, y así sucesivamente). De la misma forma se procederá con la supervisión.

En la ACL de la solapa “Seguridad” de un organigrama se podrán administrar los siguientes permisos:

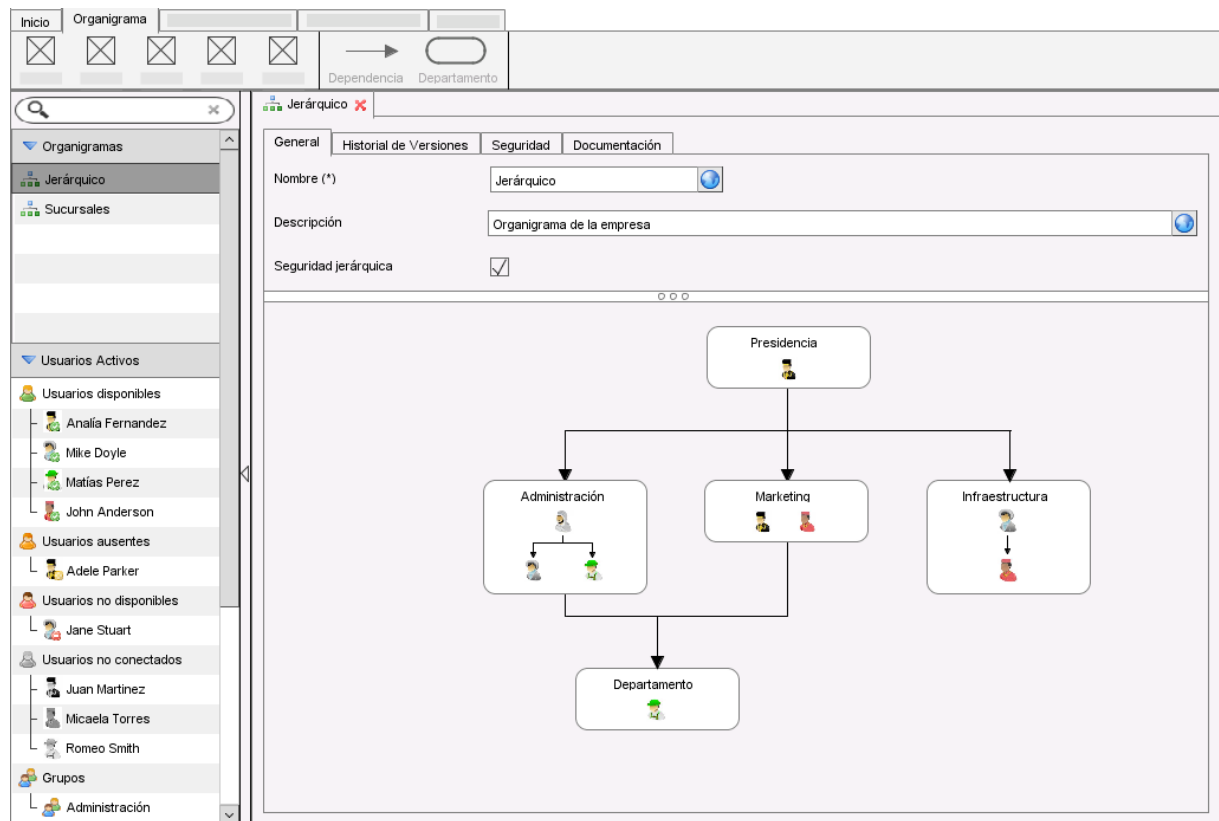
- ✓ *Administrar organigrama*: consultar/modificar datos/modificar seguridad jerárquica/modificar organigrama/modificar documentación/eliminar/traducir/administrar permisos.

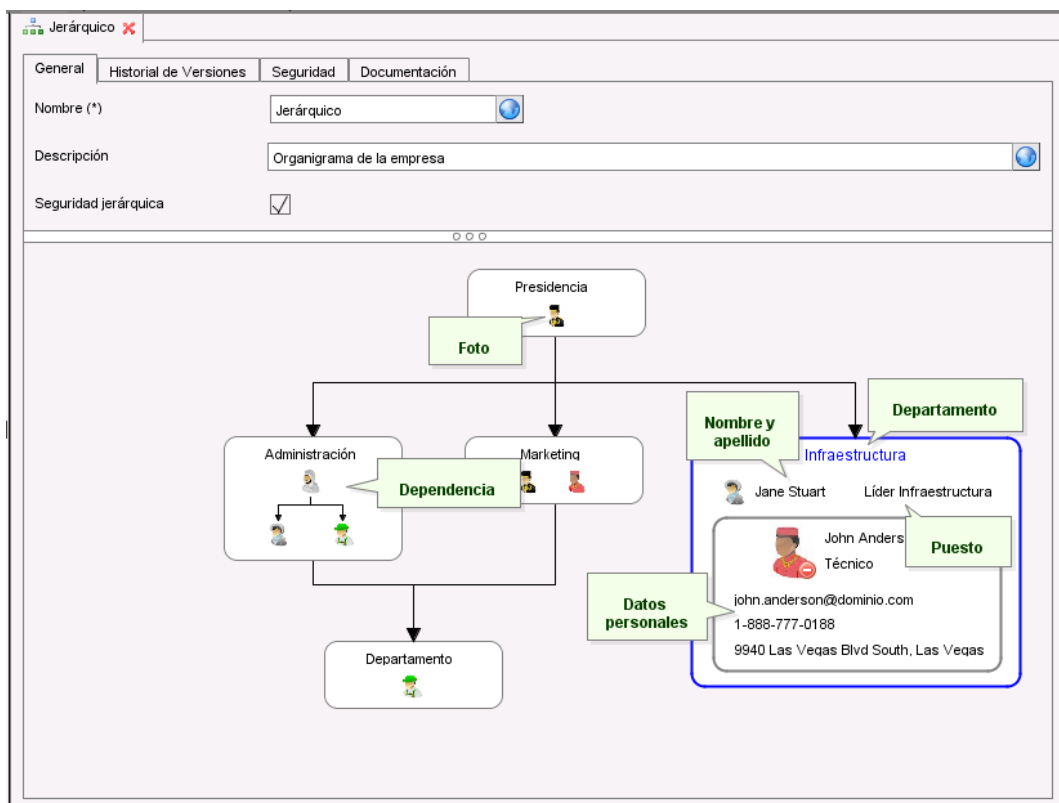
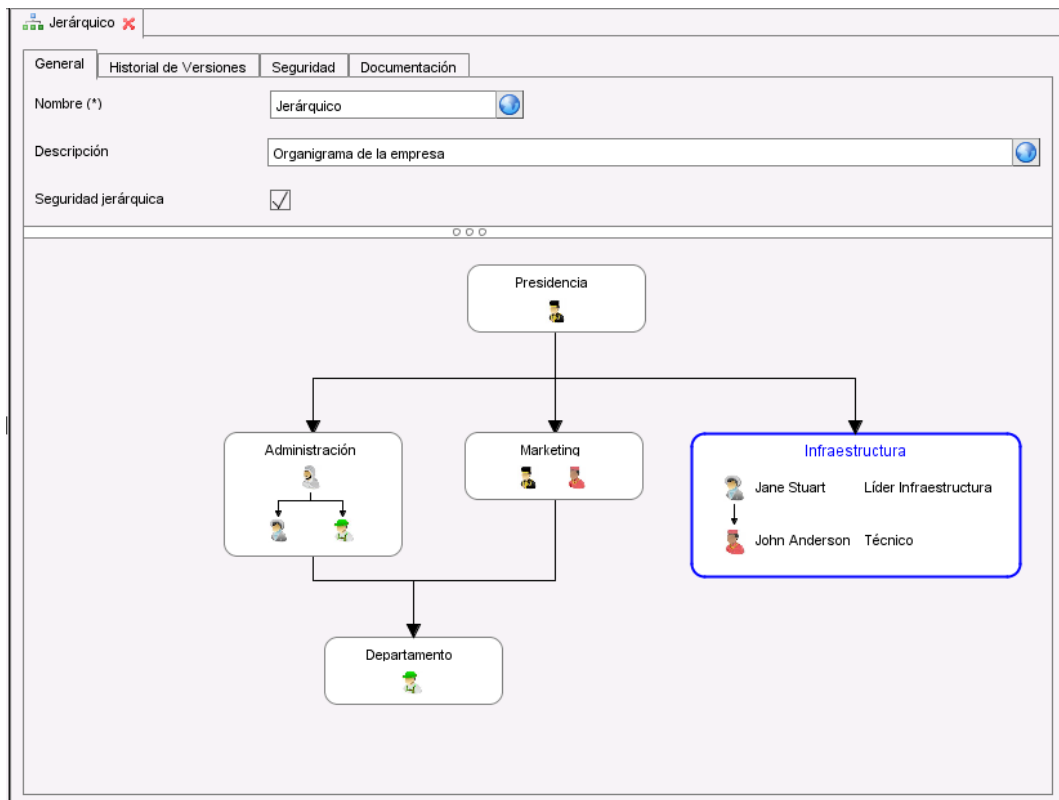
Si un usuario inhabilita la opción que indica que el organigrama tiene seguridad, o si elimina el organigrama predeterminado de seguridad, el sistema deberá consultarle al mismo si desea

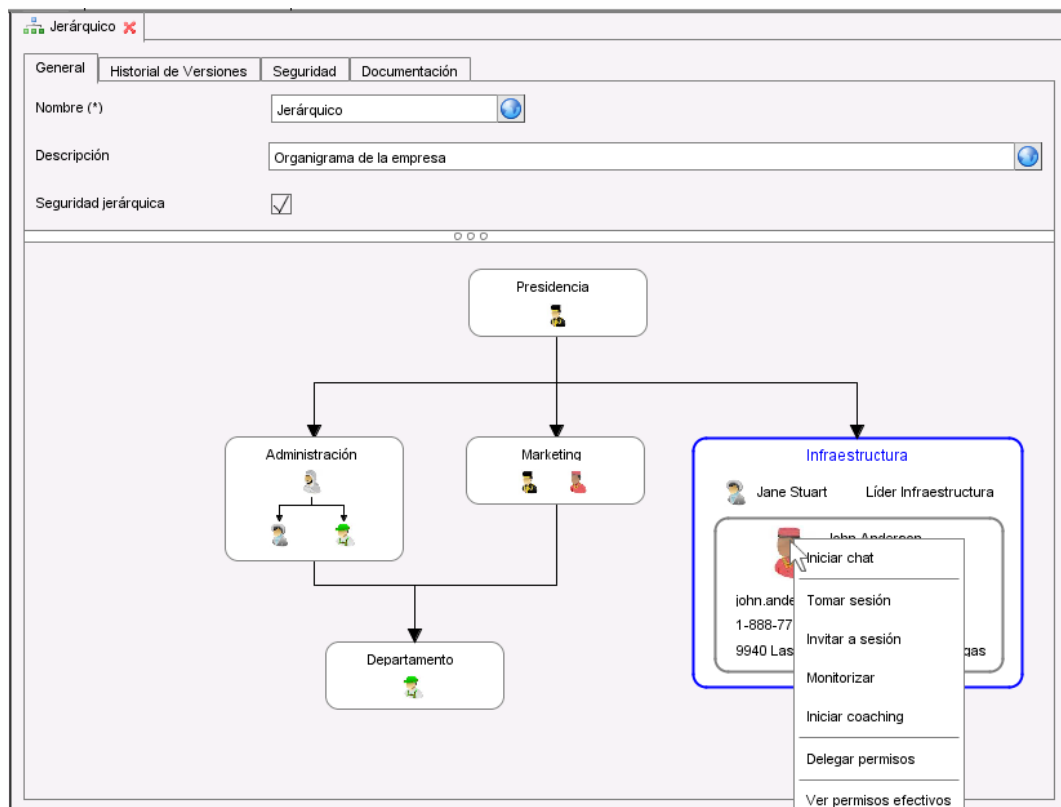
crear un nuevo organigrama con seguridad o si desea designar a otro organigrama como organigrama predeterminado de seguridad.

Existirá una paleta en el *ribbon* con los componentes propios del organigrama: departamento (área) y dependencia. Se podrán arrastrar los mismos mediante el drag & drop al diagrama, o crearlos desde el área de trabajo.

Se podrán agregar usuarios al organigrama, tanto desde el menú contextual del área de trabajo como desde el panel de navegación de usuarios mediante *drag & drop*.







The screenshot shows the 'Jerárquico' application interface with the 'Seguridad' tab selected. The page title is 'Definir la seguridad para los usuarios y grupos de usuarios:'. Below the title is a search bar and a table for defining permissions.

Permiso	Permitir	Denegar
▼ Administrar organigrama	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input type="checkbox"/>	<input type="checkbox"/>
Modificar datos	<input type="checkbox"/>	<input type="checkbox"/>
Modificar seguridad jerárquica	<input type="checkbox"/>	<input type="checkbox"/>
Modificar organigrama	<input type="checkbox"/>	<input type="checkbox"/>
Modificar documentación	<input type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>
Traducir	<input type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input type="checkbox"/>	<input type="checkbox"/>

## 7 Autenticación

La **Autenticación** en un sistema se define como el proceso de verificación de la identidad de un usuario que desea acceder al sistema.

La autenticación se divide en los siguientes pasos:

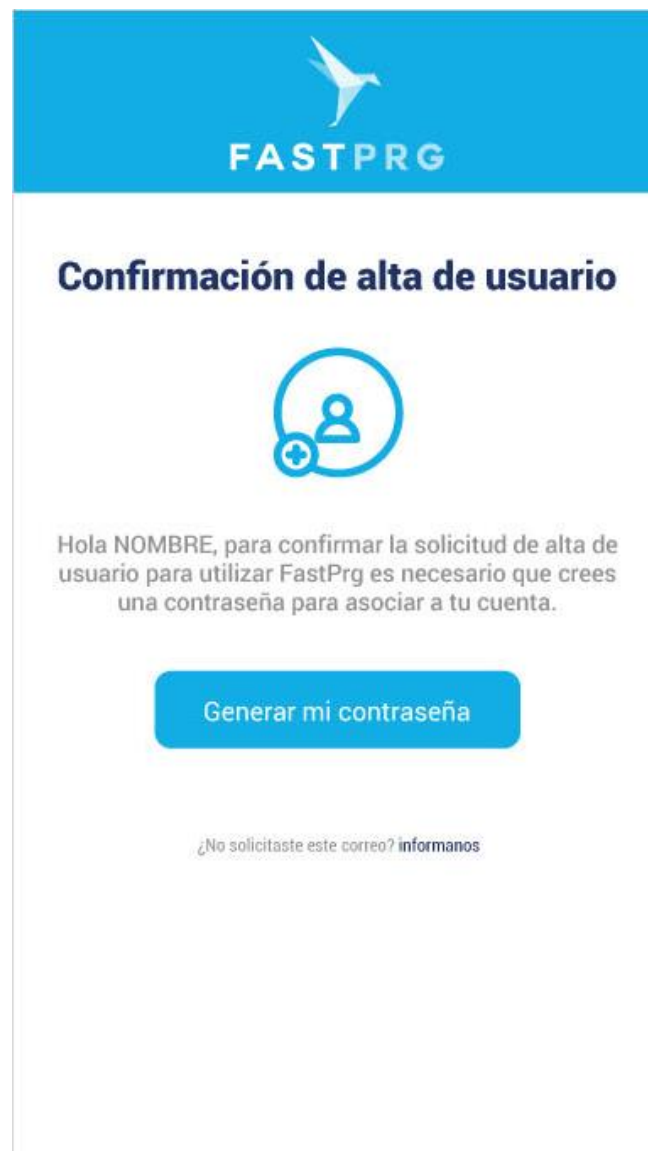
1. Pantalla inicial para realizar la autenticación.
2. Proceso de autenticación.

### 3. Ingreso al sistema.

#### 7.1 Primera autenticación


Al crear un usuario, se pedirá el email del mismo para su primer ingreso.


Al confirmar la creación del usuario nuevo, se procederá al envío de un link a la dirección de e-mail del usuario. Dicho link se podrá utilizar para acceder a un formulario de cambio de contraseña. **El link será válido por única vez, no pudiendo reutilizarse, y quedará sin efecto luego de 1 hora.**




Al ingresar al link, el usuario aparecerá en sólo lectura y se requerirá ingresar 2 veces la misma contraseña para poder ingresar:

Sign in to continue to the system







**SIGN IN**


## 7.2 Autenticación en un Dominio


La interfaz de ingreso al sistema dependerá del dominio y de la configuración de sus políticas de seguridad. La autenticación en un dominio se realizará en una url: `https://<dominio>.fastprg.com`


A continuación, se muestra un ejemplo de pantalla de autenticación.

Español (Argentina) ▼

Inicia sesión para acceder



[Olvidé mi contraseña](#) 

**INGRESAR**

Copyright 2023 FastPRG - Todos los derechos reservados

Powered by **FASTPRG**

Desde aquí en adelante, todos los ejemplos y pantallas siguen como ejemplo esta pantalla de autenticación.

El idioma de la página inicial será el mismo que el configurado en el navegador utilizado, pudiéndolo modificar el usuario desde la sección superior izquierda en la cual se visualizarán los idiomas disponibles. Si el idioma del navegador no se encuentra dentro de los idiomas disponibles de Neuralsoft, de manera predeterminada la pantalla de inicio se muestra en inglés. Tanto la lista de los idiomas disponibles de la página inicial, como la configuración regional de cada idioma serán definidas por Neuralsoft.

Para presentar la sección “Ingreso al sistema” se toman las definiciones de las siguientes políticas (detallas en la sección Políticas de Seguridad):

- **Permitir mantener sesión iniciada.**

- Tiempo de inactividad máximo para cierre automático de autenticación
- Métodos de autenticación adicionales
- Validación extra ante una autenticación en un nuevo dispositivo
- Notificación ante una autenticación en un nuevo dispositivo
- Métodos de restablecimiento de contraseña

Para la pantalla inicial se tomará lo que tenga definido cada política en el dominio.

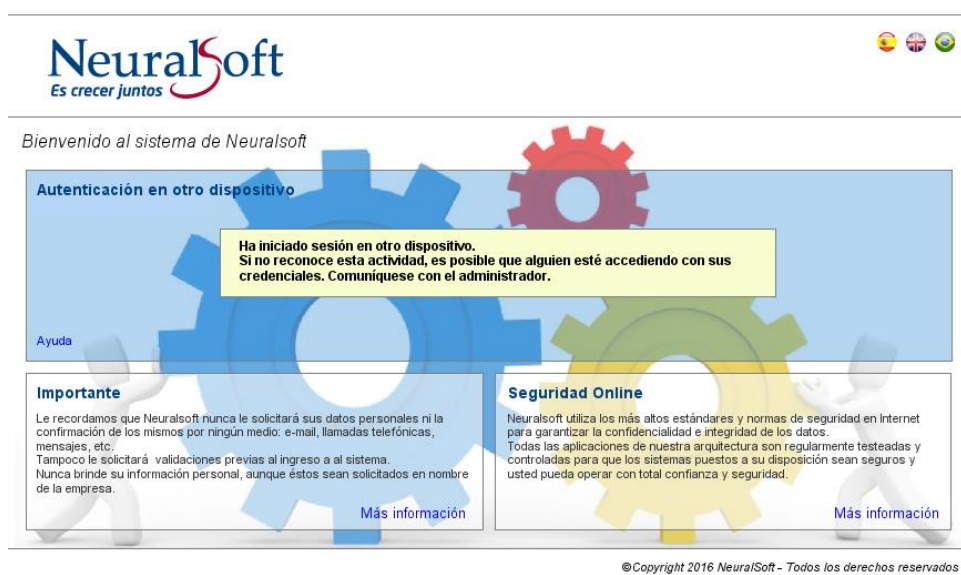
### *Permitir mantener sesión iniciada*

Si la política “Permitir mantener sesión iniciada” se encuentra habilitada, deberá aparecer el campo “Mantener sesión iniciada” en la pantalla y si el usuario lo tilda y se autentica correctamente, no deberá volver a ingresar sus credenciales en la próxima autenticación.

Mantener sesión iniciada ☒

Si el usuario selecciona esta opción y luego de un tiempo se cierra sesión por inactividad, al volver a ingresar al sistema, se auto-logueará, sin que el sistema le pida las credenciales.

En el caso de que el usuario conectado en un dispositivo A, se conecte en un nuevo dispositivo B correctamente, se cerrará la sesión del usuario en el dispositivo A (incluso si hubiese clickeado en “Mantener sesión iniciada” en A), comunicándose con el siguiente mensaje:



### *Tiempo de inactividad máximo para cierre automático de autenticación*

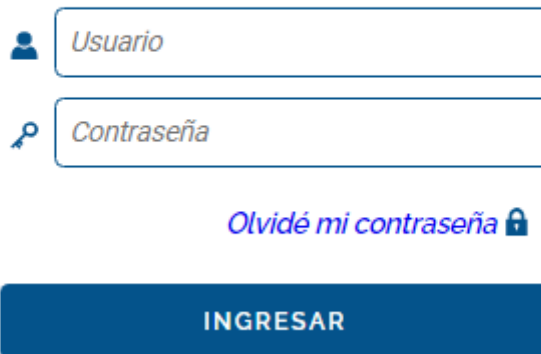
La política “Tiempo de inactividad máximo para cierre automático de autenticación” no modifica la estructura de la pantalla, pero al cumplirse el tiempo definido en esta política, se vuelve a cargar la pantalla inicial de autenticación, sin las credenciales ingresadas por el usuario (inclusive si el usuario ingresó algunas credenciales correctamente y luego se le pidieron métodos extras).

### *Métodos de autenticación adicionales*

Los “métodos de autenticación adicionales” definidos en el dominio se tienen en cuenta para la interfaz de la pantalla inicial. En la primera pantalla de autenticación siempre se visualizan los campos para ingresar usuario y contraseña:



## Inicia sesión para acceder



Usuario

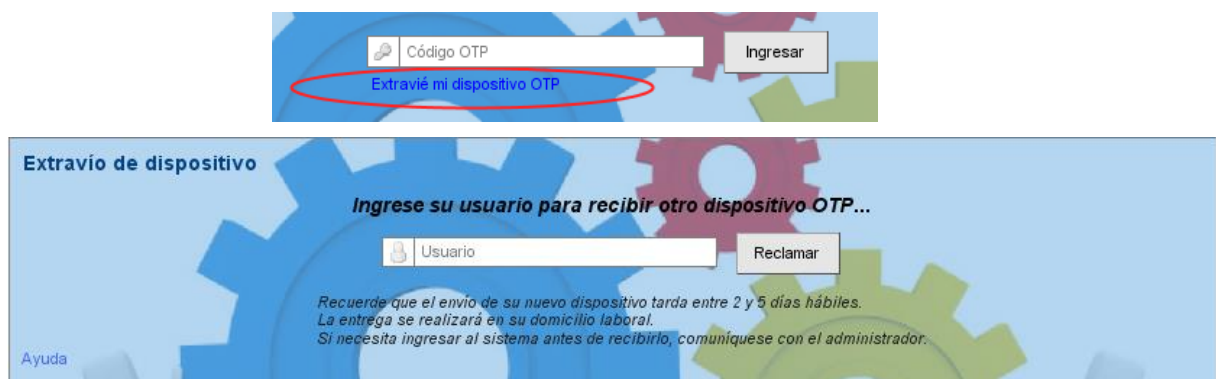
Contraseña

[Olvidé mi contraseña](#)

INGRESAR

Además, cuando el usuario se encuentre ingresando texto en mayúsculas, la pantalla indicará que la tecla “Bloq Mayús” está activa.

En el caso de seleccionarse un método que se asocie a una aplicación OTP, en la pantalla de autenticación, se presentará un link “Extravié mi dispositivo XXX” que al presionarlo, se presentará un formulario para solicitar un nuevo dispositivo.



Código OTP

Ingresar

[Extravié mi dispositivo OTP](#)

**Extravió de dispositivo**

**Ingrese su usuario para recibir otro dispositivo OTP...**

Usuario

Reclamar

Recuerde que el envío de su nuevo dispositivo tarda entre 2 y 5 días hábiles.  
La entrega se realizará en su domicilio laboral.  
Si necesita ingresar al sistema antes de recibirlo, comuníquese con el administrador.

Ayuda

Dentro de la política “Métodos de autenticación adicionales” se pueden definir más métodos en las OU y en los usuarios, por lo tanto, luego de que se ingresan las credenciales (usuario y contraseña) correctamente en la pantalla inicial, si el mismo tiene definido más métodos de autenticación, se presenta una segunda pantalla con el/los método/s correspondiente/s.

Si hay varios métodos de autenticación adicionales definidos para un usuario, este debe ingresar todos correctamente para autenticarse en la segunda pantalla, luego de ingresar correctamente la contraseña. Por ejemplo, si se solicitan código OTP, Telegram y email:

MyLogic

Español (Argentina)

Ingresar el código recibido

Código de aplicación autenticadora 13:08

Código enviado por EMAIL 17:51

Código enviado por TELEGRAM 17:49

ENVIAR

Powered by FASTPRG

Copyright 2022 FASTPRG - Todos los derechos reservados

### Aplicación OTP

Si el usuario aún no tiene una cuenta de Microsoft Authenticator asociada, luego de ingresar correctamente las credenciales, se presenta una pantalla que contiene:

- un QR para asociar la cuenta de Microsoft Authenticator
- un enlace en donde se visualiza el instructivo para asociar la cuenta
- en el caso de ingresar por un dispositivo móvil, se dará la opción de copiar un texto asociado al QR

Luego de asociar correctamente la cuenta de Microsoft Authenticator, el usuario siempre debe ingresar el código brindado por esta aplicación para poder ingresar. Es importante mencionar que por seguridad, un usuario NO puede desasociar su cuenta. Esto lo puede realizar únicamente un usuario con rol administrador de dominio mediante la opción “Restablecer credenciales” detallada en el punto [“Opción para restablecer credenciales \(sólo para administrador de dominio\)”](#) de este documento.

En el caso de que el usuario ingrese el código de manera incorrecta, se mostrará error indicando que el código es inválido y el campo para ingresar el código otp nuevamente. Si supera la cantidad de reintentos inválidos antes de bloquear cuenta definida como política, se bloqueará el usuario.

### Email

Luego de ingresar correctamente sus credenciales, si el usuario tiene configurado como método de autenticación adicional “email”, recibirá un email en su correo personal con un código de 6 dígitos, el cual deberá ingresar en una segunda pantalla de login para acceder finalmente al sistema.

El formato del email es el siguiente:

La pantalla de autenticación donde debe ingresar el código enviado por email es la siguiente:



04:59

INGRESAR

El código será válido por única vez, no pudiendo reutilizarse, y quedará sin efecto luego de 5 minutos. Esto se visualiza un contador en la pantalla. Pasado este tiempo, se visualizará la opción para 'Reenviar código'.



Reenviar código

INGRESAR

La cantidad de intentos permitidos para ingresar el código serán las definidas en la política de reintentos de acceso inválidos antes de bloquear cuenta. Luego de eso, se bloqueará el usuario de la misma manera que cuando ingresa mal sus credenciales. En este caso deberá esperar el tiempo definido para el desbloqueo e ingresar nuevamente las credenciales, luego se le reenviará un nuevo código. El bloqueo del usuario evento queda registrado en el log de seguridad.

### Telegram

Luego de ingresar correctamente sus credenciales, si el usuario tiene configurado como método de autenticación adicional "Telegram", recibirá un mensaje en su aplicación Telegram con un código de 6 dígitos, el cual deberá ingresar en una segunda pantalla de login para acceder finalmente al sistema.

El formato del mensaje es el siguiente:

La pantalla de autenticación donde debe ingresar el código enviado por Telegram es la siguiente:



04:59

INGRESAR

El código será válido por única vez, no pudiendo reutilizarse, y quedará sin efecto luego de 5 minutos. Esto se visualiza un contador en la pantalla. Pasado este tiempo, se visualizará la opción para 'Reenviar código'.

  
[Reenviar código](#)

## INGRESAR

La cantidad de intentos permitidos para ingresar el código serán las definidas en la política de reintentos de acceso inválidos antes de bloquear cuenta. Luego de eso, se bloqueará el usuario de la misma manera que cuando ingresa mal sus credenciales. En este caso deberá esperar el tiempo definido para el desbloqueo e ingresar nuevamente las credenciales, luego se le reenviará un nuevo código. El bloqueo del usuario evento queda registrado en el log de seguridad.

### Dispositivo Smart Card:



### Dispositivo llave USB



### Verificación biométrica

- Reconocimiento de voz
- Lectura de huella digital
- Reconocimiento facial
- Lectura de iris/retina

~~Sólo aparece un mensaje indicando lo que debe realizar el usuario.~~

### ~~Certificado digital: esta política no modifica la pantalla de login. El certificado digital se toma del navegador.~~

## Validación extra ante una autenticación en un nuevo dispositivo

Si hay algún método de validación extra ante una autenticación en un nuevo dispositivo, entonces debe verificarse primero la correcta autenticación del usuario con los métodos de autenticación definidos, y luego se evalúa si está queriendo ingresar desde un dispositivo en el cual el usuario no se haya autenticado anteriormente. De ser, así se procede a validar con el/los método/s definidos.

Se define autenticación en un nuevo dispositivo cuando el usuario accede desde un dispositivo diferente o incluso, desde otro navegador o una nueva pestaña de incógnito dentro del mismo dispositivo.

A continuación, se presentan los métodos de validación extra:

- Aplicación OTP  
Los detalles de la autenticación con método OTP se detallan en la sección "[Métodos de autenticación adicionales – Aplicación OTP](#)".
- Envío de email

Hemos detectado un inicio de sesión en un nuevo dispositivo. Para comprobar tu identidad ingresa el código de 6 dígitos enviado por email



04:59

INGRESAR

Hemos detectado un inicio de sesión en un nuevo dispositivo. Para comprobar tu identidad ingresa el código de 6 dígitos enviado por email



Reenviar código

INGRESAR

Los detalles de la autenticación con método Email se detallan en la sección “[Métodos de autenticación adicionales – Email](#)”.

- ~~Envío de SMS: al igual que el email, pero el código se envía por SMS al celular del usuario.~~
- Envío de mensaje mediante Telegram

Los detalles de la autenticación con método Telegram se detallan en la sección “[Métodos de autenticación adicionales –Telegram](#)”.

### ***Notificación ante una autenticación en un nuevo dispositivo.***

El objetivo de esta política es brindar mayor seguridad a los usuarios de la aplicación.

Si hay algún método de notificación ante una autenticación en un nuevo dispositivo, entonces debe verificarse primero la correcta autenticación del usuario con los métodos de autenticación definidos, y luego se evalúa si está queriendo ingresar desde un dispositivo en el cual el usuario no se haya autenticado anteriormente. De ser, así se procede enviar un e-mail para notificar tal situación.

La interfaz de la notificación por e-mail será la siguiente:



### Alerta de seguridad



Hola Matías Romero, hubo un inicio de sesión desde un nuevo navegador.

¿No fuiste vos? Por favor, bloqueá el dispositivo e informá de inmediato al administrador de seguridad.

- 24/02/2024 21:48 hs - Ubicación: Zárate, Buenos Aires, Argentina
- 23/02/2024 09:32 hs - Ubicación: Rosario, Santa Fe, Argentina
- 21/02/2024 08:55 hs - Ubicación: Rosario, Santa Fe, Argentina

Gracias por elegimos, Equipo de Fastprg  
[www.fastprg.com](http://www.fastprg.com)

La notificación que se recibe contiene la lista de los últimos 3 dispositivos utilizados recientemente con su estado (habilitado, bloqueado). Desde dicha lista se podrá bloquear los dispositivos y habilitarlos. Bloquear un dispositivo implica inhabilitar el acceso del usuario en ese dispositivo y si hay un usuario autenticado, cerrar su sesión.

### Métodos de restablecimiento de contraseña

Si hay al menos un método de restablecimiento de contraseña definido, entonces en la pantalla inicial se presentará un link para poder realizarlo según el método configurado.

Inicia sesión para acceder al sistema

Usuario

Contraseña

[Olvidé mi contraseña](#)

Si el usuario hace click en “olvide mi contraseña”, se visualiza una segunda pantalla solicitando nombre usuario o email y un botón para proceder con el restablecimiento.

En unos segundos recibirá un correo, por favor siga las instrucciones

Es importante aclarar que se tienen en cuenta todos los métodos configurados en las políticas 'Métodos de restablecimiento de contraseña' más los configurados en 'Métodos de autenticación adicionales'.

Por ejemplo, si un usuario tiene como método de autenticación adicional OTP y método de recuperación de contraseña Email, al restablecer su contraseña se enviará un link a su correo electrónico, y al ingresar al mismo se deberá ingresar el código OTP para poder restablecer contraseña correctamente.

Si se utiliza la funcionalidad de reestablecer contraseña por Telegram, se procederá al envío de un link dentro de un mensaje de Telegram al número de celular del usuario.

Si en la política se marcan los 2 métodos, le llegará el mismo link por los 2 medios.


El link será válido por única vez, no pudiendo reutilizarse, y quedará sin efecto al cumplirse la fecha de vencimiento del mismo. Además, existirá un límite de cantidad de veces que un usuario podrá solicitar restablecer la contraseña por día (inicialmente 3) y por semana (inicialmente 5). Por último, también existirá un número máximo de cantidad de solicitudes por IP por día, por semana y por hora (faltan definir los valores iniciales de estos 3 números).



Si un usuario se encuentra logueado en el momento en que solicita restablecer la contraseña, se abrirá la actividad para cambiar la misma y luego de confirmar se cerrará la sesión de dicho usuario para que pueda ingresar con su nueva contraseña.

## Cambio de contraseña

Usuario

 Genesis Carrasquero

Contraseña actual \*

Nueva contraseña \*


Repetir contraseña \*


Cambiar contraseña


Si luego de solicitar restablecimiento de contraseña, el usuario intenta iniciar sesión se le informará el mensaje de “usuario o contraseña inválida”.

Al ingresar al enlace enviado por e-mail, o Telegram, se podrá restablecer la contraseña como se muestra a continuación:

## Enter a new password

 saguilera

 Password

 Repeat Password

CHANGE PASSWORD

Aclaración: aunque el usuario tenga la posibilidad de recordar la contraseña, en el restablecimiento de la misma, no se le dará esa posibilidad.

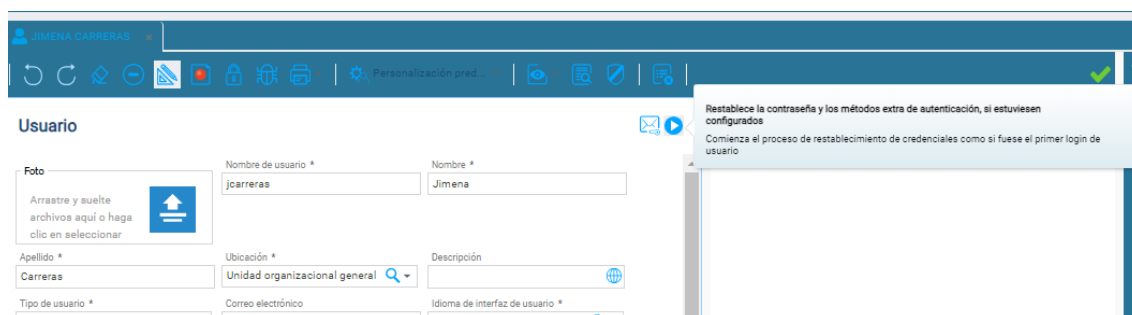


Las pantallas de ingreso anteriores serán las predefinidas, pero desde el Dominio se podrán modificar el logo de la empresa, el tema elegido para la pantalla de autenticación, la imagen para fondo o marca de agua, texto, etc.

Es importante aclarar que si se define un método de restablecimiento, éste se sumará a los métodos de autenticación adicionales definidos para el usuario. Por ejemplo, si en los métodos de autenticación adicionales se configura OTP y el método de recuperación de contraseña es Email, se deberán ingresar correctamente ambos códigos para poder restablecer la contraseña. Si en ambas políticas está definido el mismo método, ejemplo email, sólo se solicitará una vez.

### ***Opción para restablecer credenciales (sólo para administrador de dominio)***

Los usuarios que tengan el rol 'Administrador de dominio' pueden restablecer las credenciales de cada usuario mediante un botón en la edición del usuario:



Este botón se utiliza para restablecer las credenciales de todos los métodos de autenticación definidos para un usuario. ~~Al presionar el botón, se le cerrará la sesión al usuario (si el mismo está autenticado) y no podrá volver a autenticarse si no ingresa correctamente sus credenciales.~~

Es decir, si el usuario tiene como métodos de autenticación contraseña y OTP, dejará sin validez la contraseña y la asociación con la aplicación OTP. En este caso, le llegará un email al usuario (similar al que le llega en la primera autenticación para ingresar la contraseña por primera vez), y luego de restablecer su contraseña, podrá asociar la cuenta OTP mediante un QR que se muestra en la segunda pantalla de login (al igual que la primera vez que asocia la cuenta OTP con el usuario).

Con respecto al Registro de eventos, cada vez que se restablezcan las credenciales se registrará en el Registro de Seguridad, por ejemplo:

← Registro de seguridad

Mensaje

↺ ↻ B / ↗

genesole ha indicando restablecer contraseña de sluciani

Categoría de registro

Contraseña

Código de evento de registro

Restablecer contraseña exitosa

Comando de registro

Restaurar contraseña

Usuario

Genesis Sole

Sitio

Rosario

Nivel de registro

Informativo

Tipo de origen de registro

Restaurar contraseña

Entidad

Entidad directa

Dominio

ittestbase-master

Navegador

Fecha hora de actualiz...

20/02/2024 09:30

### **Mensajes de error relacionados al ingreso de contraseña:**

La contraseña debe contener al menos  $\{MINIMUM\_PASSWORD\_LENGH\}$  caracteres.  
(Definido en las políticas de cada dominio)

La contraseña debe contener al menos 3 de las siguientes características:

- Una letra mayúscula
- Una letra minúscula
- Un número
- Un caracter especial

La contraseña no puede contener parte del nombre de usuario.

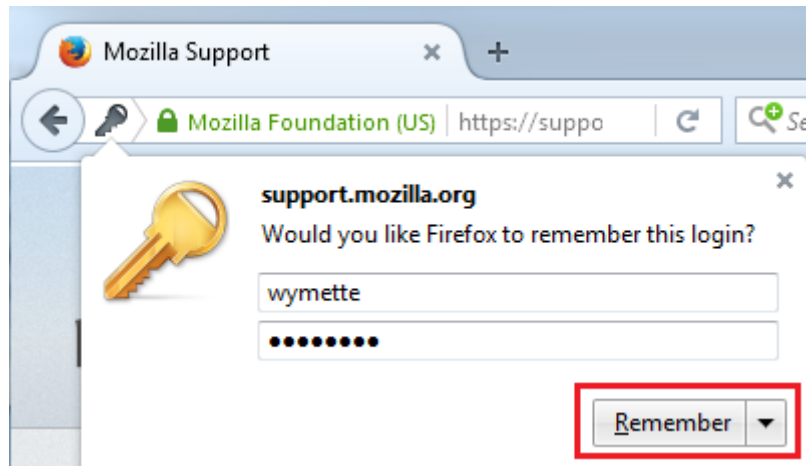
La contraseña nueva es igual a la anterior. (En este punto se define en las políticas de dominio en la cantidad de contraseñas anteriores inutilizables)

No posee permisos para cambiar la contraseña.

La contraseña actual es incorrecta. (Luego de la cantidad de intentos que definan para cada dominio el usuario quedará bloqueado por la cantidad de minutos establecido en las políticas)

### **Recordar contraseña**

Los navegadores web cuentan con la funcionalidad para guardar nombres de usuarios y contraseñas para evitar que los usuarios deban ingresar sus credenciales cada vez que ingresan al sistema, por ejemplo, Firefox mostrará la siguiente ventana:



Además, si la contraseña cambia, el navegador también permitirá actualizar la que se encuentra guardada en el mismo.

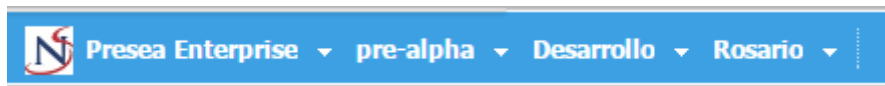
Esta opción también se podrá inhabilitar desde el mismo navegador, así como también, borrar las contraseñas guardadas.

### 7.3 Autenticación en un Modelo

La interfaz de ingreso al sistema dependerá del modelo. La autenticación en un modelo se realizará en una url: <dominio>.fastprg.com/<identificadorWebModelo>

Independientemente de si el usuario se autenticó alguna vez, accederá siempre al modelo que figura en la url. Si por algún motivo hubiese un error (por ejemplo, el usuario no posee permisos de acceso al modelo), se mostrará en la pantalla de login el mensaje “No tiene permitido el acceso a este modelo”.

De todas formas, aunque el login se haya realizado en un modelo específico podrá acceder a los demás modelos en donde el usuario posee permisos desde la barra de títulos:



### 7.4 Personalización visual en pantallas de autenticación

Dentro de la pantalla de login hay 2 secciones:

- Sección superior: contiene datos del dominio/modelo:



Se puede personalizar logo, agregar textos, cambiar tema de colores, agregar imagen de fondo, mover campos, agregar iconos con links (por ejemplo, para acceder a Facebook), no se puede eliminar el campo de idiomas.

- Sección inferior: contiene datos del login configurado en el dominio:

Ingreso al sistema

Usuario

Contraseña

[Olvidé mi contraseña](#)

INGRESAR

☒ Mantener mi sesión abierta

Se puede agregar textos, cambiar tema de colores, agregar imagen de fondo, mover campos de login pero no eliminarlos ni agregar nuevos.

## 7.5 Autenticación para usuarios externos

En la página de autenticación de un dominio de manera predeterminada se cargarán los métodos de autenticación definidos en el dominio de la url a la que se accedió, pero se contemplará el acceso de usuarios externos al dominio, previo vínculo de seguridad establecido.

Cuando un usuario externo desea ingresar a un dominio, deberá incluir el dominio local en sus credenciales. Esto se realizará dentro del campo usuario, con un símbolo particular: \ o @.

Cuando el usuario termine de ingresar dominio (no hace falta que haya salido del campo usuario, a medida que va escribiendo se va detectando el dominio), primero se validará que el dominio sea uno de los Dominios de autenticación y luego, que el usuario sea uno de los objetos externos que pueden acceder. Si esto es válido, se mostrarán en pantalla los métodos de autenticación del dominio externo, ya que el usuario deberá ingresar las credenciales que posee en dicho dominio.

**Métodos de autenticación definidos en el dominio LOCAL**

domainCC\us|

Contraseña

[Olvidé mi contraseña](#)

Ingresar

☐ Mantener sesión iniciada

**Métodos de autenticación definidos en el dominio EXTERNO**

domainCC\userCC

12|

[Extravié mi dispositivo OTP](#)

Ingresar

## 7.6 Proceso de autenticación

El usuario debe aportar las credenciales que lo identifican y permiten verificar la autenticidad de la identificación, y el sistema debe validar si las credenciales aportadas son suficientes para dar acceso al usuario o no. Este proceso comúnmente se denomina *login* o *logon*.

En el caso de no realizar una correcta autenticación debido a que se ingresa mal el nombre de usuario o la clave, se le notificará al usuario mediante un mensaje, y el mismo deberá ingresar de nuevo el usuario y clave para poder autenticarse:



La imagen muestra la interfaz de inicio de sesión con el título "Ingreso al sistema". Un mensaje de error en un recuadro amarillo indica: "El nombre de usuario y/o la clave no son correctos. Vuelva a ingresarlos.". Debajo del mensaje hay un campo de texto etiquetado "Usuario" con un ícono de persona a la izquierda, y un enlace "Olvidé mi usuario" en azul.

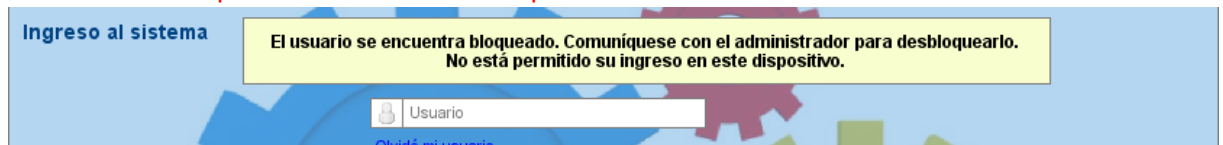
En el caso de realizar una correcta autenticación pero que el usuario no cumpla una o varias políticas de seguridad para autenticarse, se le mostrará un mensaje con el motivo o los motivos por los cuales no puede ingresar al sistema, por ejemplo:

- Si no cumple con el rango horario permitido:



La imagen muestra la interfaz de inicio de sesión con el título "Ingreso al sistema". Un mensaje de error en un recuadro amarillo indica: "No está permitido su ingreso en este horario. Vuelva a intentarlo más tarde.". Debajo del mensaje hay un campo de texto etiquetado "Usuario" con un ícono de persona a la izquierda, y un enlace "Olvidé mi usuario" en azul.

- Si su usuario está bloqueado y además la IP del dispositivo donde intenta ingresar el usuario no corresponde a las direcciones IP permitidas:



La imagen muestra la interfaz de inicio de sesión con el título "Ingreso al sistema". Un mensaje de error en un recuadro amarillo indica: "El usuario se encuentra bloqueado. Comuníquese con el administrador para desbloquearlo. No está permitido su ingreso en este dispositivo.". Debajo del mensaje hay un campo de texto etiquetado "Usuario" con un ícono de persona a la izquierda, y un enlace "Olvidé mi usuario" en azul.

En el caso de que un usuario ingrese la clave incorrectamente la cantidad de veces que indique la política "Reintentos de acceso fallidos consecutivos antes de bloquear cuenta", la cuenta de dicho usuario quedará bloqueada por el tiempo que indique la política "Tiempo de bloqueo de cuenta ante accesos fallidos consecutivos".

En el caso de que ocurra una situación inesperada en el login (ejemplos: conexión muy lenta, servidor muy cargado, etc.), se presentará al usuario el siguiente mensaje "El ingreso está demorando más de lo habitual".

En el cierre de sesión de un usuario, se mostrará la página de login y si el cierre de sesión ocurrió de manera inesperada, se mostrará el mensaje correspondiente, por ejemplo "No está permitido su acceso en este horario".

## 7.7 Ingreso al sistema

Si el usuario tiene activa la política "Forzar cambio de contraseña en el próximo acceso", luego de autenticarse correctamente, visualizará la siguiente pantalla y no podrá ingresar a ninguna aplicación hasta confirmar una contraseña nueva y válida:



La imagen muestra la interfaz de modificación de contraseña con el título "Modificar contraseña". Hay tres campos de texto con íconos de llave: "Contraseña actual", "Nueva contraseña" y "Confirmar nueva contraseña". A la derecha de estos campos hay un botón "Ingresar". En la esquina inferior izquierda hay un enlace "Ayuda".

Luego de que el usuario se autentique correctamente, el idioma será el que tenga como "idioma preferido" dicho usuario en sus preferencias.

## Preferencias de Usuario

Si es la primera autenticación del usuario, se deberá evaluar la política “Forzar carga de datos personales en primer acceso”. Si la política está activa para el usuario autenticado, el mismo visualizará sus preferencias de usuario, y deberá completar los campos obligatorios:

Preferencias de usuario ✕

Usuario (\*)

geena.mcpherson


Nombre (\*)

Geena


Apellido (\*)

McPherson

Foto



Contraseña (\*)

\*\*\*\*\* 


E-mail (\*)

geena.mcpherson@dominio.com

Teléfono celular

155555555

Domicilio

San Martín 444 

Localidad/Estado/Provincia

Rosario ▾

Código Postal

2000

País

Argentina ▾

Preferencias del sistema

Tema preferido (\*)

Estándar ▾



Idioma preferido (\*)

Español (Argentina) ▾

Interfases preferidas para acceso a modelos:

[-] Modelo:

CRM XP ▾

Interfaz preferida

Web ▾

Se hereda de la OU

Excepciones  
(modelos que el usuario  
desea ver en otra interfaz  
distinta de la predeterminada  
del modelo)

Las Preferencias de Usuario se componen de una primera sección con los datos personales del mismo, y una segunda sección para los datos correspondientes a sus preferencias en cuanto al sistema. Esta pantalla tiene en cuenta la seguridad del usuario.

Los datos personales son:

- Usuario: no editable por el usuario.
- Nombre.
- Apellido.
- Foto.
- Contraseña.
- E-mail.
- Teléfono celular.
- Domicilio.
- Código postal.
- Ciudad.
- Localidad/estado/provincia.
- País.

Las preferencias del sistema son:

- Tema preferido: el usuario debe elegir uno de los temas visuales sobre los temas que tiene permiso. De manera predeterminada, se hereda el tema del dominio. Al costado de la lista de selección para el tema, se presenta un botón para personalizar dicho tema. Esta personalización sólo la podrá realizar el usuario autenticado y aplicará para dicho usuario solamente, de acuerdo a lo establecido en el documento Editor de Temas.
- Idioma preferido de UI: indica el idioma en el que el usuario accede a todos los modelos. Si lo cambia, automáticamente se cambiará el idioma en el que se encuentra usando el modelo actualmente.
- Idioma de datos preferido: indica el idioma de datos en el que el usuario accede a todos los modelos. Si lo cambia, NO se cambiará el idioma de datos en el que se encuentra usando el modelo actualmente.

## Página de Inicio

La primera vez que un usuario se autentica en un dominio, se conecta a alguna aplicación en donde posea permiso de acceso en el ambiente producción, en algún sitio en el cual tenga permiso de acceso, el idioma predeterminado y con el tema predeterminado. En este momento se validará que dicho usuario posea los permisos necesarios para ejecutar la aplicación.

Si el usuario no tiene permisos en el ambiente de producción, se intentará loguear al mismo en el ambiente de testing y si no tiene permisos en este ambiente, en el de desarrollo. Si no tiene permisos en desarrollo, se informará mediante un usuario al usuario y quedará registrado en el Log de Seguridad.

Es importante aclarar que para que un usuario acceda efectivamente a un modelo y a un ambiente, debe tener estos 2 permisos (ambos permitidos):

- Permiso de acceso a un modelo (este permiso se configura por ambiente).
- Permiso de acceso a un ambiente de un modelo.

En el primer login del usuario en un modelo, se usa el idioma preferido del usuario.



Cada vez que se autentica el usuario, el idioma en el que acceda será el idioma preferido del usuario.

Es importante aclarar que las preferencias de usuario son distintas en cada dominio, es decir, si el usuario accede a un modelo de un Dominio de autenticación, tendrá otras preferencias.

Luego de su primera autenticación, siempre se le presentará la pantalla tal como la dejó la última vez que la estaba utilizando. En el caso de que no se pueda presentar la última pantalla (cambio de permisos en el usuario, eliminación de un modelo, etc.), el usuario verá nuevamente la pantalla inicial como si fuera su primer login.

Además siempre se evaluará si el mismo tiene licencia para utilizar dicha aplicación en dicho ambiente. De no ser así, se le informará que no tiene acceso por falta de licencias.



Tal como se detalla en Estándares UI, luego de que el usuario se autentique podrá visualizar y cambiar desde la barra de título: el modelo, la versión, el ambiente y el sitio. En el caso de que el usuario no posea permisos de ingresar a otro modelo, versión, ambiente o sitio, no se visualizará la flecha para desplegar el combo y cambiar lo seleccionado.

~~Dentro de la lista de los modelos se encuentran:~~

- ~~• Editor de Dominio: sirve para administrar las definiciones del dominio, de sus usuarios, grupos, sitios, políticas de seguridad, los vínculos de seguridad con otros dominios, etc.~~
- ~~• Administrador de Modelos: sirve para administrar los diferentes modelos, la herencia entre los mismos, etc.~~
- ~~• Editor de Market Place: sirve para administrar el Market Place, los modelos que se publican en él, el costo de las licencias, las formas de pago, etc.~~
- ~~• Etc.~~

## 8 Elementos del modelo

Cada componente que pertenezca a un *elemento*, heredará todas sus propiedades (*permisos* y *denegaciones*). Pero podrán definirse más *permisos* y *denegaciones* para ese componente en particular. Por ejemplo, los atributos de una entidad heredarán sus permisos y denegaciones.

Para cada elemento y para instancia de un elemento existirá una *Lista de Control de Acceso (ACL)* que estará compuesta por una lista de acciones que pueden ser aplicadas/ejecutadas sobre el mismo, además de los usuarios y/o grupos de usuarios con sus permisos y denegaciones sobre dicho elemento/instancia.

Los permisos específicos en cada *elemento* se definirán en el editor correspondiente, así como la creación y eliminación de los mismos y las ACL correspondientes. De la misma forma se procederá con las instancias de un elemento.

Por cada entidad, existirá una lista de operaciones permitidas y orígenes de operaciones permitidas, de acuerdo a lo establecido en el documento [Estándares de interfaz de usuario](#). Por ejemplo:



Entidad (Acción comercial)

Seguridad de instancias

Seguridad de instancias condicional

Modelado de seguridad

Grupo de usuarios

Permisos globales

Permisos por ambiente

Permiso	Todos los ambie...	
	Permitir	Denegar
Administrar instancia	<input type="checkbox"/>	<input type="checkbox"/>
Crear instancia	<input type="checkbox"/>	<input type="checkbox"/>
Creación directa	<input type="checkbox"/>	<input type="checkbox"/>
Desencadenante	<input type="checkbox"/>	<input type="checkbox"/>
Transformación	<input type="checkbox"/>	<input type="checkbox"/>
Regla de negocio	<input type="checkbox"/>	<input type="checkbox"/>
Vista de información	<input type="checkbox"/>	<input type="checkbox"/>
Importación	<input type="checkbox"/>	<input type="checkbox"/>
Consultar instancia	<input type="checkbox"/>	<input type="checkbox"/>
Actualizar instancia	<input type="checkbox"/>	<input type="checkbox"/>

## 9 Permisos efectivos

A partir de un usuario o grupo de usuarios dado existirá una visualización avanzada de los “*permisos efectivos*”.

Los permisos efectivos de un usuario son el resultado de la sumatoria de los permisos definidos en todo el sistema para ese usuario y todos los grupos a los que pertenece (directa o indirectamente).

Los permisos efectivos de un usuario sobre un elemento serán los resultantes de la sumatoria entre los permisos definidos en la seguridad del Dominio y en la seguridad del elemento. Por ejemplo, si un usuario tiene permiso de modificación de las Entidades en la seguridad del Dominio (sección Diccionario de Datos), pero se encuentra en un grupo que tiene denegado la modificación de la entidad “Factura”, dicho usuario podrá modificar todas las entidades, menos “Factura”.

Si un usuario no tiene permiso definido para modificar entidades, pero tiene permisos para modificar la entidad “Cliente”, el resultado será que sólo podrá modificar la entidad “Cliente”. Si un usuario tiene el permiso denegado para modificar entidades y tiene permisos para modificar la entidad “Cliente”, el resultado será que no podrá modificar ninguna entidad. Lo mismo aplicará para todos los elementos.

Además, y sólo para las entidades, se podrán evaluar los permisos efectivos sobre las instancias. En esta evaluación, se tendrán en cuenta las solapas “Seguridad de instancias” y “Seguridad” de los Atributos, pertenecientes al Editor de Entidades. En la mayoría de los casos,

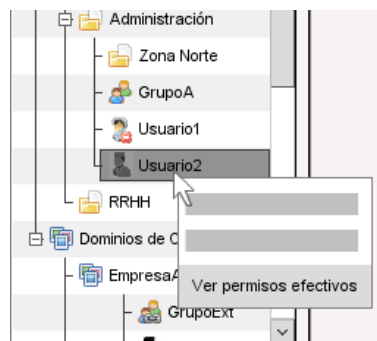
la evaluación se efectuará en los sistemas generados, pudiendo también efectuarse en los editores en algunos casos particulares, por ejemplo, en una grilla de entidades en el GDI.

Los permisos particulares se definirán sobre las instancias de los elementos teniendo en cuenta los ambientes. Por ejemplo, en la solapa “Seguridad de instancias” de la entidad “Factura” se administrarán los permisos de acceso a la misma.

Estos permisos podrán consultarse de manera centralizada desde la opción de “*Permisos efectivos*”. El resultado de esta consulta será la sumatoria de los permisos y denegaciones. Dicho resultado deberá visualizarse agrupado en solapas, por elemento del modelo (Diccionario de Datos, Funciones, etc). Las ACL de cada solapa podrán agruparse por acción, por ambiente o por instancia. **Los permisos delegados se visualizarán de manera diferente que los permisos explícitos.**

Para que un usuario pueda acceder a la visualización de permisos efectivos, deberá tener permisos de consulta de usuarios.

*Aclaración:* esta consulta no incluye las Actividades Delegadas.



Permisos efectivos Usuario2		
Diccionario de Datos    Funciones    Procesos de negocio    Reglas de negocio    Componentes de negocio    Plantillas    Sistemas finales    Herramientas		
Permiso	Permitir	Denegar
▼ Entidades		
Crear	<input type="checkbox"/>	<input type="checkbox"/>
Consultar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modificar	<input type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>
Traducir	<input type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input type="checkbox"/>	<input type="checkbox"/>
▼ Instancias de entidades		
▼ Cliente		
▼ Ambiente: Desarrollo		
▼ Todas las instancias		
Crear	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Consultar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modificar	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Eliminar	<input type="checkbox"/>	<input type="checkbox"/>
Traducir	<input type="checkbox"/>	<input type="checkbox"/>
Administrar permisos	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▼ Cliente.Provincia = "Santa Fe"		
Crear	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Consultar	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modificar	<input type="checkbox"/>	<input type="checkbox"/>

El formato general es:

- ✓ *Elemento* (hará referencia al modelo)
  - Acciones (crear/consultar/modificar/eliminar/traducir/administrar permisos)

✓ *Instancias de elemento*

- Instancia 1
  - Ambiente: Desarrollo
    - Todas las instancias
      - Crear
      - Consultar
      - Modificar
      - Eliminar
      - Restaurar
      - Traducir
      - Administrar permisos
    - Condición 1
      - Crear
      - Consultar
      - Modificar
      - Eliminar
      - Restaurar
      - Traducir
      - Administrar permisos
    - Condición n
      - Crear
      - Consultar
      - Modificar
      - Eliminar
      - Restaurar
      - Traducir
      - Administrar permisos
  - Ambiente: Testing (ídem a “Desarrollo”)
  - Ambiente: Producción (ídem a “Desarrollo”)
- Instancia 2 (ídem a “Instancia 1”)
- Instancia n (ídem a “Instancia 1”)

Los apartados que no incluyan elementos del modelo, no tendrán instancias; por lo tanto, la ACL se mostrará de la siguiente manera:

✓ *Sección:*

- Acción 1
- Acción 2
- Acción n

Por ejemplo:

✓ *Supervisión:*

- Permisos para tomar sesión
- Invitar a toma de sesión
- Monitorizar
- Iniciar coaching
- Permisos para que le tomen sesión
- Permisos para que lo monitoricen
- Administrar permisos.

## 10 Romper herencia

Se podrá romper la herencia de la seguridad definida en otros niveles. Esto significará que sólo se evaluará la seguridad definida en el elemento que estoy posicionado.

Por ejemplo:

1. Existe un grupo de usuarios con permisos de ejecutar todas las reglas de negocios del modelo, pero se requiere que una regla particular no la puedan ejecutar. En ese caso se accederá a esta regla particular, se indicará con el checkbox que rompe herencia (ya no heredará los permisos definidos a nivel de modelo) y se definirá la seguridad para esa regla particular.
2. Existe un atributo particular en una entidad que sólo debe ser visto por el administrador del modelo. Sin embargo, el resto de los atributos pueden ser vistos y editados por todos los editores. En ese caso se accederá a este atributo particular, se indicará con el checkbox que rompe herencia y se definirá la seguridad para ese atributo particular.

Es importante aclarar, en este caso, que la herencia de la instancia al atributo se rompió. Esto significa que nadie verá ese atributo a no ser que especifique lo contrario.

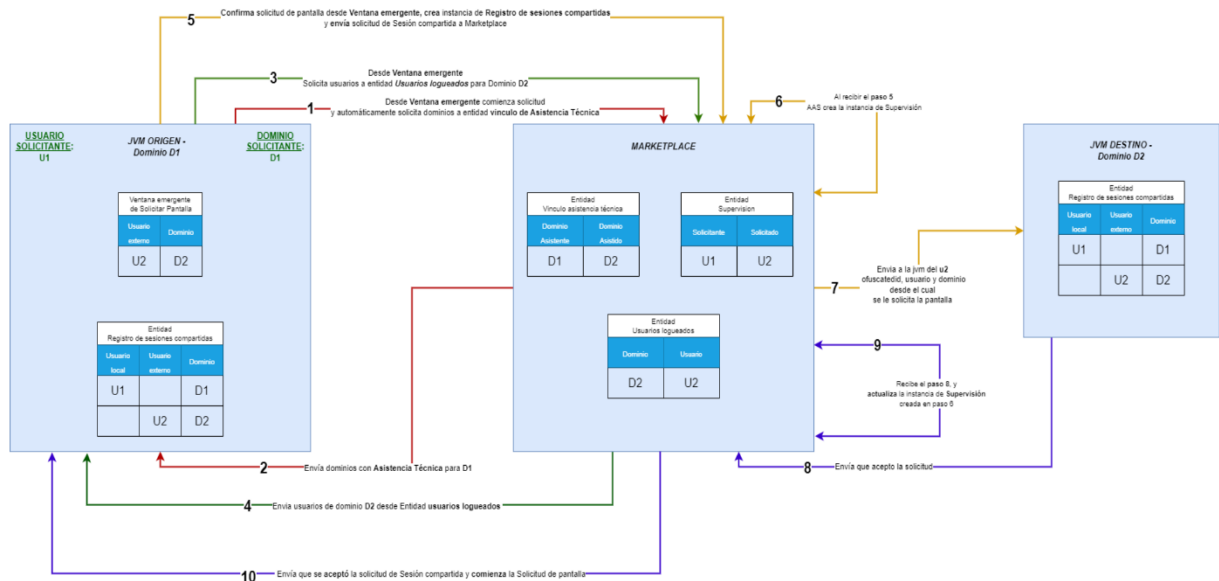
Se podrá romper herencia en los todos los elementos del modelo (aunque sea en una primera instancia), por ejemplo:

- Actividad
- Actor
- Ambiente
- Conexión
- Dispositivo
- Entidad
- Función
- GDI
- Hallazgo
- Indicador
- Mapa estratégico
- Modelo
- Objetivo
- Organigrama
- Perspectiva
- Plan de integración
- Planificación
- Proceso de negocio
- Regla de negocio
- Reporte por bandas
- Tarea de integración
- Tarea programada
- Tipo de atributo
- Unidad de desarrollo
- Versión
- Web services

- Atributo
- Instancia
- Empresa
- Sitio

## 11 Solicitar pantalla

La funcionalidad *Solicitar pantalla* se encarga de permitir a un usuario pedir control sobre la sesión de otro. Esta funcionalidad es iniciada por el usuario que desea tomar la sesión y siempre deberá ser confirmada por el usuario que está otorgando su sesión. Cualquiera de los



dos usuarios participantes, puede finalizar la acción. Para que un usuario pueda realizar esta operación, necesita los permisos de seguridad correspondientes que se mencionan en [esta sección](#) del presente documento.

A continuación, se dejan todos los links a los documentos en los que se describe cada entidad que interviene en el proceso.

- [Marketplace:](#)
  - Vinculo de asistencia técnica.
  - Supervisión.
  - Usuarios logueados.
- [Registro de sesiones compartidas.](#)
- [Ventana emergente de solicitar pantalla.](#)

## 12 Compartir pantalla

## 13 Anexo:

### 13.1 Buenas prácticas de seguridad

En esta sección se detallan recomendaciones a la hora de configurar la seguridad de un dominio:

- ✓ Dar permisos y denegaciones por grupo.
- ✓ Si se desea usar un grupo de servicios web en una RN y luego copiar la RN en modelos hijos (o vinculados), pero que no se copie información privada del usuario, se debe crear una entidad paramétrica para los parámetros necesarios y poner que no se copie en los hijos esos valores. El caso de uso más común es los ISV con WS que tengan password, donde la instancia contiene cuenta de usuario y password para el WS. Entonces, en el parámetro de WS pueden ponerse expresiones como, “En Paramétrica buscar Contraseña AFIP” o “En Paramétrica buscar CUIT”, teniendo en cuenta que estos valores de la instancia deben ser completados en el modelo nuevo.

### 13.2 Configuración regional por Idioma

En esta sección se detallan las configuraciones regionales definidas para los nuevos idiomas que se van incorporando en fastprg.

- ✓ **Idioma: Hebreo.**

Primer día de la semana	Domingo
Primera semana del año	Primera semana del año
Separador decimal	Punto
Separador de lista	Punto y coma
Separador de miles (Separador de agrupación de dígitos)	Coma
Formato de Fecha – Por defecto	Corto
Formato de Fecha – Corto	dd/MM/yy
Formato de Fecha – Medio	dd/MMMM/yyyy
Formato de Fecha – Largo	dddd dd MMMM yyyy
Formato de Fecha – Completo	dddd dd 'ב' MMMM yyyy
Formato de Hora - Por defecto	Corto
Formato de Hora - Corto	HH:mm
Formato de Hora - Medio	hh:mm tt
Formato de Hora – Largo	HH:mm:ss
Formato de Hora -	hh:mm:ss tt

Completo	
Formato Fecha y Hora - Por defecto	Corto
Formato Fecha y Hora - Corto	dd/MM/yy HH:mm
Formato Fecha y Hora - Medio	dd/MMMM/yyyy hh:mm tt
Formato Fecha y Hora - Largo	dddd dd MMMM yyyy HH:mm:ss
Formato Fecha y Hora - Completo	dddd dd 'ב' MMMM yyyy hh:mm:ss tt

### Ejemplos:

Fecha corta: 20/11/2018  
 Fecha larga: יום שלישי 20 נובמבר 2018  
 Fecha Media: 2018/נובמבר/20  
 Fecha Completa: יום שלישי 20 בנובמבר 2018

### ✓ Idioma: Japonés.

Primer día de la semana	Lunes
Primera semana del año	Primera semana del año
Separador decimal	Punto
Separador de lista (windows tiene Coma)	Punto y coma
Separador de miles (Separador de agrupación de dígitos)	Coma
Formato de Fecha – Por defecto	Medio
Formato de Fecha – Corto	yy/MM/dd
Formato de Fecha – Medio	yyyy/MM/dd
Formato de Fecha – Largo	yyyy年MM月dd日
Formato de Fecha – Completo	Yyyy 年MMM月d 日dddd
Formato de Hora - Por defecto	Corto
Formato de Hora - Corto	H:mm
Formato de Hora - Medio	HH:mm
Formato de Hora – Largo	HH:mm:ss
Formato de Hora – Completo (equivale a: tt hh:mm:ss)	午前 hh:mm:ss (am) 午後hh:mm:ss (pm)
Formato Fecha y Hora - Por defecto	Corto

Formato Fecha y Hora - Corto	yy/MM/dd H:mm
Formato Fecha y Hora - Medio	yy/MM/dd HH:mm
Formato Fecha y Hora - Largo	yyyy年MM月dd日 HH:mm:ss
Formato Fecha y Hora - Completo	Yyyy 年MMM月d日 dddd午前hh:mm:ss

### Ejemplos:

Fecha larga: 2018年11月20日

Fecha completa: 2018年11月20日 火曜日

### ✓ Idioma: Portugués

Primer día de la semana	Domingo
Primera semana del año	Primera semana del año
Separador decimal	Coma
Separador de lista	Punto y coma
Separador de miles (Separador de agrupación de dígitos)	Punto
Formato de Fecha – Por defecto	Corto
Formato de Fecha – Corto	dd/MM/yy
Formato de Fecha – Medio	dd/MM/yyyy
Formato de Fecha – Largo	D' de 'MMMM' de 'yyyy
Formato de Fecha – Completo	Dddd, d' de 'MMMM' de 'yyyy
Formato de Hora - Por defecto	Corto
Formato de Hora - Corto	HH:mm
Formato de Hora - Medio	HH:mm
Formato de Hora – Largo	HH:mm:ss
Formato de Hora - Completo	HH:mm:ss
Formato Fecha y Hora - Por defecto	Corto
Formato Fecha y Hora - Corto	dd/MM/yy HH:mm
Formato Fecha y Hora - Medio	dd/MM/yyyy HH:mm
Formato Fecha y Hora - Largo	D' de 'MMMM' de 'yyyy HH:mm:ss
Formato Fecha y Hora - Completo	Dddd, d' de 'MMMM' de 'yyyy HH:mm:ss

### Ejemplos:

Fecha corta: 22/11/18

Fecha larga: 22 de novembro de 2018



Fecha media: 22/11/2018  
Fecha completa: quinta-feira, 22 de novembro de 2018

✓ **Idioma: Portugués (Brasil).**

Primer día de la semana	Domingo
Primera semana del año	Primera semana del año
Separador decimal	Coma
Separador de lista	Punto y coma
Separador de miles (Separador de agrupación de dígitos)	Punto
Formato de Fecha – Por defecto	Medio
Formato de Fecha – Corto	dd/MM/yy
Formato de Fecha – Medio	dd/MM/yyyy
Formato de Fecha – Largo	D´de ´MMMM´de ´yyyy
Formato de Fecha – Completo	Dddd, d´de ´MMMM´de ´yyyy
Formato de Hora - Por defecto	Corto
Formato de Hora - Corto	HH:mm
Formato de Hora - Medio	HH:mm:ss
Formato de Hora – Largo	HH:mm:ss
Formato de Hora - Completo	HH:mm:ss
Formato Fecha y Hora - Por defecto	Corto
Formato Fecha y Hora - Corto	dd/MM/yy HH:mm
Formato Fecha y Hora - Medio	dd/MM/yyyy HH:mm:ss
Formato Fecha y Hora - Largo	D´de ´MMMM´de ´yyyy HH:mm:ss
Formato Fecha y Hora - Completo	Dddd, d´de ´MMMM´de ´yyyy HH:mm:ss

### Ejemplos:

Fecha larga: 20 de novembro de 2018  
Fecha completa: terça-feira, 20 de novembro de 2018

## 14 Documentos Fuentes de Información

- ✓ [Estándares de interfaz de usuario](#)
- ✓ [Versionado del Sistema](#)