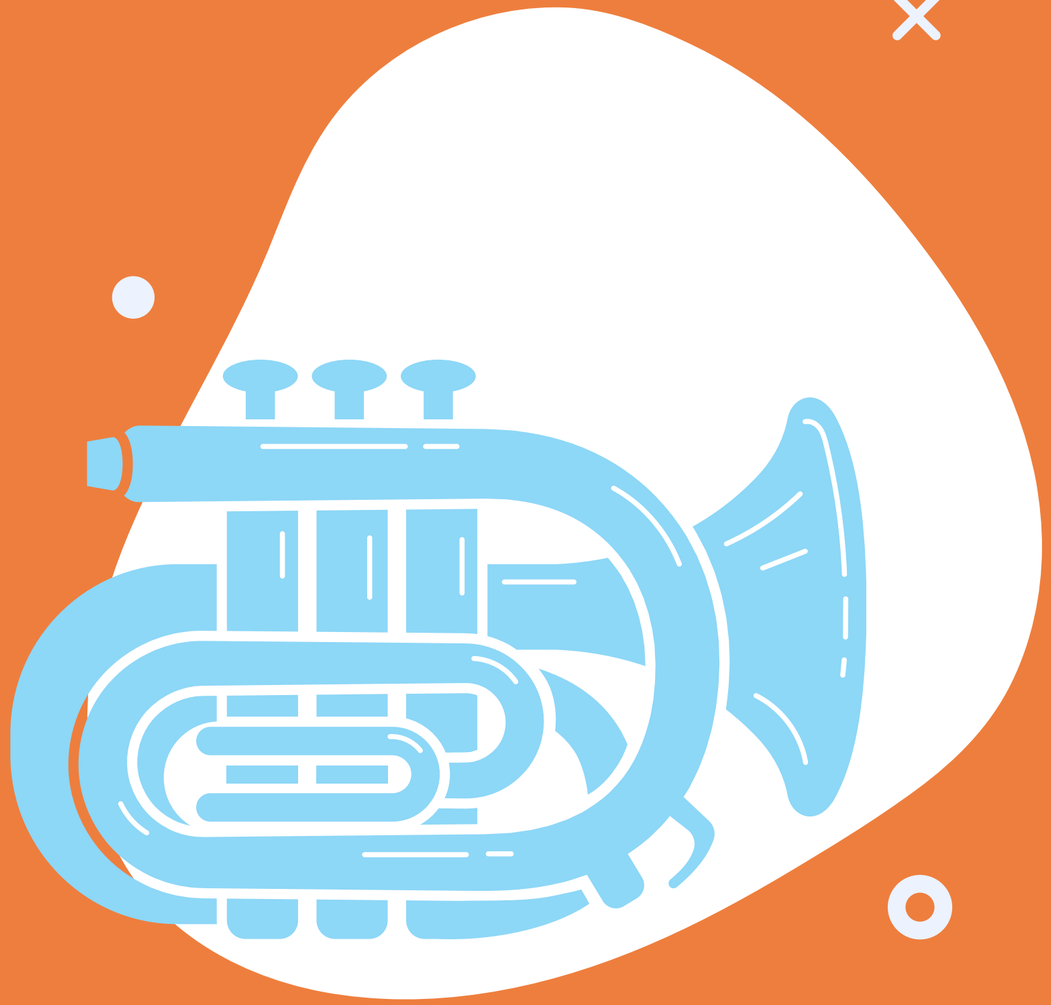
NOVASYS

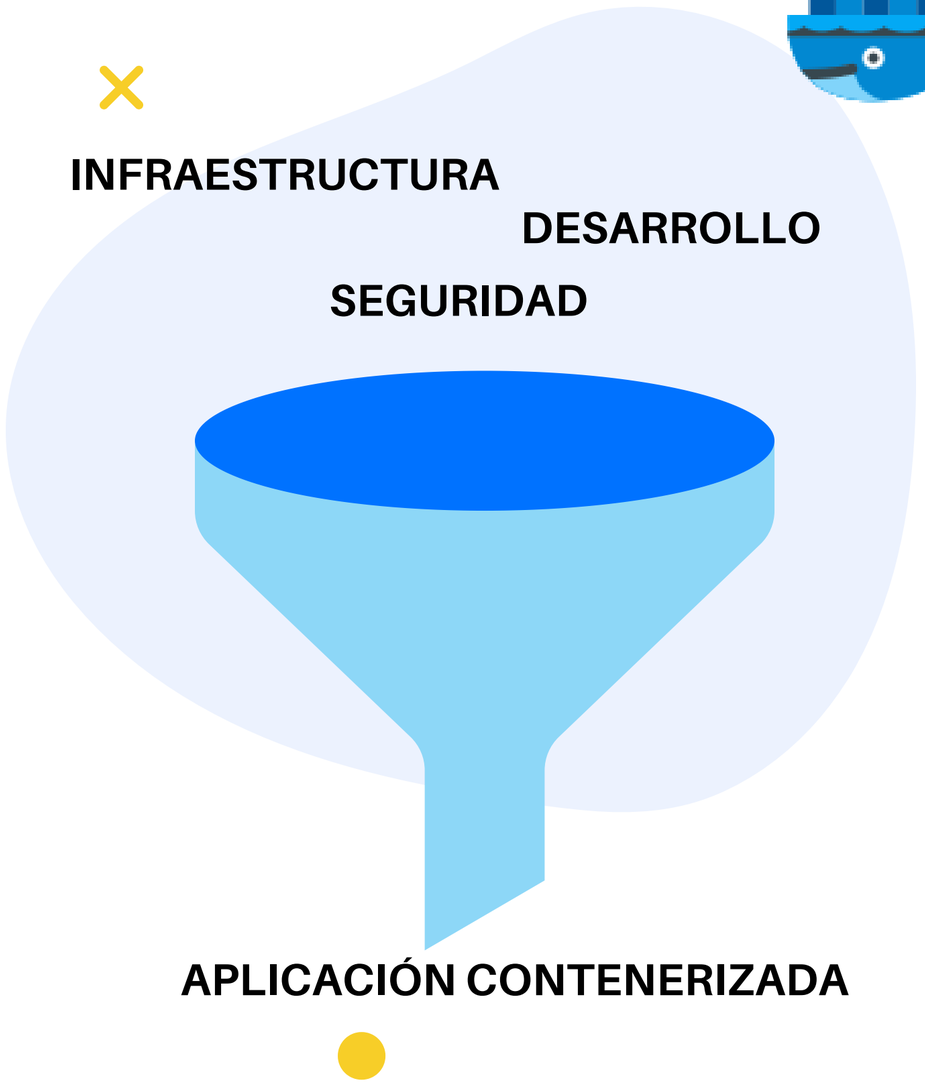
PRESENTA

SATSMO

Administración de Seguridad en Orquestadores



ORIGEN Y MODELO



SAT-SMO, es una aplicación web de desarrollada integramente en Argentina montada sobre framework de seguridad basado en un esquema RBAC y con módulos que le permiten brindar funcionalidades de uso especifico en el manejo de componentes de seguridad en aplicaciones contenerizadas.

El sistema esta basado en un esquema de colaboración y delegación de responsabilidades sin perder el foco en la seguridad y confidencialidad de la información relacionada con los Proyectos, Clusters, Contenedores y fundamentalmente las Secrets y Service Accounts utilizadas para compartir información sensible con las aplicaciones.

OBJETIVOS

SATSMO

- → Registrar los componentes básicos de seguridad en los orquestadores de contenedores con algoritmos de encripción propios
- → Proveer un punto único de acceso y desencripción de Secrets por proyecto
- → Administrar la vida útil de los componentes
- → Controlar los permisos de accesos de cada contenedor a las claves
- → Agilizar y centralizar los procesos de administración
- → Tracking de procesos
- → Agilizar la localización y uso de elementos
- → Apoyar la gestión de administración

BENEFICIOS

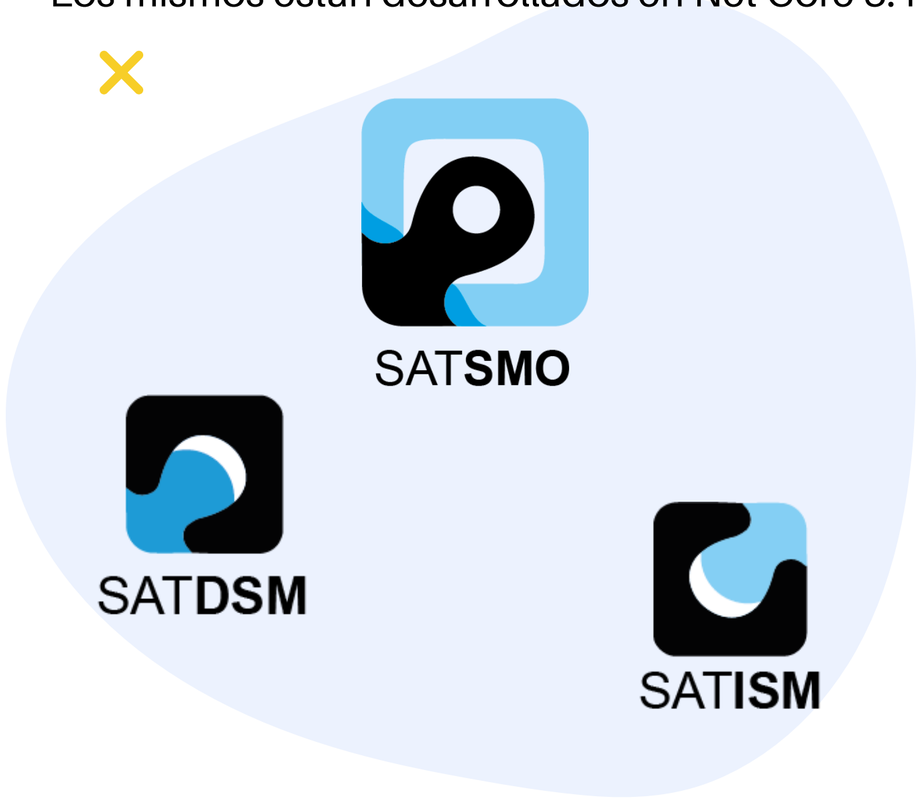
- Administración centralizada
- Gestión distribuida
- Encripción de componentes en modelos nativos de la aplicación
- Control y seguimiento de cambios
- Acceso a la información por grupos o áreas de injerencia
- Facilidad de gestión y seguimiento
- Requisitos funcionales moderados
- Uso intuitivo

CONTRAS

COMPONENTES DE LA APLICACIÓN

La aplicación esta compuesta por dos módulos separados que realizan una parte de las tareas cada uno.

Los mismos están desarrollados en Net Core 3.1 y pueden ser ejecutados tanto en plataformas Windows como Linux.



Este módulo posee una interfaz web accesible por los usuarios finales y su funcionalidad es la de:

- Administrar los Proveedores de Orquestación
- Definir las Clusters disponibles
- Identificar los proyectos implementados en cada cluster
- Especificar los contenedores (PODs o Servicios)
- Administrar los Secrets y Service Accounts
- Generar los Certificados
- Administrar la seguridad y auditoría de la aplicación

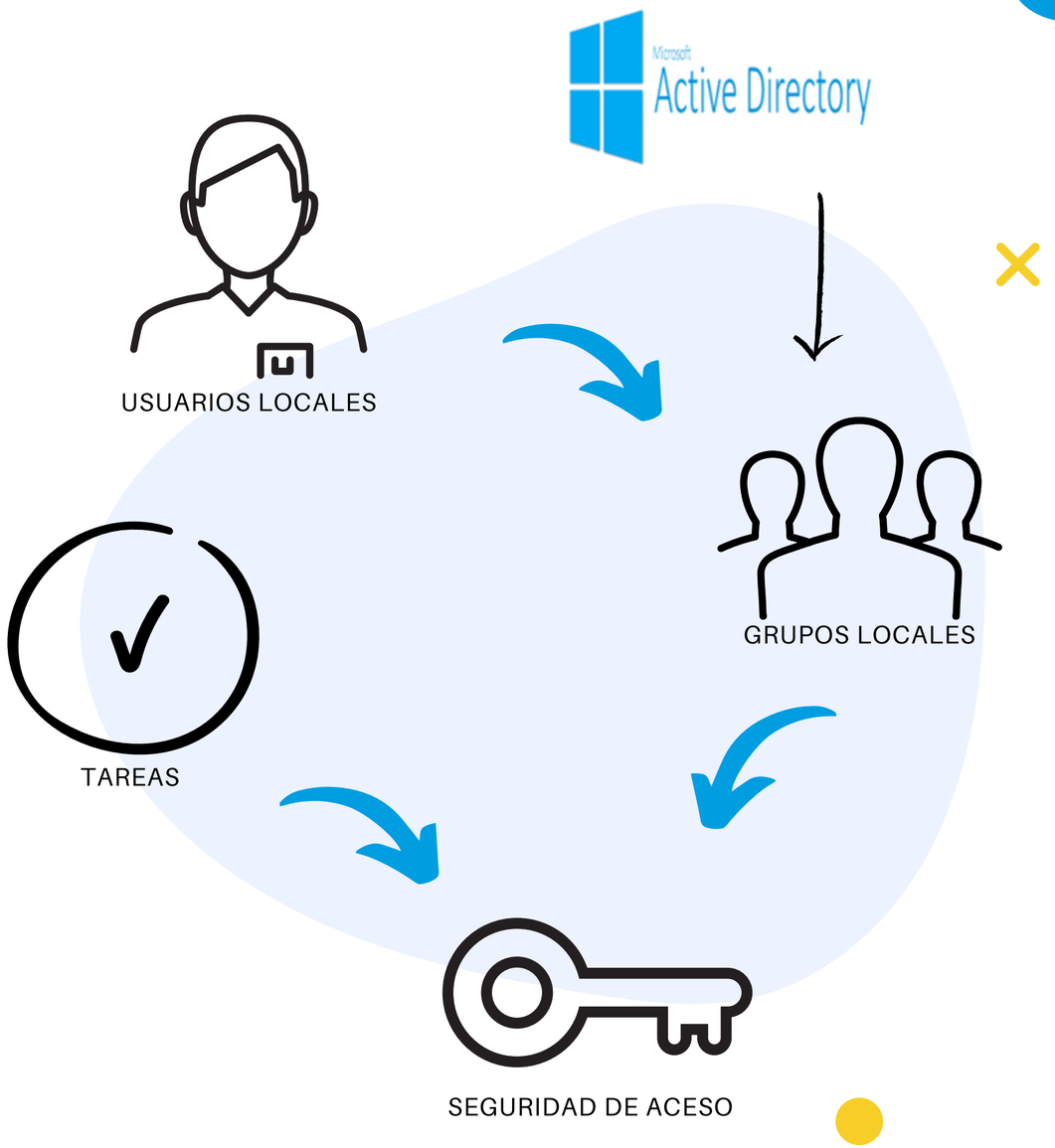
Es el módulo encargado de interactuar con los Secret Managers de los orquestadores para reunir la información sensible necesaria para los contenedores.
Las Secrets las puede obtener desde el Secret Manager, o usando volúmenes externos que almacenen los archivos con la info encriptada.
Esta última alternativa reduce en DOWN-TIME al renovar una secret.

GESTION DE USUARIO

Al estar basado en modelo RBAC, las funciones de los Usuarios de la aplicación se define localmente y de manera dinámica, pudiendo generarse diferentes perfiles de seguridad con la segregación de tareas de acuerdo a las necesidades operativas.

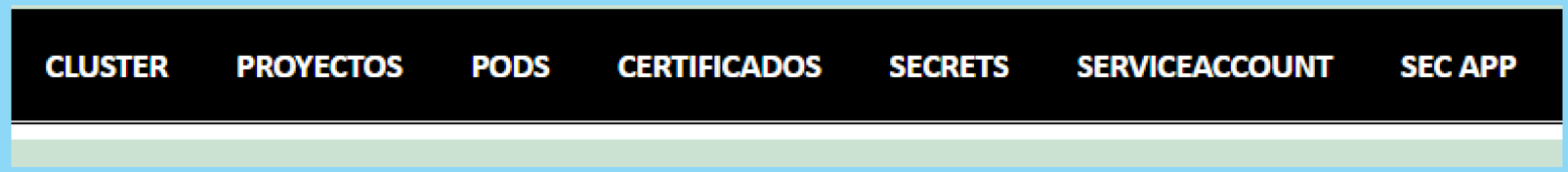
Los grupos de seguridad se definen internamente; mientras que los Usuarios pueden estar definidos internamente o ser validados por un Active Directory, en cuyo caso se valida la existencia de un grupo de seguridad interno como parte de los Member of.

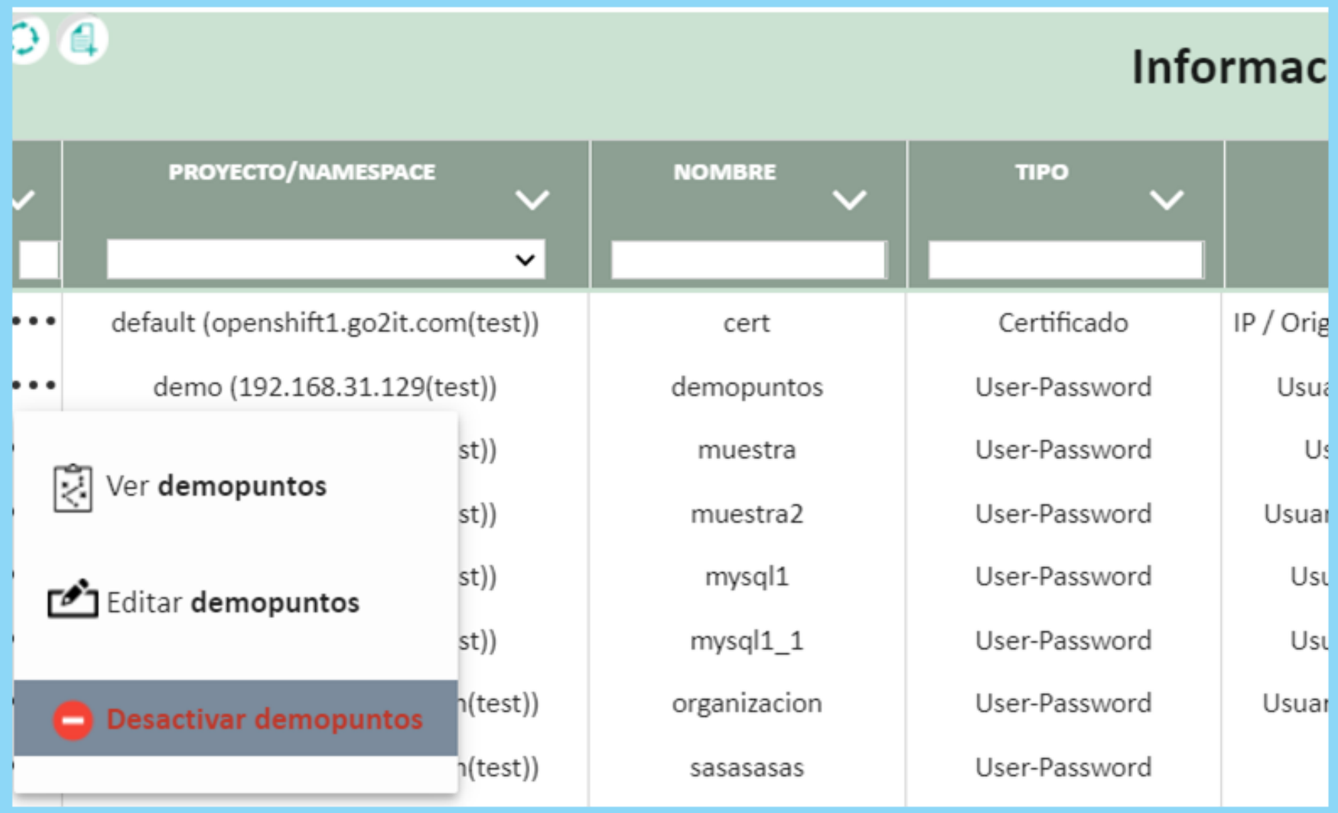
Esto permite incorporar Usuarios externos a la organización sin necesidad de incorporarlos en su sistema corporativo.



OPERATORIA GENERAL

El Usuario cuenta en todo momento con un menú que le permite acceder a todas las funcionalidades habilitadas según su perfil.

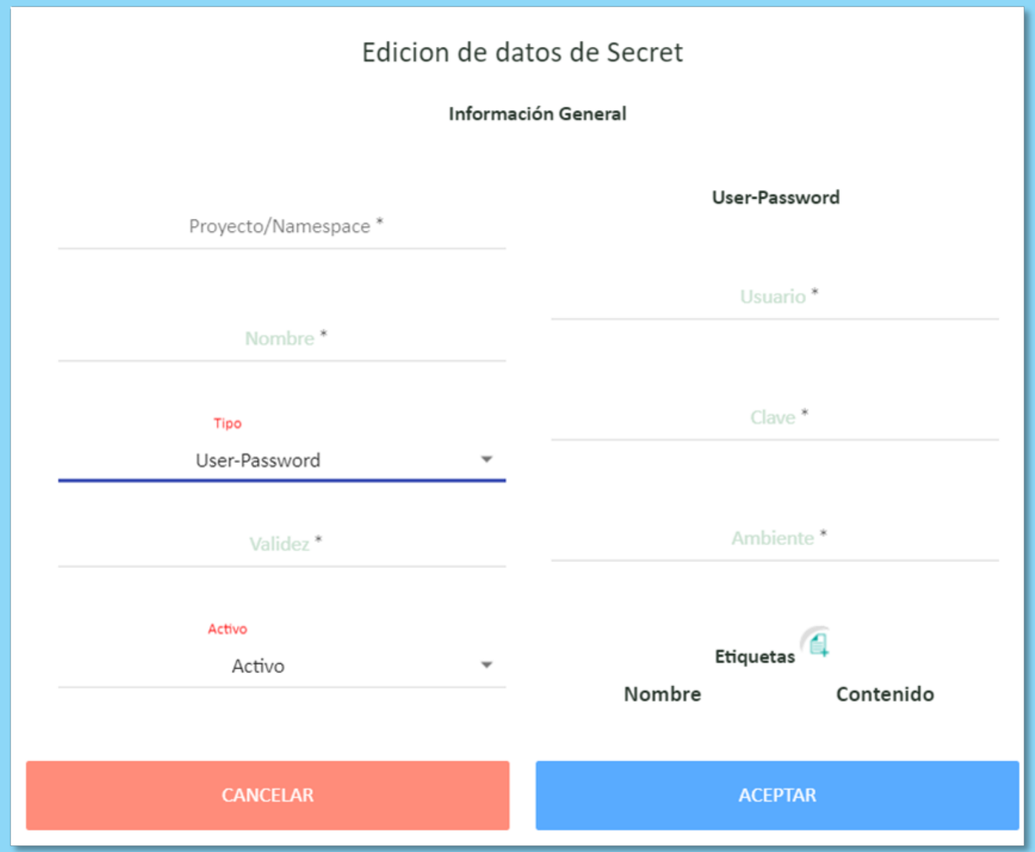




Se dispondra en cada página de la posibilidad de filtrar la información según lo requiera para facilitar la gestión .

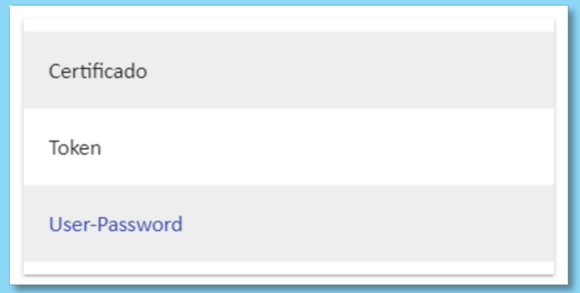
Así como tambien contara con barras de herramientas que le faciliten el acceso a tareas comunes y menúes contextuales que le permitan operar sobre elementos particulares; manteniendo siempre visible la referencia al elemento seleccionado.

OPERATORIA GENERAL

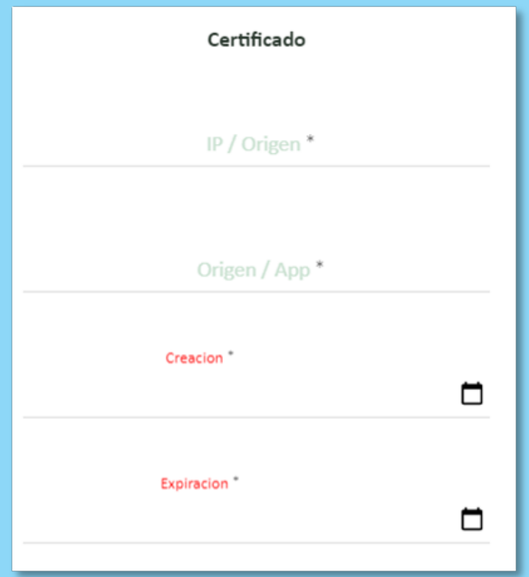


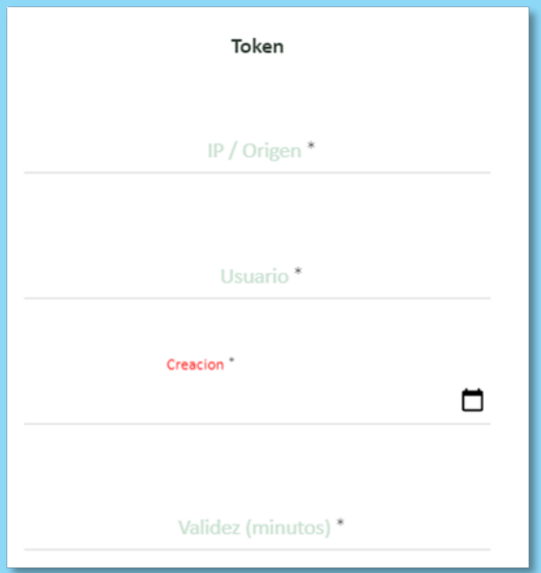
Siendo la SECRET el elemento de compartición de información sensible con los contenedores, la administración de las mismas es uno de los componentes fundamentales, pudiendo desde la aplicación generar las mismas tanto en Openshift como en Kubernetes o Swarm.

En las mismas se pueden definir los tipos estándar, así como tipos Custom que se registran encriptados con algoritmos propios.



Al cambiar la especificación del TIPO, tenemos acceso a ingresar diferentes modelos de datos según la selección





GESTION DE SERVICE ACCOUNT

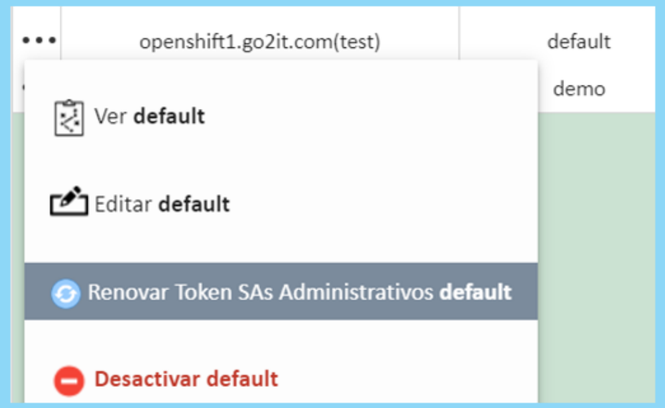
Este tipo de componente esta disponible únicamente para dos de los orquestadores (Openshift y Kubernetes); pero en ambos casos es el componente utilizado para la interrelación de la aplicación con los mismos.
Para ello se permite la creación de dos tipos de SAs, los de uso general y los administrativos, que se recomienda generar por pares.
Si bien ambos se administran desde la app, los primeros son de administración libre, no así los ADMINISTRATIVOS que son los usados para el acceso y la operatoria.

	PROYECTO/NAMESPACE	NOMBRE	ARCHIVO	SERVICE ACCOUNT I D2	ADMINISTRATIVO	ACTIVO
•••	default (openshift1.go2it.com(test))	sec-man	sec-man_test.crt		✓	✓
•••	default (openshift1.go2it.com(test))	sec-man2	sec-man2_test.crt		✓	✓
•••	CuentaCorriente (openshift1.go2it.com(...	sa_cli	sa_cli.crt	ddddddd: ddddddd - destino: test - ffff: ...	✗	✓

Pudiendo renovar los tokens de los mismos, accediendo desde diferentes lados.

Los Genericos, desde la misma definición del SA.

Los Administrativos desde la gestión del Proyecto al cual pertenecen, ya que se renueva el par de manera automática.



GESTION DE CERTIFICADOS DE VINCULACIÓN

	PROYECTO/NAMESPACE	NOMBRE	ARCHIVO	SERVICE ACCOUNT I D2	ADMINISTRATIVO	ACTIVO
•••	default (openshift1.go2it.com(test))	sec-man	sec-man_test.crt		✓	✓
•••	default (openshift1.go2it.com(test))	sec-man2	sec-man2_test.crt		✓	✓
•••	CuentaCorriente (openshift1.go2it.com(...	sa_cli	sa_cli.crt	ddddddd: ddddddd - destino: test - ffff: ...	✗	✓

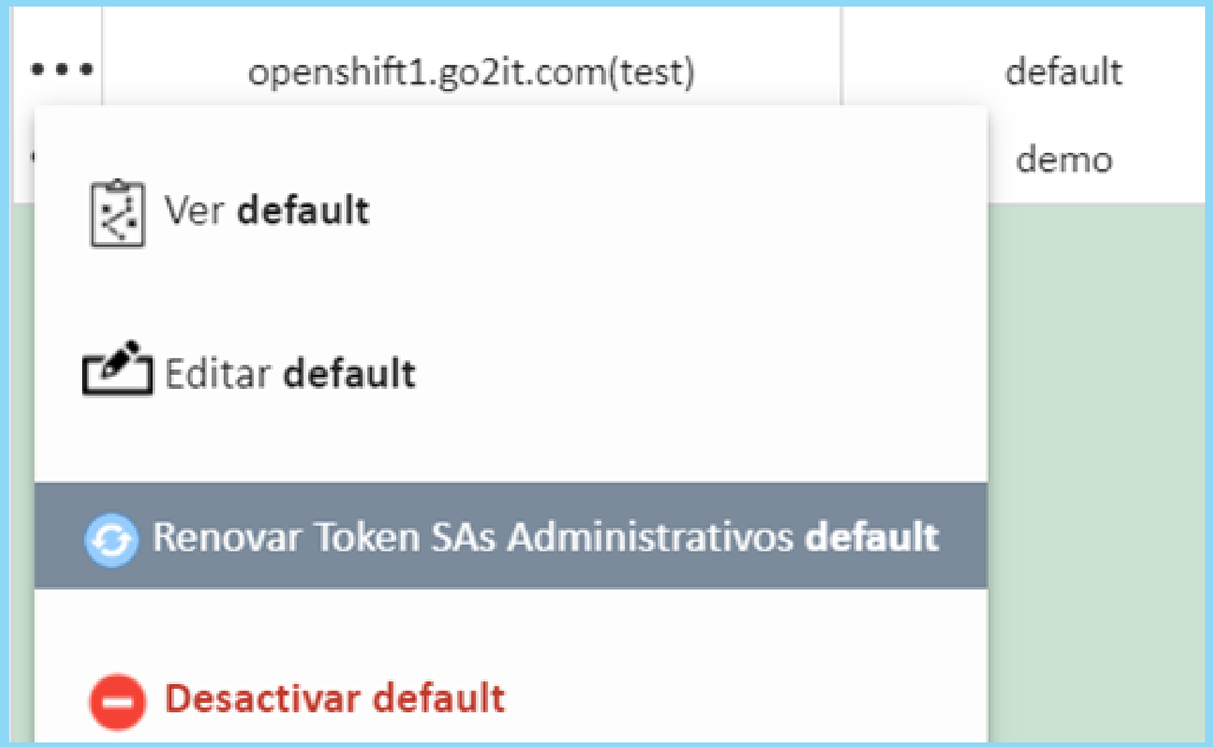
Encontramos dentro del sistema la posibilidad de gestionar certificados que se utilizan dentro de la aplicación para :

- Identificar el contenedor solicitante
- Especificar las Secrets accesibles para el mismo.

El mismo se genera como un certificado encriptado, cuyo contenido se registra en un archivo de salida para ser compartido con el contenedor especificado.

Dicho contenedor debe remitir el mismo dentro del encabezado de las solicitudes de Secrets, para ser validado como origen reconocido y accesos permitidos.

Sin este contenido, el componente de seguridad interna no validara la petición generando un retorno nulo con código de Forbidden y registrando la solicitud en el log.



Gracias.

Contactenos

(5411) 5326-0913

novasys@novasys.com.ar

www.novasys.com.ar