centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1118

Procedimiento de Empleo Seguro
SOFFID IAM

Octubre 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-121-8

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.05.05 09:41:39 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

.

ÍNDICE

1. INTRODUCCIÓN

1. *Soffid IAM* es una plataforma IAM que reúne la gestión de acceso privilegiado (PAM) y Gestión de identidades (IM) en una plataforma integral.
2. El sistema de referencia está formado por un sistema operativo base fortificado, con soporte para micro contenedores. Para este procedimiento de empleo seguro se utilizará la herramienta de micro contenedores *Docker*.
3. Así mismo, se debe crear una red privada virtual de comunicaciones, aislada de la red física real. Esta red permitirá la comunicación segura entre los distintos elementos de la solución.
4. A continuación, se muestra la arquitectura interna de los distintos módulos y cómo se relacionan entre ellos para ofrecer los objetivos funcionales del producto:

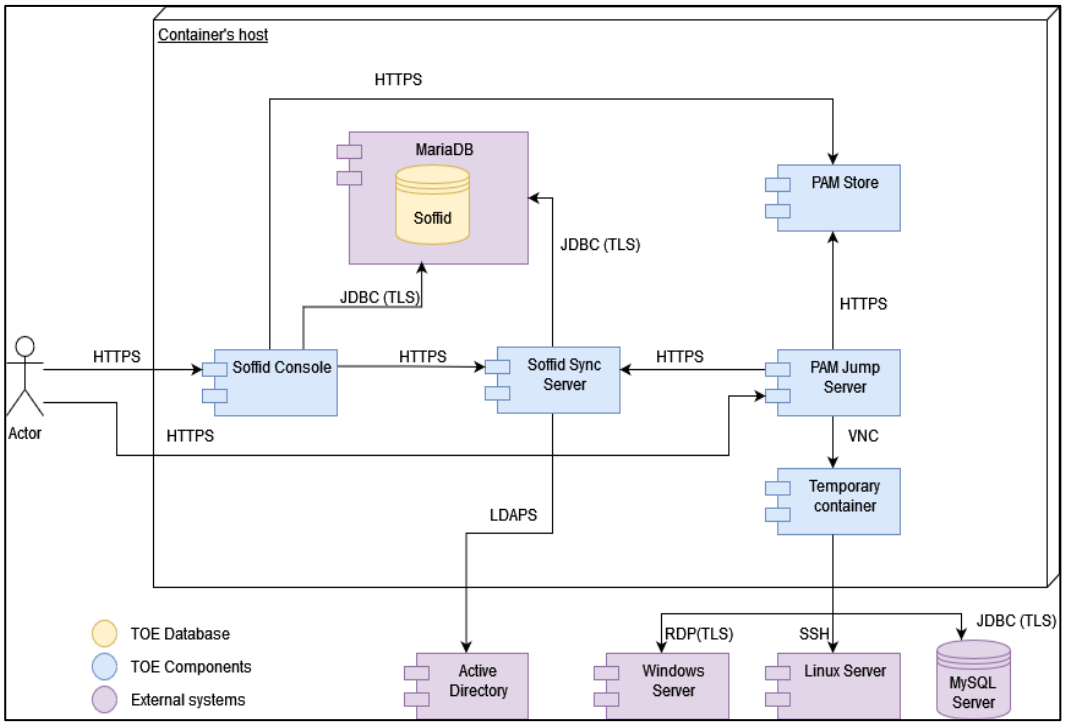


Ilustración 1: Arquitectura de Soffid IAM

5. Los componentes dentro de *Soffid IAM* interactúan entre ellos a través de conexiones HTTPS o JDBC, ambos tipos de conexiones administrados de forma segura mediante TLS.
6. La plataforma *Soffid IAM* interactúa con cinco componentes externos (Ilustración 1):
   - Servidor MariaDB para el componente del Soffid Repository;
   - *Active Directory* para la gestión de cuentas de usuario;
   - Servidor *Windows;*
   - Servidor *Linux*;
   - Servidor *MySQL* para establecer sesiones privilegiadas controladas por PAM.
7. Mediante el protocolo LDAPS *Soffid IAM* puede crear, modificar y desactivar o eliminar cuentas en el agente del *Active Directory*.

8. Mediante los protocolos SSH, RDP o JDBC, el sistema PAM Jump Server permite que usuarios autorizados accedan a los servidores Windows, Linux o MySQL de forma segura y monitorizada. Se utilizan los siguientes clientes para cada tipo de conexión:

PROTOCOLO	CLIENTE
SSH	Remminia
RDP	XFreeRDP
JDBC	DBeaver

Tabla 1: Clientes para sesiones PAM

9. Por último, es importante remarcar un aspecto fundamental para la utilización del software y para la comprensión del presente documento. En el sistema *Soffid IAM* se diferencia entre los conceptos “usuario” y “cuenta”, teniendo en cuenta lo siguiente:

   - Los usuarios son el identificador empleado para la autenticación de forma inequívoca frente al propio software *Soffid IAM*.
   - Las cuentas están asociadas a usuarios S*offid IAM* y representan las credenciales y atributos relativos a un agente o sistema gestionado por *Soffid IAM*. Por lo tanto, un usuario *Soffid IAM* puede tener asociadas varias cuentas.

2. OBJETO Y ALCANCE

10. El objetivo de este documento es servir como guía de empleo seguro para la instalación, configuración y operación del producto ***Soffid IAM* 3.5 ,** que proporciona funcionalidades de IAM y PAM.

11. Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) para categoría ALTA en las familias “Gestión de Acceso Privilegiado (PAM)” y “Gestión de Identidades (IAM)”.

12. Las conexiones entre componentes en el sistema deben estar configuradas para para cumplir los requisitos de seguridad implementados por la guía CCN-STIC-807 [REF1].

13. El despliegue del producto se realizará sobre un sistema *CentOS Stream 9*, al cual previamente se le habrá aplicado la guía CCN-STIC-610A22 Guía de Aplicación de perfilado de seguridad para Red Hat Enterprise Linux [REF2].

14. Se debe usar el software de *Docker Engine* para montar los diferentes contenedores necesarios para el despliegue de la arquitectura del producto. A este respecto, además de la configuración establecida por la guía CCN-STIC-610A22 Guía de Aplicación de perfilado de seguridad para Red Hat Enterprise Linux [REF2], únicamente será necesario añadir al sistema operativo un nuevo usuario *soffid*, con privilegios de administrador y pertenencia al grupo *docker*.

15. Para realizar la fase de configuración y administración de los contenedores usados en el despliegue de la aplicación, se usará la herramienta de *Portainer.io*, el uso de esta herramienta es opcional, pero facilita la configuración de la aplicación. Esta herramienta se usará durante la fase de configuración de este documento.

16. Se usará *MariaDB* como sistema gestor de bases de datos.

17. El software referenciado en los puntos anteriores es necesario para la utilización de este producto y debe disponer de soporte de seguridad del fabricante y estar correctamente actualizado y bastionado.

18. Se recomienda que el servidor físico donde se instale el *CentOS* cumpla con los siguientes requerimientos mínimos de hardware:

    - 16 GB RAM.
    - 250 GB de disco duro.
    - 2 CPUs.

3. ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

e) Apartado 8. En este apartado se recogen los pasos para la configuración del agente de *Active Directory*.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

19. Para proceder a la instalación del producto *Soffid IAM,* se han de descargar las imágenes correspondientes a los diferentes componentes del producto. Estos componentes se comunican entre ellos para constituir la arquitectura del producto.

20. Debemos de descargar las imágenes de cada componente desde el repositorio de *Soffid* en *Dockerhub* [REF3]. Las versiones que usaremos para cada imagen son: para *IAM-console* la **3.5.57**, para el *Sync-server* la **3.5.22**, para el *PAM-launcher* **1.4.36**, para el *PAM-store* **1.4.36**.

21. Asimismo, se deberán descargar las plantillas de las imágenes temporales que se utilizan durante las conexiones PAM: jdbc, ssh y rdp.

22. Estas imágenes se encuentran disponibles en el "Repositorio de imágenes de Soffid" [REF3]**.**

23. Para verificar la integridad de las versiones de las imágenes descargadas será necesario verificar su huella digital mediante la función resumen **sha256.** Para ello, en un terminal de sistema, deberemos listar la información de cada una estas imágenes (`sudo docker images --no-trunc`)**.**

24. Los hashes de las imágenes descargadas deben coincidir con los que aparecen definidos en la siguiente tabla:

NOMBRE DE LA IMAGEN	Hash (SHA-256)
Soffid/pam-launcher 1.4.36	b918b58d0469e2f32748ea55181b9fb2867250b3e2e222c2cf6b5cc489e86c8c
Soffid/pam-store 1.4.36	737d97f1d439e7c3c0f31f646c5c35c9bf0c8f36f2c3fa0dd23fe33648f891c2
Soffid/iam-sync 3.5.22	90d25c1f45c38e577f54bc9c1c35c095e0cc0d698bbd402e115614cd311d001
Soffid/iam-console 3.5.57	f5af5f13f49a7427b87ea64a98fd48661d31cf5dff7cecb22576fcaa193b58d1
soffid/soffid-pasr-jdbc 1.4.12	7812b49f8dfab96874015d60888cd34c41a3c5b56ba1226ed6db1fd4c54bc122
soffid/soffid-pasr-rdp 1.4.12	7ad3dc23234ee6f42c74a664f288795a1c180de10d615d527b0e432d80bc9cb2
soffid/soffid-pasr-ssh 1.4.12	f1df5c56643d6399be5b67bc320efb7e4b6c3edcc7cf65087a2b91845dc8d7a5

Tabla 2: Tabla de comprobación de hashes para las imágenes y sus versiones de componentes de Soffid IAM.

25. Una vez verificada la integridad de las imágenes y con respecto a las plantillas `soffid-pasr-ssh`, `soffid-pasr-rdp` y `soffid-pasr-jdbc`, será necesario etiquetarlas apropiadamente para que, a la hora de ser ejecutadas, no sean descargadas desde el repositorio remoto sino desde local.

26. Para ello, se utilizarán los siguientes comandos:

```
sudo docker image tag soffid/soffid-pasr-jdbc:1.4.12 soffid/soffid-pasr-jdbc

sudo docker image tag soffid/soffid-pasr-rdp:1.4.12 soffid/soffid-pasr-rdp

sudo docker image tag soffid/soffid-pasr-ssh:1.4.12 soffid/soffid-pasr-ssh
```

4.2 ENTORNO DE INSTALACIÓN SEGURO

27. Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado disponga de autorización para la configuración, despliegue y mantenimiento del producto.

28. El personal que opere y administre el producto debe estar adecuadamente formado, conforme a los procesos de selección y formación de la propia empresa.

29. La gestión de acceso durante el proceso de instalación se debe gestionar siguiendo los principios de control de acceso establecidos por la propia empresa.

30. La verificación de la identidad de los usuarios gestionados por el producto se debe realizar conforme a los principios establecidos por la propia empresa.

4.3 REGISTRO Y LICENCIAS

31. *Soffid IAM* no requiere la activación de licencias para su instalación o uso.

4.4 ENTORNO DE OPERACIÓN

32. Para realizar el proceso de instalación del producto se deben de instalar en el entorno de operación los siguientes componentes, con sus correspondientes versiones:

    - MariaDB **11.1.2** [REF4]
    - Portainer.io-CE **2.16.2** [REF4]
    - Docker Engine **23.0.1[**REF6]

33. A continuación, se muestran los hashes para las imágenes instaladas del software externo a *Soffid IAM* mencionados anteriormente:

NOMBRE DE LA IMAGEN	Hash
MariaDB11.1.2	f35870862d64d0e29598fba1d7f75cfefeb3f891cb22b3e2d4459c903e666554
Portainer.io-CE 2.16.2	5f11582196a42b895cdb9322f7a650f42a0c1ed062efc71864352f314228a187

Tabla 3: Tabla de comprobación de hashes para las imágenes y sus versiones del software externo

34. Para los agentes externos descritos en la Ilustración 1, se usarán los siguientes sistemas operativos y sus correspondientes versiones:

    - Linux server: **Ubuntu 23.04**
    - Active Directory: Windows server 2019 standard evaluation
    - Windows server: Windows 10 PRO 10.0.19045
    - Cliente gestor de base de datos: **DBeaver 22.3.0**
    - MySQL server: MariabDB 10.11.2

35. El producto requiere de una fuente de información de tiempo (sistema operativo, NTP) confiable.

36. Todos los componentes del entorno de operación, en especial los que se utilicen como fuentes autoritativas de datos, deben ser confiables y estar instalados conforme a las políticas de la empresa.

5. FASE DE INSTALACIÓN

37. Una vez creado el entorno seguro de instalación, se pasará a realizar la instalación del producto.

38. En las siguientes subsecciones, se describe la instalación de los diferentes componentes de *Soffid IAM*. Para realizar la instalación de manera correcta, se deben realizar dichas secciones de manera secuencial.

5.1 CONSIDERACIONES PREVIAS

39. Se utiliza un formato en `fuente monoespaciada y con fondo gris` para denotar un comando o una salida de texto por línea de comandos.

40. Cuando se especifican comandos, se utilizan los caracteres `{}` para delimitar parámetros que debe establecer el usuario.

41. Todos los comandos de *docker* se ejecutan con el usuario de sistema "*soffid*".

42. Algunas imágenes de docker utilizadas para la instalación no contienen ningún editor de texto. Para editar los archivos que se indican, se recomienda seguir los siguientes pasos:

    - utilizar el comando `docker cp –L {nombre del contenedor}:{ruta al archivo} /tmp/{nombre del archivo}` para copiar el archivo al sistema operativo anfitrión,
    - editar el archivo con algún editor de texto y posteriormente,
    - ejecutar el comando inverso `docker cp /tmp/{nombre del archivo} {nombre del contenedor}:{ruta al archivo}` para copiar el archivo editado al interior del contenedor.

43. En algunos puntos de este procedimiento de empleo seguro se mencionan comandos que deben ejecutarse desde el interior del contenedor. Para iniciar una sesión de consola en el interior del contenedor, basta con ejecutar `docker exec –it {nombre del contenedor} bash`.

44. Tras la instalación del producto, el sistema operativo debe exponer únicamente los puertos TCP 8082 y 8443.

5.2 CREACIÓN DE UNA RED INTERNA

45. Iniciamos sesión en el sistema *CentOS* (previamente configurado con la guía CCN-STIC-610A22 [REF2]) y abrimos un nuevo terminal de sistema.

46. Una vez abierto el terminal, iniciamos el proceso de *Docker* (`systemctl start docker`). Para comprobar que se ha iniciado correctamente el servicio se debe verificar el estado activo del mismo (`systemctl status docker`).

47. Para comunicar los diferentes contenedores que iremos creando para cada componente de *Soffid IAM*, crearemos una red virtual interna que sirva de base de comunicación entre ellos.

48. Creamos la red virtual interna con *Docker* (`docker network create -d bridge {nombre_de_la_red}),` donde se le puede asignar a la red el nombre que se desee).

49. Para poder hacer uso de las funcionalidades que nos ofrece *Portainer.io* se deberá crear un contenedor dentro de la red para este software. Una vez creado, se deberá configurar para poder desplegar la interfaz gráfica de esta herramienta en el puerto oportuno.

5.3 INSTALACIÓN Y CONFIGURACIÓN DE LA BASE DE DATOS

50. Para crear el contenedor *Docker* de base de datos, escribimos:

```
docker run -d --name mariadb-service --network={nombre_de_la_red} -e "MARIADB_ROOT_PASSWORD={Contraseña_segura}" mariadb.
```

51. La contraseña debe cumplir con la política de contraseñas especificada en el apartado 6.3.5 de este documento.

52. Posteriormente, se debe comprobar que el contenedor de la base de datos está funcionando correctamente (`docker ps`).

53. A continuación, ejecutamos el comando `mariadb –u root –p` dentro del contenedor `mariadb-service`.

54. Aparece el texto "`Enter password:`". Introducimos la contraseña que hemos establecido anteriormente.

55. Una vez accedida *Mariadb*, se crea una base de datos (`create database {nombre_db};`)y accedemos a ella (`use {nombre_db}).`

56. A continuación, damos los permisos al usuario administrador con el comando:

```
grant all privileges on *.* to ADMIN_USER@'%' identified by '{Contraseña_db}' with grant option;
```

57. Seguidamente modificamos el fichero my.cnf `(/etc/mysql/my.cnf).`

58. Las siguientes líneas deben añadirse al final del archivo:

```
[mysqld]
max_allowed_packet=128M
[mysqld]
innodb_log_file_size=254M
[mysqld]
character-set-server = utf8mb4
collation-server = utf8mb4_general_ci
innodb_large_prefix = 1
innodb_file_format = Barracuda
innodb_file_per_table = 1
```

59. Una vez finalizadas las anteriores acciones, es necesario reiniciar el contenedor para que aplique los cambios realizados en el fichero de propiedades modificado (`docker restart mariadb-service`).

60. Posteriormente, se verifica que el contenedor continúa ejecutándose correctamente (`docker ps`).

5.4 INSTALACIÓN Y CONFIGURACIÓN DE LA CONSOLA

61. Dentro de este apartado se describen las tareas necesarias para la instalación y configuración de la consola. Para ello, emplearemos el contenedor *Docker* respectivo mediante los siguientes comandos:

```
docker run -d \
-e DB_URL=jdbc:mariadb://mariadb-service/{nombre db} \
-e DB_USER=ADMIN_USER \
-e DB_PASSWORD={contraseña db} \
--name=iam-console \
--publish=8443:8443\
--network={nombre_de_la_red} \
soffid/iam-console:3.5.57
```

62. Se comprueba que los dos contenedores están funcionando correctamente (consola y base de datos) (`docker ps`). A continuación, verificamos los logs de auditoria relacionados con el contenedor de la consola (`docker logs -f iam-console).`

63. Deberá obtenerse un certificado digital en formato jks para la consola, de la Autoridad de Certificación (CA) indicada por el administrador del producto.

64. En caso de que no se trate de una CA conocida, deberá copiarse el certificado de dicha CA al directorio `/opt/soffid/iam-console-3/trustedcerts`. En caso de que dicho directorio no exista, es necesario crearlo antes de realizar la copia.

65. Se deberá copiar el certificado jks al contenedor docker de la consola (`docker cp {nombre del certificado} iam-console:/opt/soffid/iam-console-3/trustedcerts)`

66. Posteriormente, se deberá iniciar una sesión de consola en el contenedor `iam-console` y desplazarse al directorio `/opt/soffid/iam-console-3/trustedcerts`.

67. Una vez realizada la conexión, ejecutar el siguiente comando para ver el alias que identifica el certificado, `keytool -list -keystore {nombre del certificado}`, y guardar el alias para usarlo posteriormente (el alias es el primer identificador que aparece antes de la fecha).

68. A continuación, editar archivo del servidor (`server.xml)`, dentro del mismo localizar el siguiente código:

```
<Connector port=”8443”
protocol=”org.apache.coyote.http11.Http11NioProtocol”
maxThreads=”150” SSLEnabled=”true”>
  <SSLHostConfig protocols="TLSv1.3">
    <Certificate
     certificateKeystoreFile=”trustedcerts/{nombre del certificado}”
            certificateKeystorePassword=”{contraseña del certificado}”
           certificateKeyAlias=”{alias}” type=”RSA” xpoweredBy=”false”
    server=”Apache TomEE” />
  </SSLHostConfig>
</Connector>
```

69. Debemos modificar este código para introducir el nombre del certificado digital, su contraseña y el alias que hemos copiado en el paso anterior.

70. De la misma manera, debemos comentar o eliminar el apartado de XML que se encuentra entre `<Connector port="8080">` y `</Connector>` para desactivar la interfaz sin cifrado.

71. Debemos asegurarnos de que el certificado que hemos copiado a `/opt/soffid/iam-console-3/trustedcerts` permita solo lectura a su propietario (que debe ser `soffid`) y a su grupo (que debe ser `root`) y ningún otro permiso. En caso de que no sea así, podemos establecer la configuración ejecutando los siguientes comandos desde una consola en el contenedor `iam-console`: `chown soffid:root {nombre del certificado}; chmod 440 {nombre del certificado}`

72. A continuación, se debe reiniciar el contenedor para que se guarden los cambios realizados (`docker restart iam-console`).

73. El usuario por defecto es **admin** y la contraseña **changeit,** por lo que el último paso necesario será cambiar la contraseña y escribir una nueva que cumpla la política de contraseñas indicada en el apartado 6.3.5 de este documento. Para ello, accedemos a la url `https://localhost:8443` e introducimos dichas credenciales. Acto seguido el sistema nos solicita un cambio de contraseña.

5.5 INSTALACIÓN Y CONFIGURACIÓN DEL SYNC-SERVER

74. La siguiente tarea es la instalación del contenedor de Sync-server. Para ello, es necesario ejecutar las siguientes líneas de comandos en la terminal:

```
docker run -d \
-e DB_URL=jdbc:mysql://mariadb-service/{nombre db} \
-e DB_USER=ADMIN_USER \
-e DB_PASSWORD={contraseña db} \
-e SOFFID_PORT=1760 \
-e SOFFID_HOSTNAME=iam-sync.{nombre de la red}  \
-e SOFFID_MAIN=yes \
--name=iam-sync \
--network={nombre de la red} soffid/iam-sync:3.5.22
```

75. Para comprobar que el Sync-server se ha desplegado correctamente, se debe revisar la interfaz gráfica del navegador del paso anterior y acceder a la monitorización del sistema en: `Administración > Monitorización e informe > Monitorización del sistema.`

76. En caso de que, pasados unos minutos, no aparezca el Sync-server como "OK", se debe reiniciar el contenedor utilizando el comando `docker restart iam-sync`.

77. Si el problema continúa, será necesario despublicar el servicio de Sync-server. Para ello, en primer lugar, se debe eliminar el servidor de la pantalla de Servidores de Sincronización (`Administración > Configurar Soffid > Motor de Integración > Servidores de Sincronización`), procediendo a parar y borrar el contenedor del mismo y reiniciando su ejecución mediante el comando descrito anteriormente

78. Una vez se ha establecido la conexión entre el Sync-server y la Consola, es necesario configurar un cifrado seguro en el contendor. Para ello, se debe acceder al directorio /opt/soffid/iam-sync/bin/ dentro del contenedor y ejecutar ./configure –reencodeSecrets –newkey para activar el cifrado seguro RSA_OEAP de 3072 bits.

79. Una vez finalizada la ejecución, se debe de reiniciar el contenedor para que se apliquen los cambios.

5.6 INSTALACIÓN Y CONFIGURACIÓN DEL PAM

80. En esta sección se configura el PAM conforme al diagrama mostrado en la Ilustración 2:

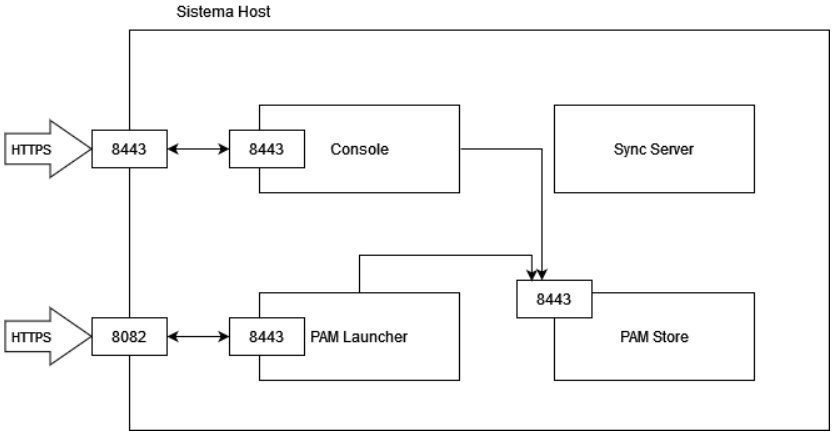


Ilustración 2: Conexiones internas y externas del PAM y la consola

81. En primer lugar , debe crearse el volumen que contendrá los certificados TLS para permitir conexiones seguras HTTPS, así como los volúmenes para la configuración de los contenedores. Para ello, ejecutamos los siguientes comandos:

```
docker volume create certificados
docker volume create soffid-pam-store
docker volume create soffid-pam-launcher
```

82. Se deben obtener dichos certificados de una CA en formato jks y common name (CN) `soffid-pam-launcher` y `soffid-pam-store` respectivamente.

83. A continuación, deben copiarse ambos certificados al directorio `/var/lib/docker/volumes/certificados/_data` del sistema operativo anfitrión. Cabe destacar que generalmente este directorio solo puede ser escrito por el usuario “root”.

84. En primer lugar, se instala el componente PAM Store, ejecutando el siguiente comando:

```
docker create \
     -v certificados:/opt/soffid/tomee/certificados \
     --network {nombre de la red} \
     -v soffid-pam-store:/opt/soffid/tomee/data \
     --name soffid-pam-store \
-e JAVA_KEYSTORE=”/opt/soffid/tomee/certificados/{nombre del certificado para
el PAM store”} \
-e KEYSTORE_PASS=”{contraseña del certificado para el PAM store}” \
     soffid/pam-store:1.4.36
```

85. Una vez creado el contenedor, este debe iniciarse ejecutando el comando `docker start soffid-pam-store >/dev/null.`

86. En caso de que no lo conozcamos, podemos verificar el valor del alias del certificado utilizando el comando `keytool -list -keystore {nombre del certificado}`.

87. Es necesario reiniciar el contenedor y verificar que funciona antes de continuar.

88. A continuación, es necesario registrar un nuevo usuario en el PAM store. Para ello, en primer lugar, será necesario verificar que no existe previamente ningún usuario mediante el siguiente comando:

```
docker exec soffid-pam-store cat /opt/soffid/tomee/data/passwd
```

89. Si se comprueba que es así, procedemos a ejecutar el siguiente comando, tomando nota de la salida que muestra por pantalla, puesto que esta será la contraseña:

```
docker exec soffid-pam-store /opt/soffid/tomee/bin/add-user.sh $(hostname)-launcher launcher
```

90. En caso de que la comprobación previa del contenido de /opt/soffid/tomee/data/passwd indique que sí existe un usuario, entonces el comando anterior deberá ejecutarse utilizando un nombre de usuario único, por ejemplo `$(hostname)-launcher-$(date '+%s')`

91. Una vez terminado se deberá comprobar que se ha procesado correctamente.

92. A continuación, y con la contraseña mostrada por pantalla tras la ejecución del comando anterior, se instala el PAM Launcher ejecutando el siguiente comando:

```
     docker create \
       -v certificados:/opt/soffid/tomee/certificados \
       --network {nombre de la red} \
       -v soffid-pam-launcher:/opt/soffid/tomee/launcher \
       -v /var/run/docker.sock:/var/run/docker.sock \
       -p 8082:8443 \
       -e STORE_SERVER=”https://soffid-pam-store:8443” \" \
       -e STORE_USER="$(hostname)-launcher" \
       -e STORE_PASSWORD="{Contraseña}" \
        -e     JAVA_KEYSTORE=”/opt/soffid/tomee/certificados/{nombre     del certificado para el PAM launcher”} \
        -e KEYSTORE_PASS=”{contraseña del certificado para el PAM launcher}” \
       --name soffid-pam-launcher \
       soffid/pam-launcher:1.4.36
```

93. A continuación es necesario modificar el archivo de propiedades del sistema (`/opt/soffid/tomee/conf/system.properties`) dentro del contenedor del PAM launcher, y copiar las configuraciones de la siguiente ilustración para cada caso específico.

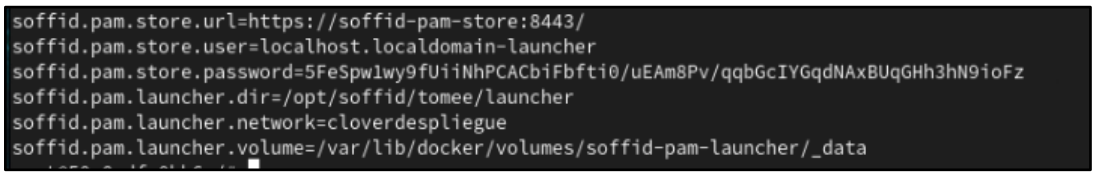


Ilustración 3: Archivo de propiedades del PAM-launcher

94. Una vez realizados las acciones anteriores, se debe garantizar una comunicación segura entre los componentes del sistema mediante la definición de los certificados de los otros componentes como confiables. Para ello, se crea el directorio `/opt/soffid/tomee/trustedcerts/` en ambos contenedores, en caso de que no exista, y se copia en su interior el certificado de la CA que haya firmado los certificados de la consola, el PAM launcher y el PAM store.

95. Para definir el certificado del sync-server como confiable, ejecutamos el siguiente comando desde el directorio `/opt/soffid/tomee/trustedcerts/` de ambos contenedores:

```
openssl s_client -connect iam-sync:1760 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > iam-sync.crt
```

96. A continuación, debe importarse el certificado en el almacén de claves del launcher. Para ello, se ejecuta el siguiente comando en el mismo directorio:

```
keytool -import -file iam-sync.crt -keystore cacerts -alias iam-sync
```

97. Después de realizar las modificaciones en ambos archivos, se deben reiniciar los contenedores ejecutando docker restart soffid-pam-launcher soffid-pam-store.

98. Finalmente, para registrar los servidores PAM en la consola, es necesario crear un nuevo usuario en el PAM Store. Para ello, ejecutamos el siguiente comando:

```
docker exec soffid-pam-store /opt/soffid/tomee/bin/add-user.sh $(hostname)-launcher console
```

99. Accedemos a la Consola (https://localhost:8443) y navegamos hasta la siguiente ruta:

```
Menú principal > Administración > Configurar Soffid > Configuraciones de Seguridad > Configurar servidores de sesión PAM
```

100. A continuación, hacemos click en el icono “+” en la parte inferior derecha de la tabla para acceder al formulario para añadir un nuevo servidor e introducimos los siguientes datos:

CAMPO	CONTENIDO
Nombre del grupo	A decisión del usuario
Descripción	A decisión del usuario
Nombre de usuario	Salida del comando hostname
Contraseña	Contraseña que mostró el comando ejecutado en el paso anterior
URL	https://soffid-pam-store:8443
Servidores de salto	https://{nombre servidor}:8082

Tabla 4 Datos para el registro del servidor para PAM en la consola

101. Tras introducir estos datos, hacemos click en el botón “Aplicar Cambios” y se debería mostrar una nueva fila en la tabla de servidores de sesión PAM con el nombre, descripción y URL configurados.

6. FASE DE CONFIGURACIÓN

6.1 INICIALIZAR SOFFID

102. Para inicializar el producto *Soffid IAM*, será necesario arrancar el sistema CentOS (donde tenemos instalados los contenedores dockers y los componentes de *Soffid IAM)* e iniciar sesión.

103. Una vez dentro del sistema, debemos ejecutar secuencialmente los siguientes comandos para ir iniciando los procesos:

```
sudo systemctl start docker
sudo docker start mariadb-service iam-console iam-sync soffid-pam-launcher
soffid-pam-store
```

104. Los nombres de los contenedores se van imprimiendo por pantalla a medida que estos se van iniciando.

105. **Nota:** Si queremos comprobar que se han inicializado todos los contenedores correctamente escribimos (`sudo docker ps`), para comprobar el estado de los contenedores *Docker*.

106. Una vez esta todo inicializado, abrir el navegador y conectar al portal web en `https://localhost:8443`.

6.2 AUTENTICACIÓN

107. Para poder realizar cualquier función en *Soffid IAM*, los usuarios se deben autenticar en la interfaz gráfica de *Soffid* IAM a través del componente de la Consola.

108. Para poder acceder a la herramienta de la Consola de *Soffid IAM* se debe de iniciar sesión en la interfaz gráfica. Para ello, se debe escribir *IP:PORT* en el navegador, dónde "IP" es la dirección IP donde está corriendo la Consola web de *Soffid* IAM y "PORT" es el puerto que se haya especificado durante la instalación.

109. Una vez se introduzcan las credenciales, si las credenciales coinciden con las almacenadas en la base de datos, el usuario podrá realizar las funciones a las cuales tenga acceso y hayan sido habilitadas previamente por el administrador. Dichas funciones vendrán determinadas por el rol asociado al usuario.

110. El producto se despliega en un ambiente local, por lo que los dispositivos deben de estar conectados entre ellos.

111. A la hora de realizar la fase de instalación, se crea un primer usuario administrador el cual tiene acceso a todas las funcionalidades de *Soffid IAM*, este usuario administra y crea los demás usuarios. Cada una de las cuentas de usuarios que se crean son administradas por este perfil administrador, que es el que decide que permisos y funcionalidades tienen mediante la determinación de roles.

112. La creación de cuentas de usuario se puede realizar de manera manual por el administrador o mediante un proceso conciliador con un sistema ligado a *Soffid IAM*.

113. El proceso conciliador funciona de la siguiente manera: primero se crea un agente en *Soffid* IAM del sistema que se va a gestionar, una vez creado este agente, hacemos uso de la funcionalidad de proceso conciliador de *Soffid IAM*, el cual importa todas las cuentas

existentes en este sistema dentro de la base de datos de *Soffid IAM* (como nuevos usuarios). En el despliegue del producto, se ha usado *Active Directory* cómo agente para realizar este proceso de importación de usuarios, dicho proceso esta explicado en detalle en 8 ANEXO 1: CONFIGURACIÓN DEL AGENTE DE ACTIVE DIRECTORY de este documento.

114. Los dos tipos de usuarios diferenciados en el sistema son los usuarios básicos y los usuarios administradores. Para poder diferenciar los permisos y atributos de los usuarios se utilizan roles, a saber:

    - Los usuarios administradores tienen un control completo del sistema y sobre los usuarios básicos, y tienen asociado el rol de administrador.
    - Los usuarios básicos tienen control mínimo sobre sus propias funcionalidades y podrían realizar una conexión PAM a un sistema si se les asigna el rol necesario de acceso a PAM para realizar dicha conexión.

115. Los usuarios básicos se pueden crear de dos maneras distintas: por un lado, pueden ser importados desde un Agente externo, en este caso *Active Directory* o, por otro, pueden ser creados de manera manual por parte del Administrador (Ver apartado 6.3.10).

116. Los usuarios básicos, por defecto, no tienen control sobre la administración de las funcionalidades de *Soffid IAM*. Para poder realizar actividades dentro de la aplicación deben de tener asociados los roles necesarios.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ACCESO A LA INTERFAZ DE ADMINISTRACIÓN

117. La administración del producto se lleva a cabo desde la interfaz gráfica de la herramienta mediante el componente de la Consola, a la que se accede desde el navegador de forma local escribiendo IP:PORT. Esta administración de la herramienta se lleva a cabo por parte de los administradores.

118. Para realizar las conexiones con la consola de herramienta se usa un protocolo de transferencia segura HTTPS (ver apartado 6.1 INICIALIZAR SOFFID para su configuración).

119. **Nota:** En caso de que al acceder a la ruta `Administración> Recursos > Cuentas` aparezca un error, se debe acceder a `Administración >Configurar Soffid > Ajustes Globales > Metadatos`, hacer click en "com.soffid.iam.api.Account" para editarlo y, desde la ventana de edición, hacer click en las tres líneas horizontales del menú y seleccionar "Establecer como predeterminado".

6.3.2 ELIMINACIÓN DE PLUGINS INNECESARIOS

120. Los *plugins* son componentes necesarios para poder crear y trabajar con agentes en los diferentes entornos de operación. En este caso, como solo vamos a trabajar con *Active Directory* como agente, debemos de eliminar todos los *plugins* innecesarios.

121. Accedemos a la funcionalidad: `Administración >Configurar Soffid > Ajustes Globales > Gestión de componentes`

122. Seleccionamos aquellos *plugins* a eliminar y hacemos click sobre el símbolo "menos".

123. Tras hacer click en "Ok" en el cuadro de diálogo de confirmación, se puede comprobar que los *plugins* eliminados ya no aparecen en la lista.

6.3.3 CREACIÓN DE ROLES

124. Dentro del sistema de *Soffid IAM* se pueden diferenciar tres roles: rol de usuario administrador, rol de usuario básico y rol de acceso a PAM.

125. El rol de usuario administrador viene ya creado por defecto con la instalación e inicialización de *Soffid IAM*, ya que el primer usuario que se crea durante la instalación del producto tiene asociado este rol. Este rol tiene control sobre todas las configuraciones de *Soffid IAM* y puede gestionar y administrar al resto de usuarios y sus roles.

126. El rol de usuario básico es el rol que se le asigna a todo el resto de los usuarios del sistema que no tengan permisos de administrador. Este rol de base puede acceder a la Consola web de *Soffid* IAM para consultar y realizar operaciones básicas. Dichas operaciones se explican con más en detalle en el apartado 7.2 de este documento.

127. Para crear el rol de usuario básico se deben de seguir los siguientes pasos:

- Se accede a la funcionalidad: `Administración > Recursos > Roles` y se hace click sobre el signo de "+" y se rellenan los campos siguiendo el ejemplo de la siguiente ilustración:

Ilustración 4: Rol de Usuario Básico

128. Tras hacer click sobre el botón "Aplicar Cambios", observaremos que el nuevo rol aparece en la lista de roles disponibles.

129. Una vez creado el rol, debemos asignarle las autorizaciones necesarias para que los usuarios básicos que tengan atribuidos este rol puedan realizar operaciones. Para ello:

- Se accede al directorio `Administración > Configurar Soffid > Configuraciones de seguridad > Autorizaciones`,

- Se asignan las autorizaciones que se muestran en la Ilustración 5 al rol de usuario básico que se ha creado previamente:

Ámbito	código	Descripción	Roles
Filter	Filter	Filter	u
Additional data	metadata:query	Query the additional data types	SOFFID_USER@soffid
Agents	agent:query	Query the agents configuration	SOFFID_USER@soffid
Custom objects	customObject:query	Query custom object types	SOFFID_USER@soffid
Custom objects	customObjectType:query	Query custom objects	SOFFID_USER@soffid
SelfService	selfservice:tasks	View my tasks	SOFFID_USER@soffid
SelfService	selfservice:directory	Browse corporate directory	SOFFID_USER@soffid
SelfService	sso:createSharedFolders	Create root shared folders	SOFFID_USER@soffid
SelfService	sso:createAccount	Create shared accounts using SSO	SOFFID_USER@soffid
SelfService	sso:manageAccounts	Manage shared accounts using self service	SOFFID_USER@soffid
SelfService	selfservice:search-process	Search current processes	SOFFID_USER@soffid
SelfService	selfservice:accounts	View my accounts	SOFFID_USER@soffid

Filas mostradas: 11

Ilustración 5: Autorizaciones para rol de Usuario Básico

- Para asignar una autorización a un rol, se hace click sobre la autorización y dentro de la autorización se hace click en el signo "+". Esto abre un panel de búsqueda, dentro del buscador se escribe el nombre del rol de usuario básico y le damos a "aceptar" para cerrar el buscador. Finalmente se deben de aplicar los cambios para que esta autorización tome efecto.

130. A continuación, se va a crear el rol de acceso a PAM. Este rol se crea para que los usuarios puedan realizar conexiones PAM con equipos externos sin necesidad de ser usuarios administradores. Este rol se debe de asignar, por un lado, a los usuarios básicos a los que se desee dar dichas funcionalidades, para que puedan acceder a los equipos externos que se desea, por otro lado, también se debe de asignar dicho rol dentro `Password Vault` a las carpetas donde tengamos almacenadas las máquinas a las que queramos dar acceso al usuario.

131. Creamos el rol de acceso a PAM siguiendo el ejemplo de la Ilustración 6:

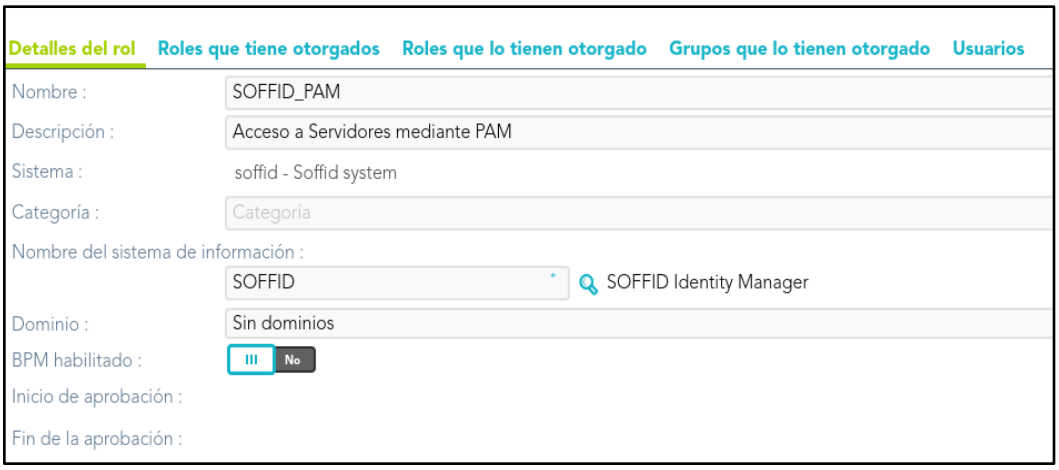


Ilustración 6: Rol de Acceso a PAM

132. A continuación, se deben realizar las asignaciones de las autorizaciones para este rol de acceso a PAM igual que hemos hecho con el rol de usuario básico. Para este rol solo debemos de asignarle la autorización de "selfservice:applications". Seguimos el mismo proceso que se ha explicado previamente.

6.3.4 ASIGNACIÓN DE ROLES

133. Para los distintos usuarios que se creen dentro del sistema, se deben de asignar los correspondientes roles dependiendo de las funcionalidades que se les quiera asignar a cada usuario.

134. Los usuarios están diferenciados entre usuarios básicos o usuarios administradores. A cada nuevo usuario del sistema se le deberá asignar correspondientemente el rol de usuarios administrador o el rol de usuario básico. Para hacer esto se deben de seguir los siguientes pasos.

135. Para asignar un rol a un usuario se accede a la siguiente funcionalidad: `Administración > Recursos > Usuario` y seleccionamos el usuario. Dentro del usuario, nos desplazamos a la ventana de Roles y hacemos click sobre el "+", elegimos el rol correspondiente y guardamos los cambios realizados. El nuevo rol aparece en la lista de Roles del usuario.

136. Podemos también asignar el rol de acceso a PAM a un usuario básico, este rol es específico y se debe de asignar a los usuarios a los cuales se les quiera permitir acceder a un equipo mediante el uso del PAM.

137. Para asignar el acceso a una máquina, se deberá de añadir dicho rol al usuario indicado (de la misma forma que se ha explicado anteriormente) y dentro de las máquinas administradas mediante PAM, asignar dicho rol a la carpeta donde se encuentre la máquina a la cual se le quiere dar acceso al usuario, las máquinas administradas por *Soffid* IAM se encuentran en la dirección de Administración > Recursos > Password Vault.

138. Cada carpeta del Password Vault tiene una lista de control de acceso en la que se puede indicar que Roles, Grupos y/o usuarios tienen acceso a esta carpeta. Para que las cuentas que cuelgan de esta carpeta tengan esta misma lista de control de acceso se debe indicar marcando el check de Herederar nuevos permisos o asignando a cada cuenta su propia lista de control de acceso.

6.3.5 POLÍTICA DE CONTRASEÑAS

139. Para configurar una política de contraseñas segura se deben seguir estos pasos:

- Autenticarse en la consola IAM como administrador.
- Dirigirse a `Menú principal > Administración > Configurar Soffid > Configuraciones de seguridad > Políticas de contraseña`
- Aplicar la política de contraseñas que cumpla con las siguientes directrices a las políticas por defecto:
  - Longitud mínima y máxima de la contraseña. Se deberá configurar una longitud mínima de 15 caracteres.
  - Complejidad. Las contraseñas deberán estar compuestas por una mezcla (al menos uno de cada) de mayúsculas, minúsculas, números y caracteres especiales ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")").
  - Validez de la contraseña. El valor recomendado para la vigencia y expiración de contraseñas es de 30 días.
  - Histórico de contraseñas. No deberá permitirse la repetición de al menos las 10 últimas contraseñas utilizadas.
  - Máximo número de intentos fallidos de autenticación. Se deberá configurar el bloqueo de las cuentas al introducir, como máximo, 3 intentos erróneos. En caso de

superar el número máximo de intentos fallidos la cuenta quedará bloqueada 20 segundos.

140. Una vez se ha establecido la configuración, hacer click en “Aplicar cambios”. El sistema muestra de nuevo la lista de políticas de contraseñas activas.

6.3.6 CONFIGURACIÓN DEL BANNER

141. Antes de realizar un inicio de sesión, se debe de configurar el sistema para que despliegue un mensaje de advertencia al usuario que está intentando realizar el inicio de sesión.

142. Para configurar dicho mensaje de seguridad, o banner, se accede a la siguiente funcionalidad: `Administración > Configurar Soffid > Configuraciones de seguridad > Autenticación.` Dentro de esta dirección, en la sección de `Global Status` se debe escribir en el cuadrado de texto el mensaje de advertencia correspondiente para nuestro sistema.

143. Una vez escrito, se debe hacer click en “Aceptar” para cerrar el editor y en “Aplicar cambios” para que el cambio surta efecto. Si se vuelve a hacer click en “Autenticación”, se muestra el mensaje configurado en Global Status.

6.3.7 GESTIÓN DE CERTIFICADOS

144. Los certificados que se usan para garantizar una conexión segura HTTPS entre los diferentes componentes del sistema son proporcionados por una CA reconocida, salvo para el certificado que se utiliza para realizar la conexión entre la Consola y el Sync-server, este certificado se autogenera a la hora de realizar la instalación de *Soffid* IAM y es incluido en el volumen de certificados aceptados por los componentes.

145. Este certificado autofirmado, es incluido como parte de los certificados aceptados y debe de mantenerse así durante la vida del producto. Para garantizar esto, cuando el certificado vaya a caducar, se realiza el siguiente proceso de renovación:

    - Cuando quedan 45 días para la expiración del certificado, se autogenera un nuevo certificado autofirmado.
    - Cuando quedan 15 días para la expiración del certificado, las claves de este nuevo certificado que se ha autogenerado son enviadas al volumen de claves públicas aceptadas del sistema, por lo tanto, la aplicación aceptará las claves de ambos certificados, el sistema esperará a ser reiniciado para poder eliminar el certificado antiguo y así solo aceptar el nuevo. En caso de no ser reiniciado de manera manual durante este periodo de 15 días, el último día a las 00:00 se reiniciará de manera automática y borrará el certificado antiguo junto a sus claves, dejando solo el nuevo certificado. Este proceso se repetirá de manera automática durante el periodo de vida del producto.

146. El resto de los certificados obtenidos de la CA se guardan en los volúmenes y contenedores *Docker* correspondientes para garantizar una conexión segura entre los componentes. Este almacenamiento y distribución de los certificados ha sido explicado en más detalle en apartados de Instalación y Configuración previos.

147. *Soffid IAM*, para la configuración del protocolo de comunicación HTTPS, debe proporcionar las siguientes suites criptográficas:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

148. El cifrado que se usa para las contraseñas es RSA_OEAP de 3072 bits.

6.3.8 ACTUALIZACIONES

149. Primero, se debe comprobar que la actualización para el componente que se desea actualizar ha sido publicada para su uso. Una vez sepamos cuál es el número de versión de la nueva actualización, eliminamos los contenedores actuales ejecutando el comando `docker rm {nombre del contenedor}`, y repetimos los pasos del apartado 5 de este documento, modificando los números de versión por los nuevos.

150. **Nota**: En caso de que se vaya a actualizar el componente de la base de datos, se recomienda encarecidamente realizar un backup previamente para no perder ninguna información (ver sección 6.5.1).

151. Una vez realizados estos cambios y desplegados los contenedores, tendremos actualizada la nueva versión para nuestro componente.

152. **Nota**: Las nuevas actualizaciones se deben comprobar de forma manual y realizarse cuando sea oportuno. No hay ninguna notificación por parte de *Soffid IAM* para realizar estas actualizaciones.

153. **Nota**: Se deberán hacer las mismas comprobaciones que para la instalación original (Ver sección 4.1)

6.3.9 IMPORTAR Y ADMINISTRAR USUARIOS

154. En esta sección se explican los pasos a seguir por parte de los administradores para crear y administrar de forma segura los usuarios de *Soffid IAM* del agente usado *Active Directory*.

155. El primer paso es la configuración de los tipos de usuarios de *Soffid IAM*. El único tipo de usuario que se va a crear es el de "internal user" y servirá solo para identificarlo cómo usuario interno de Soffid IAM, cómo se muestra en la Ilustración 7. Para consultar o añadir algún tipo de usuario adicional será necesario acceder a: `Administración >Configurar Soffid > Ajustes Globales> Tipos de usuario`.

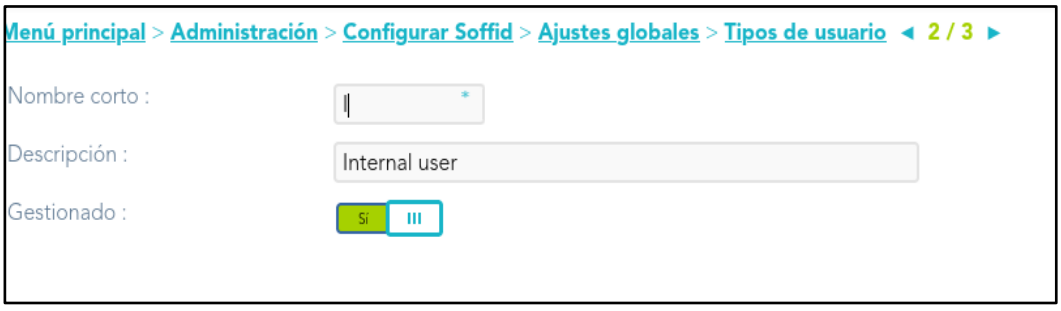


Ilustración 7: Usuario Interno de Soffid IAM

156. Se deberá configurar la política de contraseñas para cada uno de los tipos de usuarios existentes, para ello acceder a: `Administración >Configurar Soffid >`

`Configuración de seguridad > Políticas de contraseñas`, y configurar cada tipo de usuario siguiendo la política de contraseñas establecida en el apartado 6.3.5 de este documento.

157. Desplazarse a: `Administración >Configurar Soffid > Motor de integración >Regla de nomenclatura de cuentas`, donde se va a definir los nombres de las cuentas cuando se creen en *Soffid IAM*. Por defecto existe un dominio principal, pero se puede modificar el script para cambiar la nomenclatura de dichas cuentas. Esto puede ser necesario para ajustar la nomenclatura de *Soffid IAM* a la de los agentes de *Active Directory* que conectemos.

158. A continuación, nos desplazamos a `Administración >Configurar Soffid > Motor de integración > Agentes`, desde aquí se pueden configurar los diferentes sistemas que queremos enlazar con *Soffid IAM,* siguiendo los pasos que aparecen en la interfaz (en la sección 8 ANEXO 1: CONFIGURACIÓN DEL AGENTE DE ACTIVE DIRECTORY se explica cómo enlazar un sistema de *Active Directory*). Si queremos que el agente funcione como fuente autoritativa de datos, es decir, que importe todos sus usuarios a Soffid IAM, debemos marcar las opciones de: `Fuente autoritativa de datos` y `creación manual de cuentas.`

159. Una vez creados los usuarios en el sistema, se les deberá asignar de manera local el rol adecuado a cada nuevo usuario siguiendo los pasos especificados en el apartado 6.3.4.

160. Los usuarios básicos a los que se les asigne dicho rol, se les deberá de introducir la contraseña inicial que deberán usar en el primer inicio de sesión en la Consola web de *Soffid IAM.*

161. Esta asignación se realiza por parte de un usuario administrador para cada usuario básico después de haberle asignado el rol de usuario básico, para hacer esto se debe acceder al directorio de `Cuentas` del usuario básico, dentro de este directorio se debe de hacer click en `Cambio de contraseña` e introducir la nueva contraseña.

6.3.10 CREAR USUARIOS MANUALMENTE

162. Para crear usuarios manualmente, se accede a `Administración > Recursos > Usuarios` y se hace click en el símbolo “+”.

163. Aparece una ventana con múltiples pestañas. En la de “Información Básica” es necesario indicar, como mínimo: el código o identificador, el nombre de pila, un apellido, tipo de usuario y grupo primario del nuevo usuario. Además, es necesario marcar el usuario como “Activo” en el apartado “Estatus de usuario”.

164. En caso de que se quiera asociar el nuevo usuario a algún grupo, el siguiente paso es acceder a la pestaña “Grupos” y hacer click en el símbolo “+” para después buscar el grupo o grupos que quieran asociarse al usuario.

165. A continuación, es necesario asociar el usuario a la cuenta de *Soffid IAM* para que este pueda acceder. Para ello, se accede a la pestaña “Cuentas” y se hace click en el símbolo “+”. Posteriormente, se selecciona el sistema de destino Soffid, la cuenta con el mismo nombre que el código del usuario y el estado activado. Se hace click en aplicar cambios y la nueva cuenta aparece en la lista de cuentas del usuario. Opcionalmente, se puede establecer una nueva contraseña para el usuario haciendo click en el botón “Cambio de contraseña” en esta misma pestaña.

166. Finalmente, si se vuelve a navegar a `Administración > Recursos > Usuarios`, se puede comprobar que el nuevo usuario ha sido creado.

6.3.11 CONFIGURACIÓN DEL PERIODO DE INACTIVIDAD

167. Para configurar el tiempo de inactividad, en primer lugar se accede a `Administración > Configurar Soffid > Configuraciones de seguridad > Autenticación`.

168. A continuación, en el apartado "Periodo de inactividad", se debe configurar dicho tiempo en 1 minuto. Una vez transcurrido este periodo, se mostrará un mensaje al usuario y la sesión se cerrará si no hay ninguna interacción durante el minuto siguiente.

6.4 AUDITORÍA

6.4.1 REGISTRO DE EVENTOS

169. Dentro de la herramienta *Soffid IAM* se realiza un registro de todos los eventos y operaciones que se llevan a cabo durante su uso. Se registran tanto los eventos de configuración, cómo los eventos de operación de la aplicación con el uso de la herramienta PAM.

170. Los registros relacionados con la auditoria y configuraciones iniciales de *Soffid* IAM se almacenan en la base de datos *MariaDB* creada previamente, el resto de las acciones relacionadas con cada contenedor se almacenan en los propios contenedores.

171. Los registros para cada máquina se almacenan en cada uno de los contenedores, dependiendo del evento que se esté registrando. Para acceder a los logs almacenados, se puede hacer de dos formas:

    - Por un lado, se puede hacer desde la interfaz gráfica de *Soffid IAM,* dentro del directorio de `Administración > Monitorización e informes`, desde este directorio *Soffid IAM* nos permite acceder y consultar de forma ordenada todos los eventos y acciones que se han llevado a cabo en la aplicación.
    - Por otro lado, se puede acceder a los ficheros de logs a través de la línea de comandos, de esta forma podemos consultar todas las acciones llevadas a cabo en formato texto. Para poder acceder a estos logs, se debe de acceder a los contenedores donde se encuentran almacenados, esta acción solo la puede realizar un usuario administrador del sistema CentOS.

172. Para poder acceder a los ficheros de logs directamente, el usuario administrador de CentOS debe dirigirse a la dirección `/var/lib/docker/volumes/;` esta es la dirección local donde se almacenan los logs sobre los que están construidos los contenedores. Una vez dentro de esta dirección, se pueden ver los volúmenes para los diferentes contenedores que han sido creados, si se entra en cualquiera de los volúmenes, dentro del directorio `_data`, se pueden encontrar todos los logs almacenados de ese contenedor.

173. De todos los eventos se almacena el nombre del evento, el usuario que lo ha generado y la fecha y hora en las que ha tenido lugar. Adicionalmente, se almacena la siguiente información de los siguientes eventos:

EVENTO	CAMPO	DESCRIPCIÓN

Intento de autenticación	Nombre de usuario	Nombre del usuario que ha realizado el intento de autenticación
	Resultado	Aceptación o rechazo del intento de autenticación
Modificación o creación de información del usuario	Nombre de usuario	Nombre del usuario modificado
	Atributo	Identificador del atributo modificado
Creación de usuario	Nombre de usuario	Nombre del usuario creado
Bloqueo de cuenta por intentos de autenticación fallidos	Nombre de usuario	Identificador del usuario bloqueado
Desbloqueo de cuenta	Nombre de usuario	Identificador del usuario desbloqueado
Incumplimiento de la política de contraseña	Razón	Razón por la que se ha incumplido la política
Modificación de la política de contraseña	Atributo	Atributo modificado de la política de contraseña
	Valor previo	Valor del atributo previo al cambio
	Valor nuevo	Valor del atributo a consecuencia del cambio
Inicio de sesión PAM	url	URL del servidor destino de la sesión PAM
Asignación de permisos	Sujeto	Usuario, grupo o rol al que se asigna un permiso.
Configuración de un agente externo	Nombre	Nombre del agente
Registro de cuenta PAM	Parámetros	Parámetros de la cuenta configurados
Cierre de sesión	Usuario	Usuario cuya sesión se ha cerrado

Tabla 5: Información almacenada

6.4.2 ALMACENAMIENTO LOCAL

174. El almacenamiento del registro de eventos o *logs* se realiza de forma local.

175. Los logs correspondientes a las funcionalidades de la aplicación se almacenan en la base de datos *MariaDB.* Algunos ejemplos de logs que se almacenan en la base de datos son la información relativa a los datos de: creación de usuarios, asignación de permisos, integración con el *Active Directory*, etc.

176. Dentro de los archivos de los contenedores, se guardan los *logs* relativos a la depuración y gestión de sistemas.

6.5 BACKUP

177. La realización de backups se debe realizar de forma manual, *Soffid IAM* no cuenta con una funcionalidad dentro de la propia aplicación para realizar los backups correspondientes.

178. Teniendo en cuenta los componentes de *Soffid IAM* y las herramientas utilizadas en el despliegue de este producto, hay dos tipos de backups que podemos realizar.

6.5.1 BACKUPS DE LA BASE DE DATOS Y SU CIFRADO

6.5.1.1 REALIZACIÓN DEL BACKUP

179. Para poder realizar backups de la base de datos de *Soffid IAM* y cifrarlos, vamos a usar comandos propios de *Mysql.*

180. Los siguientes comandos se ejecutan desde una terminal en el contenedor de `mariadb-service`. Para iniciarla, se ejecuta `docker exec –it mariadb-service bash`.

181. Primero se debe de realizar el backup de la base de datos, para hacer esto se puede usar la siguiente línea de comandos: `mariadb-dump –p ––databases {nombre de la base de datos} > {nombre de archivo .sql}`.

182. Cuando finalice la ejecución del comando, se puede comprobar que existe el archivo y no está vacío utilizando el comando `wc –c {nombre del archivo .sql}` y comprobando que el número que muestra es distinto de 0.

183. Una vez extraído el archivo *.sql* se debe de cifrar usando el algoritmo de encriptación AES-CBC-256. Para hacer esto primero se debe de crear una clave aleatoria y un vector de inicialización.

```
openssl rand –out clave.txt 32
openssl rand –out 16 | od -A n -t x1 | tr -d ‘ \n’>iv.txt
```

184. A continuación, se cifra el backup de la base de datos con los archivos creados:

```
openssl enc -aes-256-cbc -pbkdf2 -in {nombre del archivo .sql} -out {nombre del archivo cifrado} -pass file:clave.txt -iv $(cat iv.txt)
```

185. Una vez cifrado el archivo del backup se debe de eliminar de forma segura el archivo del backup sin cifrar (`dd if=/dev/urandom of=<deletefile.txt>`).

186. A continuación, se calcula el código de verificación HMAC-SHA256 del fichero cifrado, siguiendo el esquema “*encrypt-then-MAC*”. Para ello, se utiliza el siguiente comando:

```
openssl sha256 -mac HMAC -macopt hexkey:$(od -A n -t x1 clave.txt | tr -d ‘ \n’) {nombre del archivo cifrado} > {nombre del archivo de verificación}
```

187. Por último, se debe de asegurar que el archivo cifrado de la base de datos, así como los ficheros de clave, vector de inicialización y verificación HMAC, se almacenan en un lugar seguro externo al entorno de operación.

188. **Nota:** De esta misma forma, se pueden automatizar scripts con comandos de este tipo para realizar backups de la base de datos de manera automática.

6.5.1.2 RESTAURACIÓN DEL BACKUP

189. Para restaurar la copia de seguridad, se asume que se dispone de los ficheros de backup cifrado, verificación, clave y vector de inicialización generados en el apartado 6.5.1.1. De igual manera que en dicho apartado, la ejecución de comandos se realiza desde una terminal en el contenedor de ***mariadb***.

190. En primer lugar, se verifica la integridad y autenticidad del fichero cifrado calculando su HMAC y comparándolo con el que se almacenó previamente:

```
openssl sha256 -mac HMAC -macopt hexkey:$(od -A n -t x1 clave.txt | tr -d ' \n') backup_cifrado.sql | diff -s verificación.txt –
```

191. Tras ejecutar este comando, la terminal debería mostrar el mensaje "Files backup_cifrado.sql and – are identical". En caso de que no se muestre dicho mensaje, la verificación habría fallado y no se debería restaurar el backup.

192. Tras ejecutar este comando, el terminal debería mostrar el mensaje "`Files backup_cifrado.sql and – are identical`". En caso de que no se muestre dicho mensaje, la verificación habría fallado y no se debería restaurar el backup.

193. Después de la verificación, se descifra el archivo de backup utilizando el siguiente comando: `openssl enc -aes-256-cbc -pbkdf2 -in backup_cifrado.sql -out backup.sql -pass file:clave.txt -iv $(cat iv.txt)`

194. Tras descifrar el archivo de backup, se restaura la base de datos mediante el siguiente comando: `mysql --password=$MYSQL_ROOT_PASSWORD --user=miuser mibasededatos < backup.sql`

195. Finalmente, se borra el archivo de backup de manera segura (`dd if=/dev/urandom of=<deletefile.txt>`)

6.5.2 BACK UP DE CONFIGURACIÓN CON PORTAINER

196. Al usar una herramienta de gestión de contenedores cómo *Portainer.io*, se pueden realizar backups de las configuraciones de los volúmenes, imágenes y contenedores gestionados con ella, usando la funcionalidad de backup de la propia herramienta.

197. Una vez realizadas las configuraciones de los componentes en sus contenedores vamos a realizar un primer backup de dichos componentes y sus configuraciones.

198. Para descargar el archivo de backup de dichas configuraciones, se debe abrir la interfaz web de *Portainer.io* y dirigirse a la pestaña de `Ajustes`, al final de esta pestaña podemos ver la opción de `Descargar archivo Backup`. Antes de descargar este backup, debemos verificar que la opción de `Protección con contraseña` esta activada (de forma que el backup realizado se encuentre cifrado con dicha contraseña), en caso de no ser así habría que activarla. Una vez hecho esto, se debe de hacer click en `Descargar Backup`, y se descargará un archivo comprimido y cifrado con todas las configuraciones necesarias para restaurar los contenedores gestionados en *Portainer.io*.

6.6 FASE DE FINALIZACIÓN

199. Una vez terminados los procesos de instalación y configuración del sistema se debe de borrar el historial de la terminal. Para hacer esto se debe de escribir el comando `history -c` y posteriormente el comando `history -w` .

7. FASE DE OPERACIÓN

7.1 CONEXIONES REMOTAS CON PAM

200. Una vez realizados los pasos de instalación y configuración segura de los componentes del PAM, podemos añadir diferentes dispositivos a los que conectarse de forma remota.

201. *Soffid* IAM permite realizar conexiones remotas con dispositivos Windows, a través del protocolo *RDP*, con dispositivos Linux, a través de *SSH* y con bases de datos MySQL usando *JDBC* y el gestor de bases de datos de *DBeaver*.

202. Para hacer esto se deberá acceder a la siguiente dirección `Administración>Recursos>Password vault`, una vez allí, hacer click sobre una de las carpetas creadas y seleccionar la opción de `Crear una nueva cuenta`. Seguidamente introducir los datos de la maquina a la que nos queremos conectar.

203. **Nota:** Para crear una nueva carpeta, se debe de hacer click sobre el "+" que aparece abajo a la derecha. Se debe asegurar que en la sección ¨Usuarios de SSO¨ de forma que aparezcan otorgados los Grupos, Usuarios o Roles necesarios.

204. A continuación, se proporciona un ejemplo de una configuración para una conexión *SSH* a un equipo remoto, de IP 10.10.1.73, con nombre de usuario "kali".

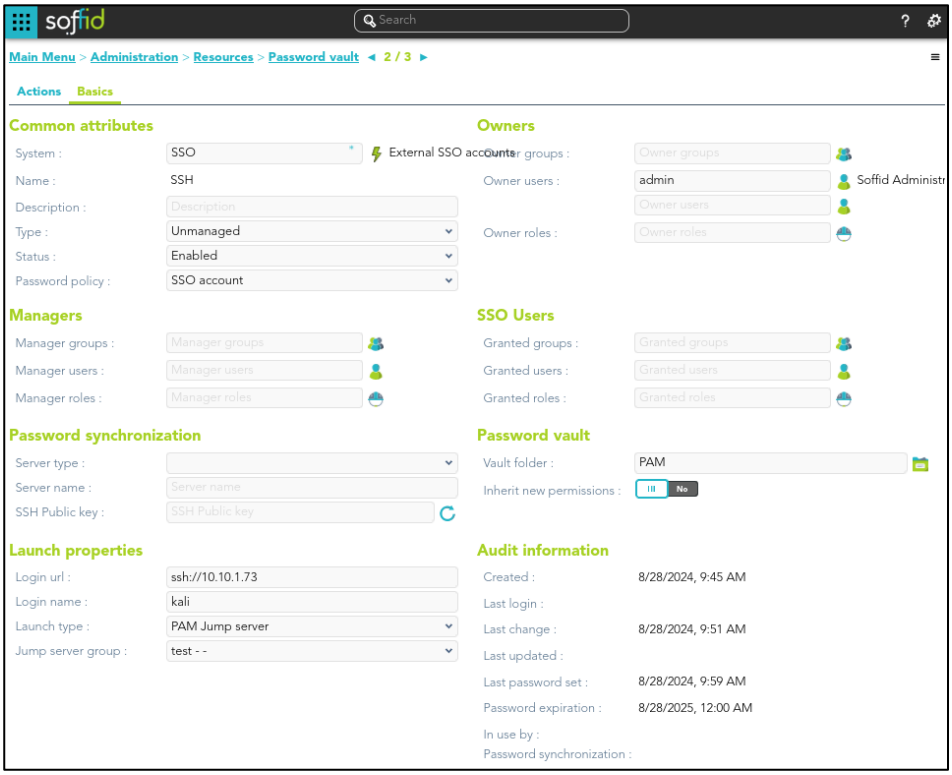


Ilustración 8: Ejemplo de conexión SSH

205. **Nota**: Como campos importantes a destacar y que deben de ser configurados como aparecen en la imagen anterior, son: `Tipo, Estado, Política de Contraseñas, Tipo de lanzamiento y Saltar grupo de servidores` (este último debe tener el nombre de la sesión PAM establecida).

206. **Nota**: Para las máquinas Windows se deberá escribir *RDP* al comienzo de la URL de inicio de sesión, para las máquinas Linux se deberá escribir *SSH* al comienzo de la URL de inicio de sesión, y para las bases de datos se deberá escribir *JDBC:://mysql://* al comienzo de la URL de inicio de sesión.

207. Una vez realizados estos cambios, se procederá a introducir la contraseña del equipo al que nos queremos conectar. Para ello, hacer doble click sobre la nueva cuenta que hemos creado y seleccionar la opción de `Ver Contraseña`, dentro de la pestaña que se abre, hacer click sobre `Establecer Ahora` y escribir la contraseña de inicio de sesión del equipo al que se quiere conectar.

208. Una vez proporcionada la contraseña, seleccionar la opción de `Lanzamiento` para comenzar la conexión de sesión remota.

209. Las acciones que se lleven a cabo durante la sesión remota quedarán grabadas en formato vídeo, y se podrán consultar accediendo a la siguiente dirección `Administración>Monitorización e informes>Buscar en grabaciones PAM`, en este directorio, estarán almacenadas todas las sesiones remotas que se han realizado. Se pueden realizar búsquedas y seleccionar sesiones por sus características. Haciendo doble click sobre una sección se podrán ver los detalles de dicha sesión, junto al vídeo correspondiente. Las grabaciones se almacenan por defecto dentro del contenedor del PAM-store un total de 90 días antes de ser eliminadas.

210. **Nota**: Los días de persistencia de los vídeos en el contenedor del PAM-store pueden ser modificados. Para establecer otro número de días de persistencia se debe acceder al directorio `/opt/soffid/tomee/bin` del contenedor PAM-store y ejecutar el script `purge.sh`, escribiendo el nuevo número de días de persistencia (`./purge.sh {X}`, dónde la X representa el nuevo número de días).

211. **Nota:** Con cada conexión PAM se creará un nuevo contenedor temporal, este contenedor registrará la conexión, y cuando este acabe, será eliminado, habiendo transmitido previamente los datos de la conexión al PAM-store.

7.2 OPERACIONES DE LOS USUARIOS BÁSICOS

212. Los usuarios básicos están divididos en dos: por un lado, tenemos los usuarios básicos que solamente tienen el rol de usuario básico, y por otro lado, tenemos los usuarios básicos que, además de este rol de usuario básico, también tienen el rol de acceso a PAM. Los usuarios con este último rol podrán acceder por PAM a los equipos que se les hayan permitido acceso, tal y como se ha explicado en el apartado 7.1.

7.2.1 USUARIOS BÁSICOS

213. Estos usuarios tienen el rol de usuario básico, cuyo proceso de asignación se explica en el apartado 6.3.4. Con este rol, el usuario puede acceder a la Consola web de *Soffid IAM* introduciendo el usuario y la contraseña asignada a dicho usuario por el administrador para realizar el primer inicio de sesión.

214. Después del primer inicio de sesión en la Consola web de *Soffid IAM,* el sistema obligará a dicho usuario a introducir una nueva contraseña siguiendo la política de contraseñas establecida.

215. Una vez establecida la nueva contraseña, aparece un diálogo confirmando el cambio de contraseña.

7.2.2 USUARIOS BÁSICOS CON ACCESO A PAM

216. Los usuarios básicos a los que se les hayan añadido también el rol de acceso a equipos por PAM, además de poder realizar las mismas operaciones que los usuarios básicos, también tienen acceso a `Mis Aplicaciones`, dentro de este directorio el usuario tiene compartida una carpeta desde donde se podrá acceder a las máquinas habilitadas para dicho usuario por parte del usuario administrador.

7.3 CERRAR SESIÓN EN SOFFID

217. Para cerrar la sesión en la Consola, se debe hacer click sobre la imagen de dos engranajes situada arriba a la derecha de la Consola, esto abre un menú que nos proporciona la opción de `Cerrar sesión`, si hacemos click sobre esta opción, se finalizará la sesión del usuario en la Consola y se volverá a la pantalla de Inicio de sesión de la Consola.

8. ANEXO 1: CONFIGURACIÓN DEL AGENTE DE ACTIVE DIRECTORY

218. Los plugins sirven para poder trabajar con agentes en diferentes entornos de aplicación, por lo tanto, si se quiere utilizar un agente se debe de instalar el plugin necesario para dicho agente. En el despliegue de este sistema hemos usado el agente de *Active Directory* para el funcionamiento de la aplicación.

219. En esta sección se va a explicar cómo enlazar un dominio de *Active Directory* con la herramienta de *Soffid IAM.* El plugin del Conector de Windows de *Active Directory*, viene instalado por defecto al realizar los pasos de la sección 5. Para realizar los pasos indicados a continuación se debe usar un usuario Administrador de *Soffid IAM.*

220. Se accede a la dirección `Administración > Configurar Soffid > Motor de integración > Agentes` y se hace click en el símbolo del "+" para añadir un nuevo Agente.

221. Se deben de rellenar los campos de configuración de la siguiente manera (los campos que no se incluyen a continuación se deben de dejar cómo aparecen por defecto):

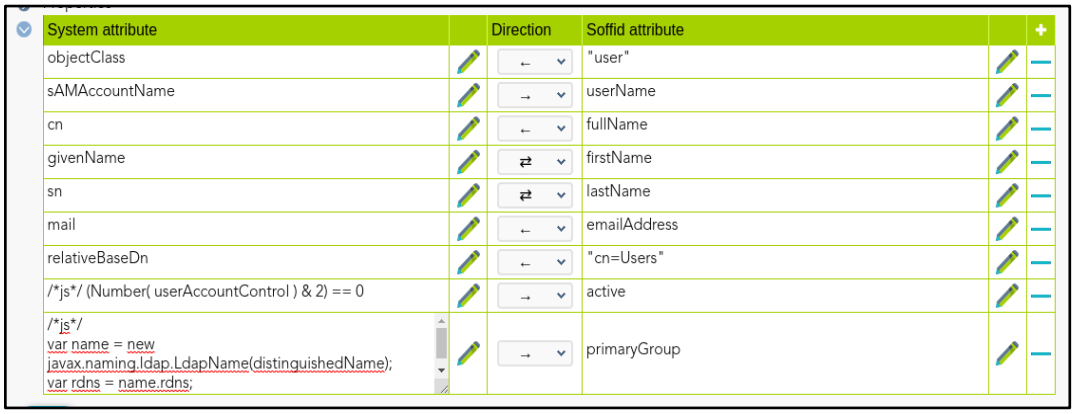
```
Código: Nombre del agente
Descripción: Breve descripción
Tipo: Active Directory
Servidor: iam-sync.{nombre_de_red}
Thread compartido: No Hilos compartidos: 1
Contraseña de confianza: Si
Fuente de identidad autorizada: Si
Solo lectura: No
Creación manual de cuentas: No
Basado en roles:No
Dominio de usuarios: Default user domain
Dominio de contraseñas: Default password domain
Tipo de usuario: Seleccionamos todos
Parámetros del agente:
Hostname: {Nombre_equipo}-SERVER.{nombre_del_dominio_ActiveDirectory}
LDAP base DN: dc=dominio de Active Directory ( domain controller)
Principal name = SOFFID/{usuario_administrador_ActiveDirectory}
Password={Contraseña_usuario}
Enable debugin: No
Accepted certificates: Any
Follow referrals: Don´t
Manage child domains: No
Create OUs when needed: Yes
Generate flat groups: Yes
Undelete deleted users: No
Real time load last login attribute: No
Real time load identity changes: No
```

222. Una vez se hayan completado los campos necesarios, se hace click sobre las barras horizontales situadas en la parte superior derecha de la pantalla, en el menú desplegable que aparece, se hace click en la opción de `?Prueba`, con esto debería aparecer un diálogo indicando "`La conexión es exitosa`".

223. Una vez realizados los pasos anteriores, se deben mapear los objetos que vamos a sincronizar entre *Soffid IAM* y el *Active Directory*. Para hacer esto, se accede a la ventana de `Asignación de atributos` y se hace click en el menú situado en la parte superior

derecha (el mismo que se ha empleado anteriormente), dentro del menú se selecciona `Create default mapping`.

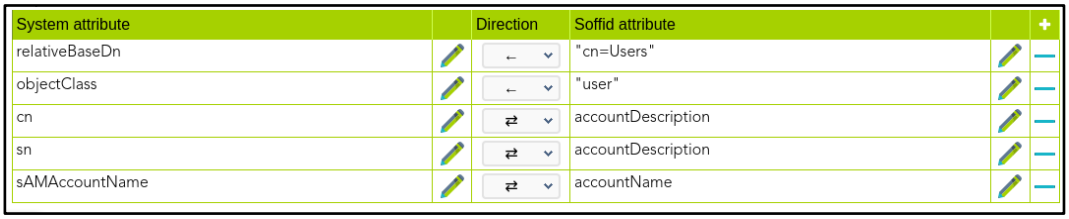
224. Dentro del apartado de User, se hace click sobre `attribute` y se deben crear (manualmente) los usuarios de *Active Directory* para posteriormente traerlos a *Soffid* IAM (mediante un *pull*), para hacer esto los campos de `Attribute` deben de ser iguales a los representados en la Ilustración 9.



System attribute		Direction	Soffid attribute		
objectClass		←	"user"		
sAMAccountName		→	userName		
cn		←	fullName		
givenName		⇄	firstName		
sn		⇄	lastName		
mail		←	emailAddress		
relativeBaseDn		←	"cn=Users"		
/*js*/ (Number(userAccountControl) & 2) == 0		→	active		
/*js*/ var name = new javax.naming.ldap.LdapName(distinguishedName); var rdns = name.rdns;		→	primaryGroup		

Ilustración 9 : Atributos de usuario AD Soffid

225. Dentro del apartado de Account, se hace click sobre `attribute` y se deben crear (manualmente) las cuentas de *Active Directory* para posteriormente traerlas a *Soffid* IAM (mediante un *pull*) y asociarlas al usuario correspondiente, para hacer esto los campos de `Attribute` deben de ser iguales a los representados en la Ilustración 10.



System attribute		Direction	Soffid attribute		
relativeBaseDn		←	"cn=Users"		
objectClass		←	"user"		
cn		⇄	accountDescription		
sn		⇄	accountDescription		
sAMAccountName		⇄	accountName		

Ilustración 10: Atributos de cuenta AD Soffid

226. Una vez hecho esto, accedemos a la sección de `Acciones masivas` y se hace click sobre `Cargar datos autorizados para identidades y grupos`, lo que hace esta opción es traer todos los usuarios desde *Active Directory* a *Soffid IAM,* al haber declarado el Agente del *Active Directory* cómo `fuente autoritativa`, esta operación crea todos los usuarios que existen en el *Active Directory* en *Soffid IAM.* Para consultar que estos usuarios han sido creados, se accede a: `Administración > Recursos > Usuarios.`

227. Si el agente que estamos usando no queremos que actúe cómo `fuente autoritativa`, no marcaremos esta opción en la configuración del Agente. Si no se marca esta opción, no se podrá realizar el paso 222 y solo se podrá realizar el paso 223 de asignación de cuentas a los usuarios.

228. A continuación, hay que ligar las cuentas del *Active Directory* con los usuarios de *Soffid IAM,* para hacer esto, se hace click sobre `Conciliar` y se selecciona `iam-sync.{nombre_de_red}`

229. **Nota:** El proceso de conciliación se debe lanzar siguiendo los parámetros de tiempo establecidos por la empresa, cada vez que se lance este proceso, se actualizarán las cuentas de dicho *Active Directory* sobre las cuentas de *Soffid IAM.*

230. A continuación, se debe acceder a `Administración > Recursos` y comprobar que las cuentas importadas han sido ligadas a los correspondientes usuarios, en caso de no ser así (las cuentas no están asociadas si el campo `Tipo` esta establecido cómo `No gestionado`), se debe cambiar el campo `Tipo` y ponerlo cómo `Usuario único`. En el campo de `Usuarios propietarios` se debe seleccionar el usuario de *Soffid* IAM propietario de dicha cuenta.

9. REFERENCIAS

[REF1] Guía de Seguridad de las TIC CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad – Mayo 2022

[REF2] CCN-STIC-610A22 GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX – Octubre 2022

[REF3] https://hub.docker.com/u/soffid

[REF4] https://hub.docker.com/layers/library/mariadb/11.1.2/images/sha256-e51c275914b2da5e8e8e0ed9eaecf1e4d5142b5e570f231224320001cf5c86cf

[REF5] https://hub.docker.com/layers/portainer/portainer-ce/2.16.2/images/sha256-a2938b24f6d1ea49db59866c4d7985e34c4cb78d8b468220b1a117bf616e421f

[REF6] https://docs.docker.com/engine/install/

10. ABREVIATURAS

AD	*Active Directory*
AES	*Advanced Encryption Standard*
CA	Certification Authority
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las TIC
ENS	Esquema Nacional de Seguridad
HMAC-SHA256	Hash-based Message Authentication Code using SHA-256
HTTPS	HyperText Transfer Protocol Secure
IAM	Identity and Access Management
IGA	*Identity Governance and Administration*
IM	Identity Management
IP	*Internet Protocol*
IRC	*Identity Risk Compliance*
JDBC	Java Database Connectivity
LDAPS	*Lightweight Directory Access Protocol*
NTP	Network Time Protocol
PAM	Privileged Access Management
RDP	Remote Desktop Protocol
RSA	*Rivest-Shamir-Adleman*
RSA_OEAP	Rivest-Shamir-Adleman Optimal Asymmetric Encryption Padding
SQL	*Structured Query Language*
SSH	*Secure shell*
SSL	*Secure Socket Layer*
SSO	Single Sign-On
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL