Aprovisionamiento de Usuarios

Manual de Usuario

Versión 4.39

Fecha de la versión 20/11/2024

Madrid, 20 de noviembre del 2024.

Elaborado por la Secretaría General de Administración Digital

© Ministerio de Asuntos Económicos y Transformación Digital

NIPO: Pendiente de asignación.

ÍNDICE

1. OBJETO 4

2. DESCRIPCIÓN 5

2.1. ACCESO 5

2.1.1.AUTENTICACIÓN 5

2.1.2.PERMISOS 6

2.1.3.NOTIFICACIONES PENDIENTES 7

2.2. BANDEJA DE ENTRADA 7

2.2.1.BANDEJA DE ENTRADA DE SOLICITUDES DE USUARIOS 8

2.2.2.BANDEJA DE ENTRADA DE SOLICITUDES DE AUTORIZACIÓN 12

2.3. USUARIOS 13

2.3.1.GESTIÓN DE USUARIOS 14

2.3.2.GESTIÓN DE GRUPOS DE USUARIO 23

2.3.3.GESTIÓN DE ATRIBUTOS DE VPN 25

2.3.4.CARGA MASIVA DE USUARIOS 27

2.4. APLICACIONES 29

2.4.1.ALTA DE APLICACIONES 29

2.4.2.MODIFICACIÓN DE APLICACIONES 41

2.4.3.BAJA DE APLICACIONES 45

2.4.4.CONSULTA DE APLICACIONES 47

2.4.5.CARGA CONFIGURACIÓN ACL 50

2.4.6.COPIA DE APLICACIÓN 50

2.5. AUTORIZACIÓN 52

2.5.1.GESTIÓN DE PERFILES 52

2.5.2.GESTIÓN DE ROLES 55

2.5.3.GESTIÓN DE APLICACIONES 57

2.5.4.AUTORIZACIÓN DE USUARIOS 63

2.5.5.CARGA MASIVA DE AUTORIZACIONES DE USUARIO 72

2.5.6.SINCRONIZACIÓN DIR3 74

2.5.7.BÚSQUEDA USUARIOS PERFIL 75

2.5.8.GESTIÓN DE GRUPOS 80

2.6. ADMINISTRACIÓN DEL SISTEMA 88

2.6.1.GESTIÓN 89

2.6.2.DOCUMENTACIÓN 127

2.6.3.SINCRONIZACIÓN DIR3 127

2.6.4.CONSULTA TRAZABILIDAD 129

2.6.5.CARGA MASIVA DE PERMISOS DE USUARIOS 137

2.6.6.CONSULTA Y ACTUALIZACIÓN DE USUARIOS EN EL LDAP 139
2.6.7.BÚSQUEDA DE USUARIOS POR ORGANISMO 144
2.6.8.ESTADÍSTICAS 146
2.7. HERRAMIENTAS 149
2.7.1.CREACIÓN DE BOTON CERRAR SESIÓN PERSONALIZADO 149
2.8. MIS DATOS 150

1. OBJETO

El objeto de este manual es el de servir como guía de referencia para el usuario del módulo de Aprovisionamiento de Usuarios dentro del Sistema de Repositorio Horizontal de Autenticación.

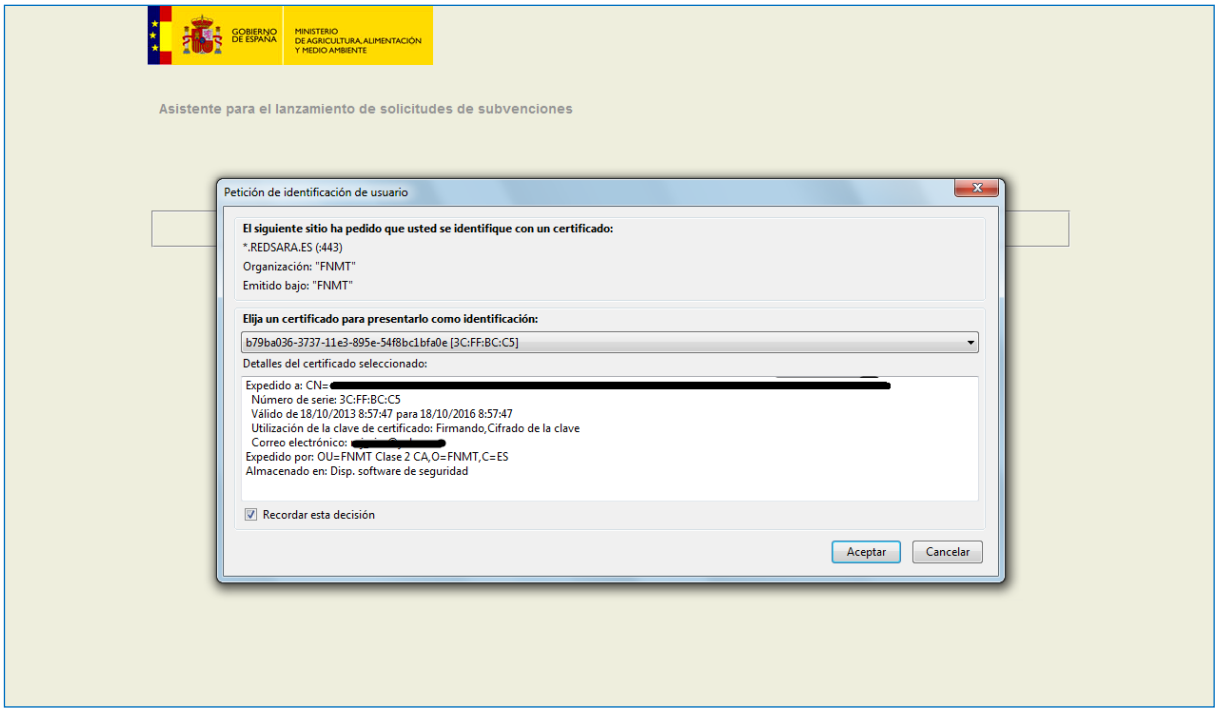
2. DESCRIPCIÓN

2.1. ACCESO

2.1.1. AUTENTICACIÓN

Para acceder al módulo de Aprovisionamiento de Usuarios será necesario autenticarse mediante la aplicación AutenticA. Hay dos modos de autenticación:

- Mediante certificado electrónico:



- Mediante usuario y contraseña:

2.1.2. PERMISOS

En las diferentes funcionalidades accesibles desde el módulo de aprovisionamiento de usuarios, es necesario tener un perfil determinado que te permita el acceso, ya que se deben tener permisos de administrador para acceder a ellas.

Existen dos tipos de administradores:

- *Administrador Central*: Tiene acceso a todas las funcionalidades y además puede realizar operaciones con cualquier usuario del repositorio horizontal de autenticación.
- *Administrador Delegado*: Puede tener asignado permiso de *Gestión de usuarios*, con el que únicamente tendrá acceso a las funcionalidades de la pestaña Usuarios, o/y permiso de *Autorización,* con el que únicamente tendrá acceso a las funcionalidades de la pestaña Autorización. Sólo puede realizar operaciones con usuarios que pertenezcan a su misma organización (nivel superior de la unidad orgánica). En las búsquedas sólo aparecerán usuarios de su organización y de igual manera no podrá modificar este nivel en la unidad orgánica.

  Existen 3 niveles de Administrador delegado para dar permisos a otros usuarios, de tal manera que pueda dar permisos iguales o inferiores a los suyos.

En los diferentes apartados correspondientes a cada funcionalidad, se indica qué tipo de perfil tiene acceso.

2.1.3. NOTIFICACIONES PENDIENTES

Si el usuario autenticado tiene notificaciones pendientes se muestra en todos los apartados de las funcionalidades un ícono de color azul en la cabecera indicando que tiene ficheros pendientes de descargar.

2.2. BANDEJA DE ENTRADA

Toda la gestión de solicitudes por parte de los administradores se hará a través de las opciones accesibles desde la pestaña “Bandeja de entrada”. Sólo tendrán acceso a esta pestaña los administradores (tanto central como delegado con permiso de bandeja de entrada de usuarios o de autorizaciones).

2.2.1. BANDEJA DE ENTRADA DE SOLICITUDES DE USUARIOS

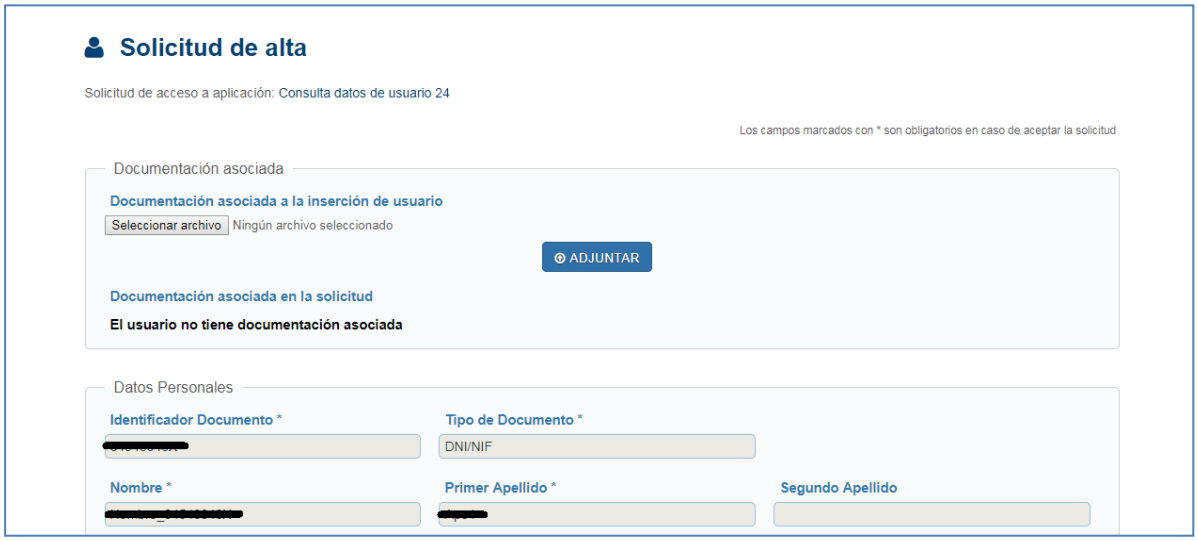
Una vez que se pulsa la opción de “Bandeja de entrada” se tienen las opciones de ver las solicitudes de alta y las solicitudes de modificación.

2.2.1.1. Solicitudes de alta.

Si se pulsa en “Solicitudes de alta” aparecerá un listado con aquellas solicitudes para el alta en el repositorio horizontal de autenticación que enviaron los usuarios (bien a través del autoregistro o bien que se enviaron mediante servicio web), encabezado por un filtro de búsqueda, para que se puedan acotar los resultados del listado, si se desea, por Aplicaciones o por Organismo.

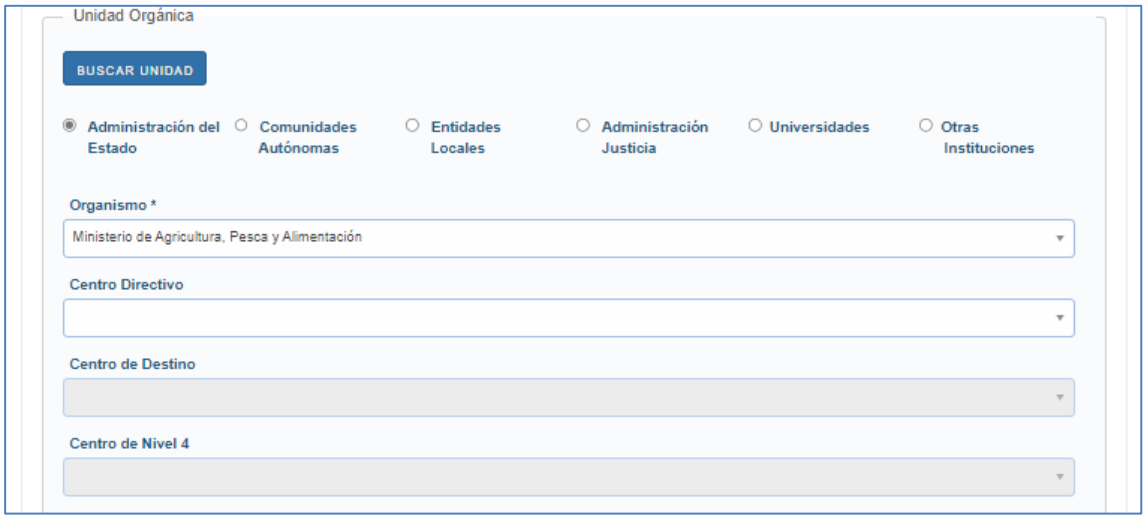
Cuando al lado del icono de Tipo aparece una bandera roja, significa que es una solicitud nueva desde la última conexión del administrador.

El administrador elegirá una de las solicitudes y aparecerá el formulario de detalle de la misma. El administrador con permiso para recibir correo de notificación de la solicitud, también podrá acceder a la pantalla de la solicitud de alta mediante el enlace de gestión de solicitud del correo de notificación de solicitudes pendientes, si la solicitud ha sido procesada se le mostrará una pantalla de información con los datos del usuario de la solicitud, del administrador que la procesó y la fecha en que se realizó.



El administrador estudiará los datos, podrá corregir aquellos relativos a la unidad orgánica así como completar la motivación y podrá adjuntar documentación, siempre que no supere un tamaño predeterminado establecido en el servidor y tenga extensión .doc, .docx ó .pdf.

En los datos relativos a la unidad orgánica, podrá buscar la unidad a corregir mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



El administrador podrá visualizar los datos de la ubicación asociada al usuario, en el cual se incluye el código del bien inmueble, la planta, la sala y el puesto físico del usuario.

Vendrá marcado por defecto el check ‘Incluir datos en EasyVista’, con el que se pasarán los datos del usuario a la BBDD de la citada aplicación, pero el administrador podrá desmarcar el check si lo requiere.

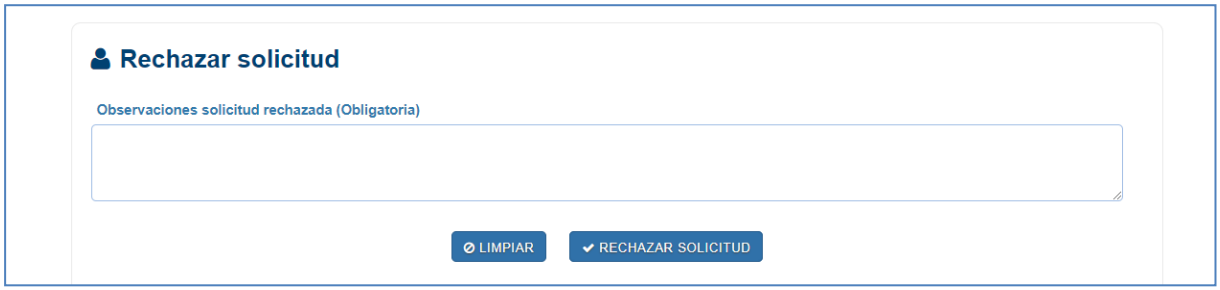
Finalmente aceptará, eliminará o rechazará la solicitud. En el caso de aceptarla o rechazarla se le enviará un email al solicitante con el resultado.

Puede darse el caso de que el usuario que se quiere dar de alta ya exista en Ldap como ciudadano. Si es así, al pasar al formulario de firma, se mostrará un mensaje indicando al

administrador que el usuario existía como ciudadano y al firmar la solicitud de alta será reemplazado por el nuevo usuario.

Si el administrador decide rechazarla o eliminarla, deberá rellenar el motivo del rechazo o eliminación en una pantalla específica para ello.

La diferencia entre la eliminación y el rechazo, es que si se elimina, se pierde totalmente la solicitud ya que se borra de la base de datos, mientras que si se rechaza, es un borrado lógico y permanece en la base de datos.



2.2.1.2. Solicitudes de modificación.

Si se pulsa en “Solicitudes de modificación” aparecerá un listado con aquellas solicitudes para la modificación de los datos en el Repositorio Horizontal de Autenticación que enviaron los usuarios (bien a través de la opción de modificación de datos o bien a través de servicio web), encabezado por un filtro de búsqueda, para que se puedan acotar los resultados del listado, si se desea, por Aplicaciones o por Organismo.

El administrador elegirá una de las solicitudes y aparecerá el formulario de detalle de la misma. El administrador con permiso para recibir correo de notificación de la solicitud, también podrá acceder a la pantalla de la solicitud de modificación mediante el enlace de gestión de solicitud del correo de notificación de solicitudes pendientes, si la solicitud ha sido

procesada se le mostrará una pantalla de información con los datos del usuario de la solicitud, del administrador que la procesó y la fecha en que se realizó.

En la columna de la izquierda aparecen los datos actuales del usuario. En la de la derecha los datos tal y como quedarán si se acepta la modificación propuesta. El administrador estudiará los datos, podrá corregir aquellos relativos a la unidad orgánica y la motivación (siempre de la segunda columna) y podrá visualizar la documentación adjuntada y modificarla, siempre que no supere un tamaño predeterminado establecido en el servidor y tenga extensión .doc, .docx ó .pdf; además, podrá visualizar los datos de la ubicación asociada al usuario, en el cual se incluye el código del bien inmueble, la planta, la sala y el puesto físico del usuario.

En los datos relativos a la unidad orgánica, podrá buscar la unidad a corregir mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Finalmente aceptará, eliminará o rechazará la solicitud. En el caso de aceptarla o rechazarla se le enviará un email al solicitante con el resultado. Si el administrador decide rechazarla o eliminarla, podrá rellenar el motivo del rechazo en una pantalla específica para ello, tal como ocurría en la solicitud de alta.

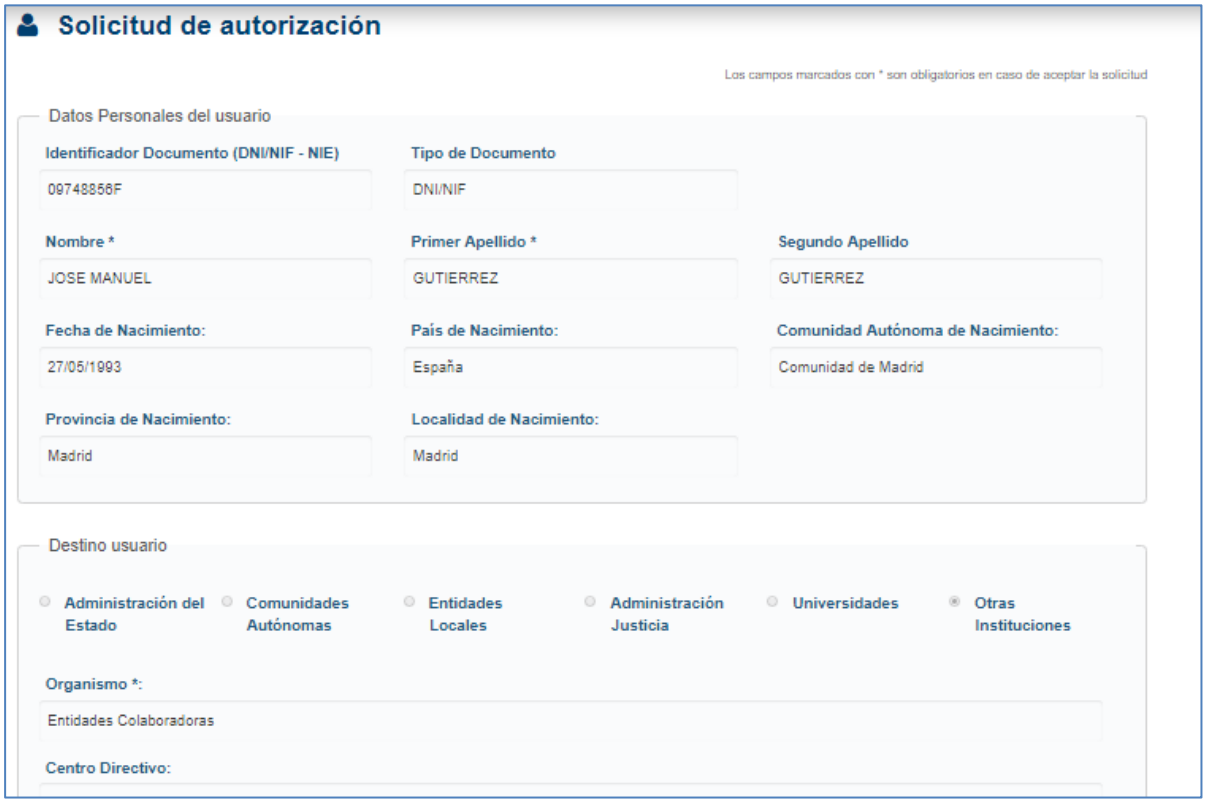
2.2.2. BANDEJA DE ENTRADA DE SOLICITUDES DE AUTORIZACIÓN

Una vez que se pulsa la opción de “Bandeja de entrada” se tienen las opciones de ver las solicitudes de autorización.

2.2.2.1. Solicitudes de autorización.

Si se pulsa en “Solicitudes de autorización” aparecerá un listado con aquellas solicitudes de autorizaciones en el repositorio horizontal de autenticación que enviaron los usuarios, encabezado por un filtro de búsqueda, para que se puedan acotar los resultados del listado, si se desea, por Aplicaciones o por Organismo.

El administrador elegirá una de las solicitudes y aparecerá el formulario de detalle de la misma. El administrador con permiso para recibir correo de notificación de la solicitud, también podrá acceder a la pantalla de la solicitud de autorización mediante el enlace de gestión de solicitud del correo de notificación de solicitudes pendientes, si la solicitud ha sido procesada se le mostrará una pantalla de información con los datos del usuario de la solicitud, del administrador que la procesó y la fecha en que se realizó.



El administrador estudiará los datos, podrá modificarlos-crearlos-eliminarlos manualmente mediante el botón que se encuentra en la parte inferior de la página llamado “ir autorización del usuario”.

Finalmente aceptará o rechazará la solicitud. En el caso de aceptarla o rechazarla se le enviará un email al solicitante con el resultado.

Si el administrador decide rechazarla, deberá rellenar el motivo del rechazo o eliminación en una pantalla específica para ello.

2.3. USUARIOS

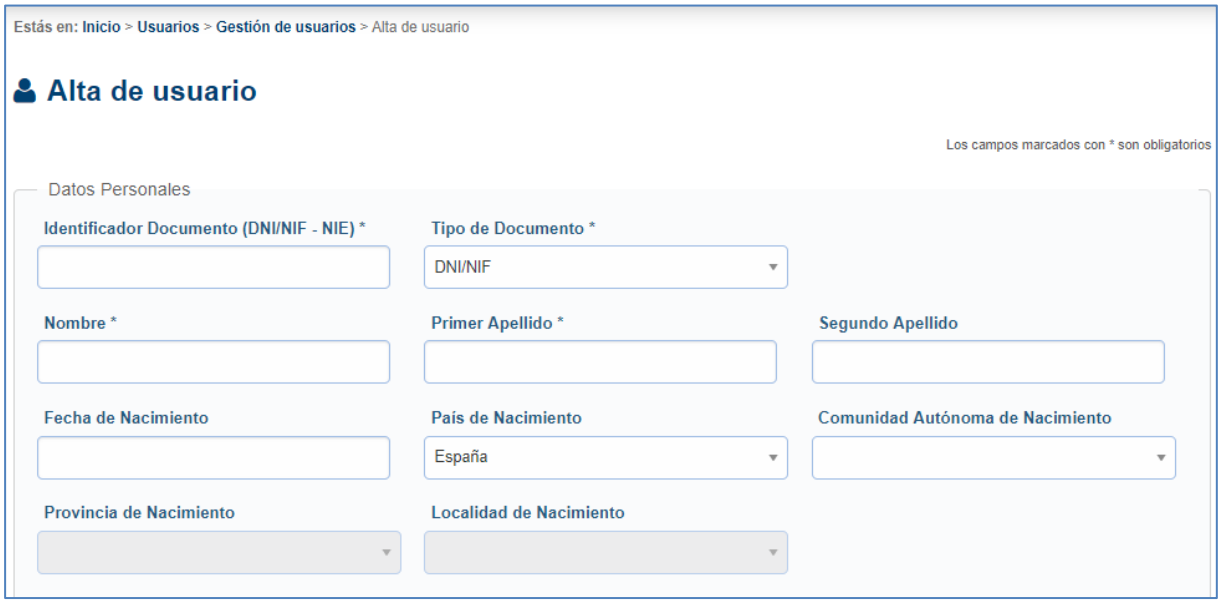
Toda la gestión de usuarios por parte de los administradores se hará a través de las opciones accesibles desde la pestaña “Usuarios”. Sólo tendrán acceso a esta pestaña los administradores (tanto central como delegado con permiso de gestión de usuarios).

2.3.1. GESTIÓN DE USUARIOS

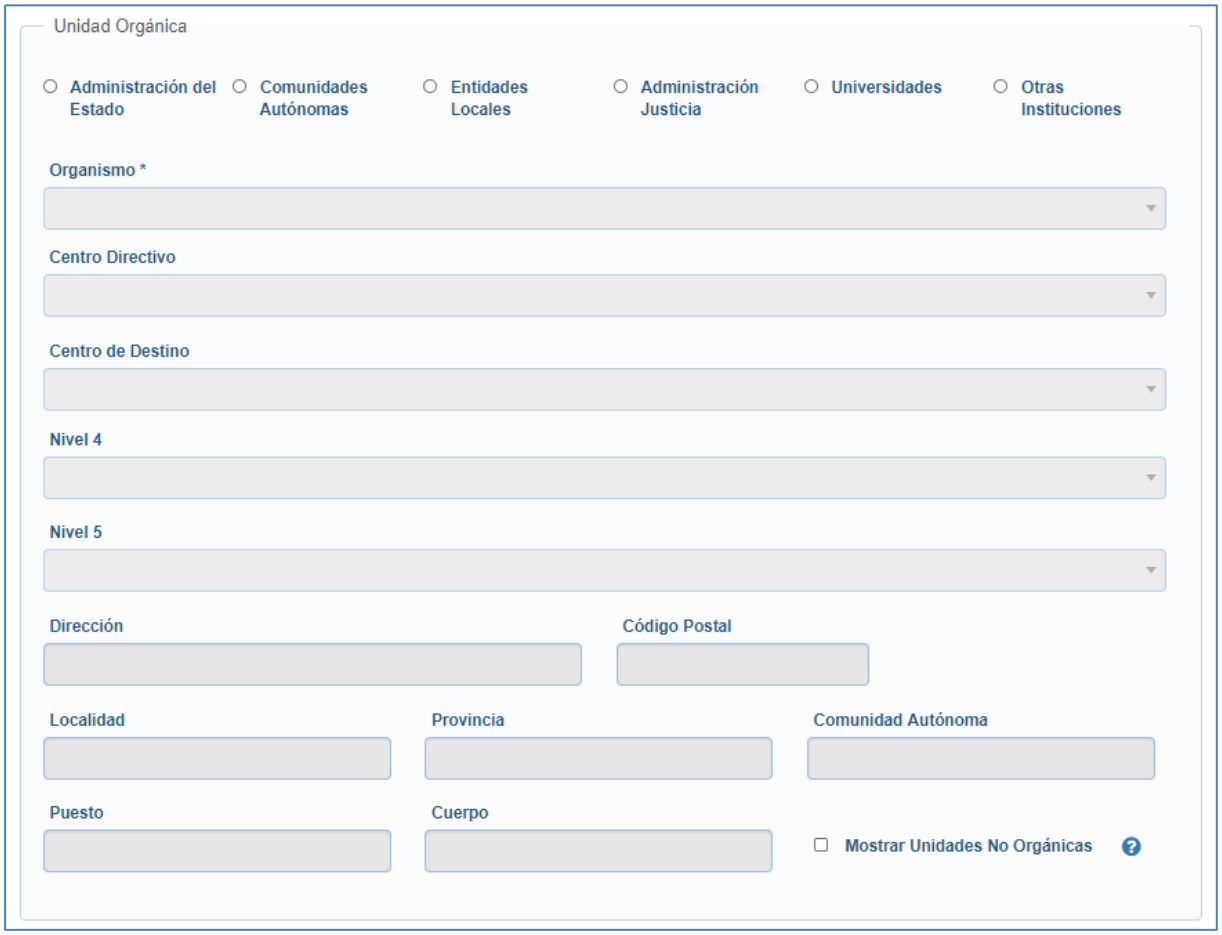
Una vez que se pulsa desde la pestaña “Usuarios” la opción de “Gestión de Usuarios” se tienen las opciones de “Alta de usuario”, “Mantenimiento de usuarios”, “Desbloqueo de usuarios” y “Simulación de XML respuesta de usuario”.

2.3.1.1. Alta de usuario.

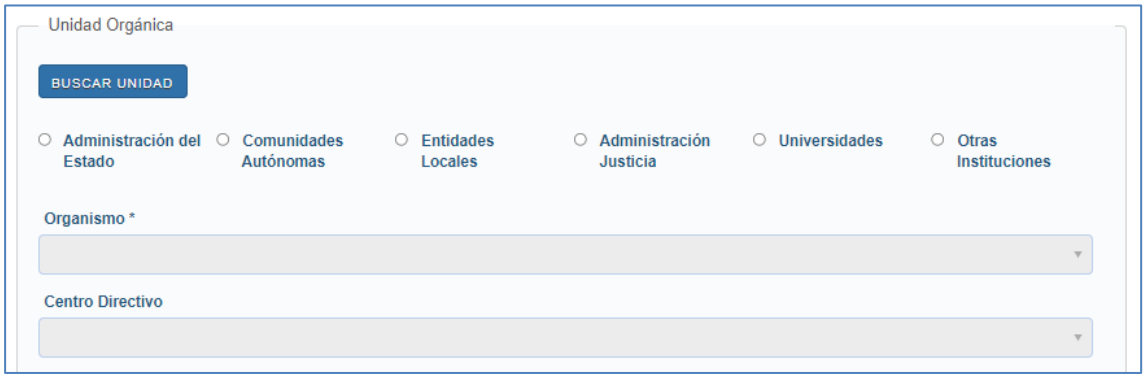
Eligiendo esta opción se mostrará el formulario de alta, que deberá cumplimentar un administrador.



Se podrá seleccionar la unidad orgánica correspondiente incluyendo el campo “Cuerpo”.

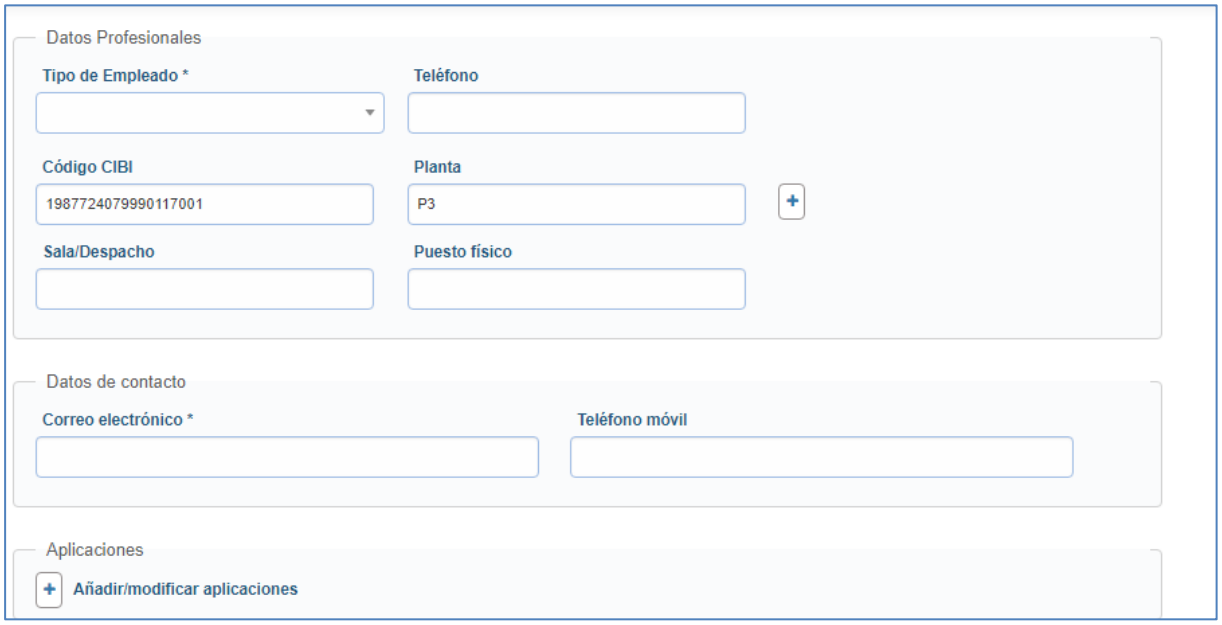


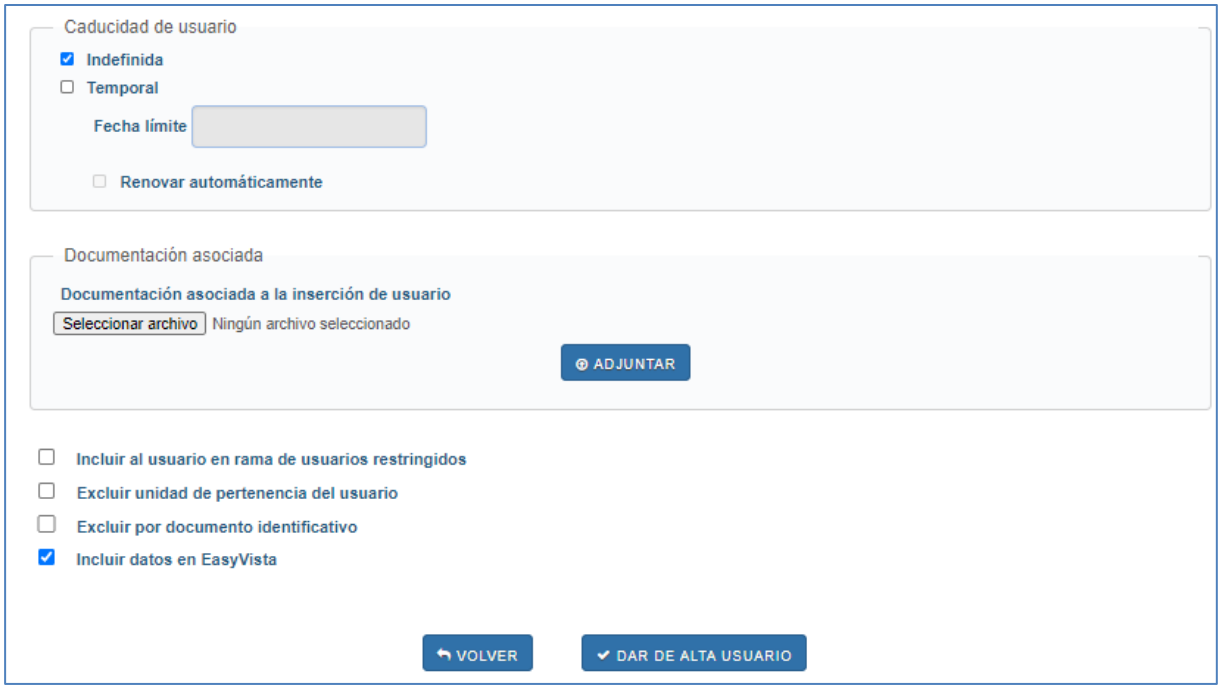
En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



En la parte inferior de la pantalla, se podrá adjuntar documentación, siempre que no supere un tamaño predeterminado establecido en el servidor y tenga extensión .doc, .docx ó .pdf

Un usuario podrá añadir código CIBI y planta en la parte de datos profesionales. Para ello, existe un botón con el icono de un más, al pulsarse saldrá un modal con un buscador para ayudar a la búsqueda. Otros datos relevantes que se pueden añadir son sala y puesto físico.

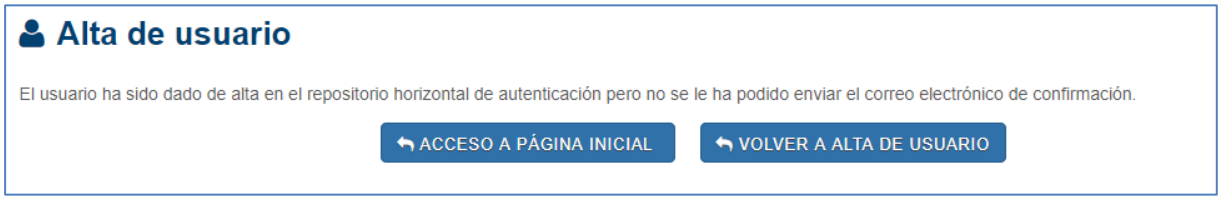




Puede darse el caso de que el usuario que se quiere dar de alta ya exista en Ldap como ciudadano. Si es así, al pasar al formulario de firma, se mostrará un mensaje indicando al administrador que el usuario existía como ciudadano y al firmar el alta será reemplazado por el nuevo usuario.

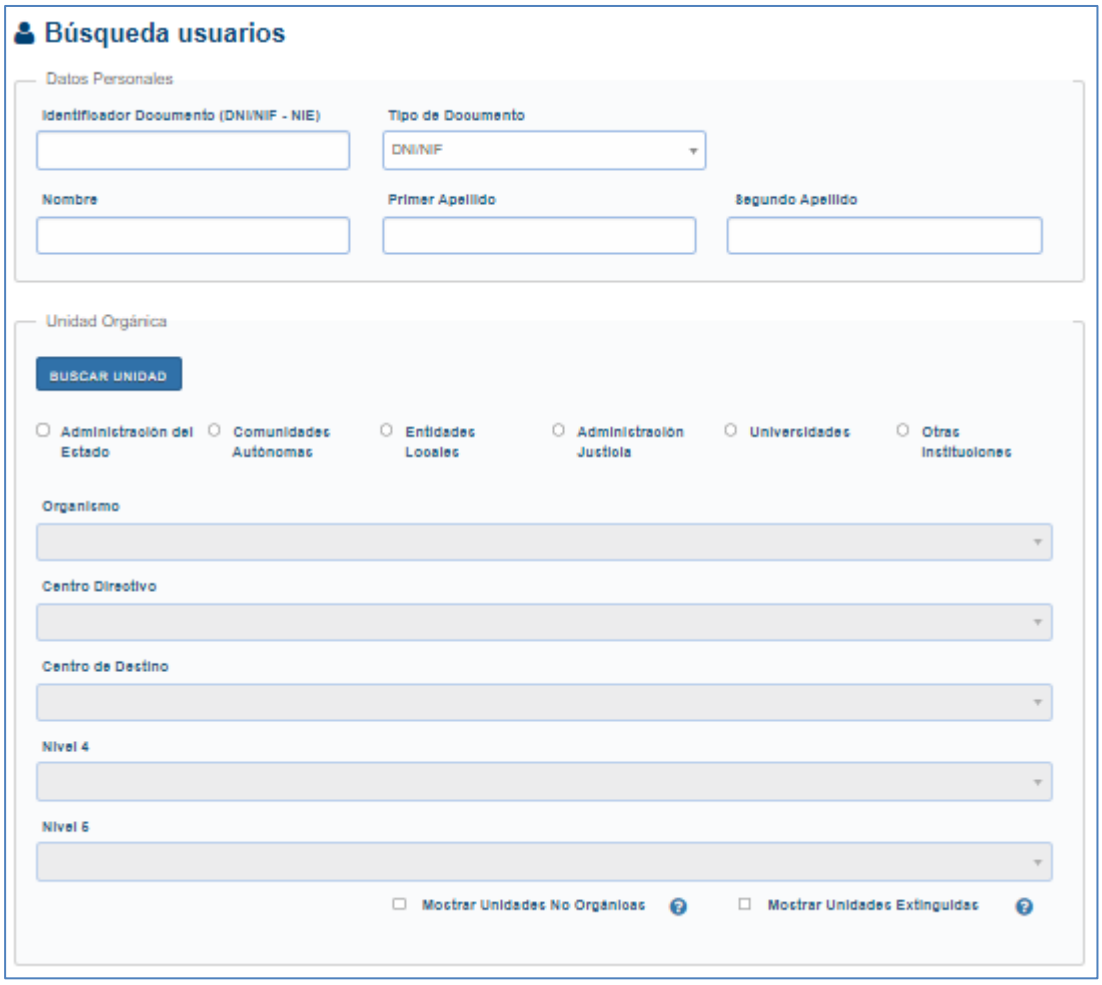
La opción ‘Caducidad de usuario’ al final del formulario, permite al administrador asignar una fecha límite en que el usuario ya no podrá acceder a la aplicación.

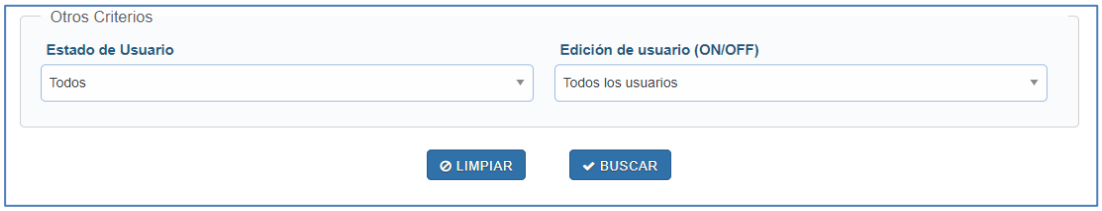
Una vez cumplimentado el formulario y aceptado, se le enviará por mail al usuario dado de alta la confirmación de la misma e información de su identificador de usuario y contraseña en el repositorio. Como resultado se muestra una pantalla con la confirmación del alta.



2.3.1.2. Mantenimiento de usuarios.

Esta opción mostrará un formulario de búsqueda con diversos criterios:





En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Marcando el check ‘Permitir unidades extinguidas’, se mostrarán en los combos Unidades orgánicas que ya no tienen estado Vigente sino Extinguido.

Seleccionando la edición de usuarios (On/Off) se podrá obtener el listado de usuarios excluidos o no del proceso de sincronización.

Si como en el ejemplo se hubiese discriminado por Unidad Orgánica, este podría ser el resultado:

Saldrá un listado paginado con los usuarios que cumplen los criterios de búsqueda y se tendrá la opción de consultar, modificar los datos o de eliminar al usuario, así como la opción de descargar un fichero con los resultados obtenidos.

Si al realizar la búsqueda el número de registros es mayor que el límite establecido se mostrará un mensaje de confirmación con la opción de descarga directa del fichero sin mostrar por pantalla los resultados.

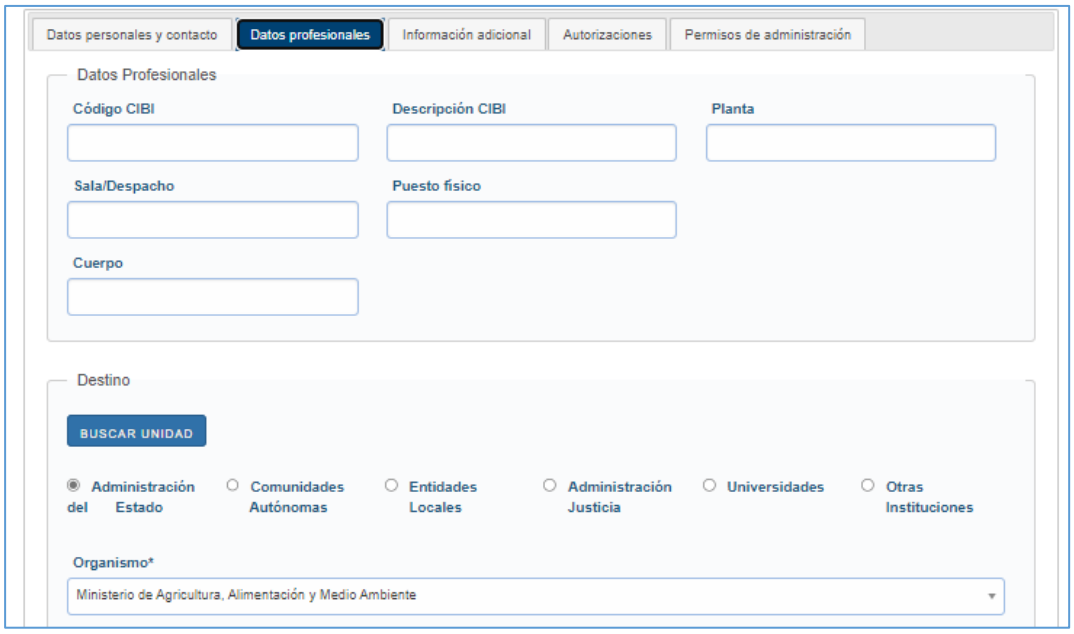
Si se decide seleccionar la opción de consultar, el administrador podrá visualizar los datos del usuario. La pantalla se mostrará con los datos divididos en diferentes pestañas.

Si se decide modificar los datos de un usuario se presenta el siguiente formulario dividido en pestañas:

El administrador podrá modificar casi todos los datos del usuario, podrá visualizar la documentación adjuntada y modificarla, siempre que no supere un tamaño predeterminado establecido en el servidor y tenga extensión .doc, .docx ó .pdf.

En la pantalla se muestra la unidad orgánica del usuario, en la cual se incluye el campo cuerpo/subescala. Si el usuario tiene como fuente de procedencia “Registro Habilitados” se mostrará el literal “Subescala” y si procede de cualquier otra fuente se mostrará el literal “Cuerpo”.

En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Otros datos que se mostrarán son el código CIBI, planta, sala y puesto físico.

Si un administrador es central o delegado con el permiso marcado “Exclusión Fuente Primaria” en la pestaña Administración > Gestión > Gestión de permisos mediante un botón pueden habilitar la modificación de datos independientemente de la fuente de origen del usuario a modificar.

En el campo de correo electrónico, que es obligatorio, se realizará una comprobación del dominio de correo introducido, que deberá ser corporativo. En caso de no serlo, saldrá el siguiente mensaje:

Este correo no pertenece a un dominio de las Administraciones Públicas o del Sector Público. Si usted piensa que es un error o incidencia, puede contactar a través del formulario de incidencias

Puede darse el caso de que el usuario a modificar sea Ciudadano, con lo que se mostrará el formulario de modificación de ciudadano.

Si se modifica el usuario ciudadano a otro tipo de empleado se mostrará una sección para la selección de la unidad orgánica. El usuario se cambiará de la rama de ciudadano a la rama pública.

Desde la modificación de usuarios, se permite enviar a Easy Vista la información de usuarios mediante el botón de volcado de datos que se muestra en la pantalla; el cual aparece en el final de la página. El botón estará siempre activo, con independencia de la fuente de procedencia del usuario.

Si se elige la opción de eliminar el usuario, se presentará una pantalla con el detalle de sus principales datos para que se confirme o no el borrado:

También existe la posibilidad de volver a activar un usuario que ha sido dado de baja.

Esto nos llevará al formulario de Modificación de usuario.

2.3.1.3. Desbloqueo de usuarios.

Esta opción mostrará una lista de los usuarios bloqueados para proceder a su desbloqueo.

Un usuario se bloqueará si ha introducido tres veces sus datos incorrectamente.

Se podrá desbloquear varios usuarios a la vez.

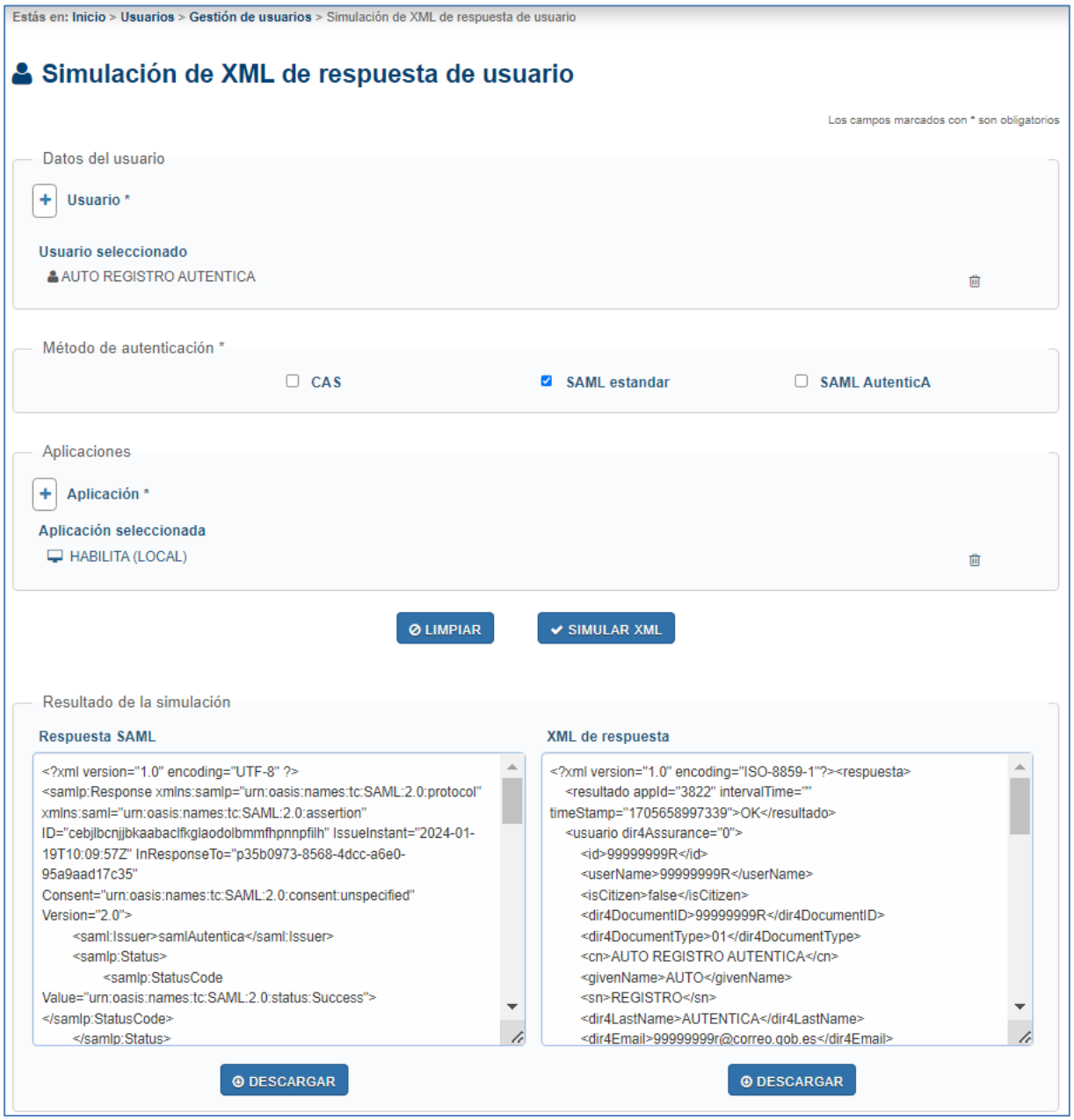
Pulsando en el botón de ‘Histórico’ se mostrará una pantalla con la lista de usuarios que ya han sido desbloqueados.

2.3.1.4. Simulación de XML de respuesta de usuario.

Esta opción mostrará un formulario para la simulación del XML de respuesta para un usuario en la autenticación contra una aplicación. En dicho formulario, aparecerán los campos para seleccionar el usuario, el método de autenticación (CAS o SAML) y la aplicación para la que se desea simular la autenticación.

El administrador podrá simular la autenticación tanto de usuarios de Autentica como usuarios de Correos. Al lanzar la simulación se generará el XML de respuesta y se mostrará en pantalla con la opción de descarga del fichero con el XML. Si para la simulación se ha elegido como método de autenticación SAML estándar o SAML AutenticA, a demás del XML

de respuesta se mostrará, en otro campo, la respuesta en formato SAML.

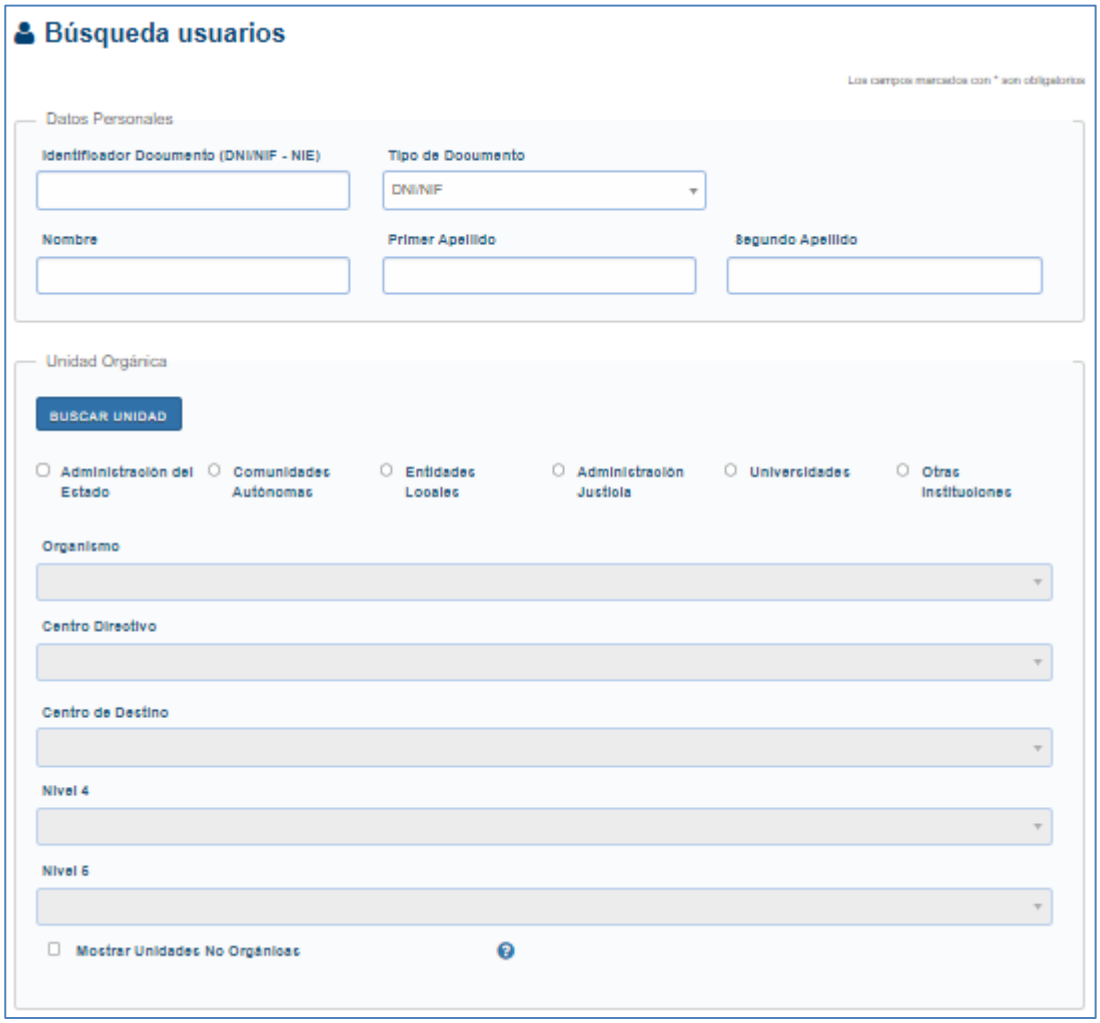


Si el administrador generó la simulación con CAS como método de autenticación podrá descargar el fichero con el XML de respuesta pulsando el botón “Descargar”; y si generó la simulación con SAML, estándar o AutenticaA, también podrá descargar este tipo de respuesta.

2.3.2. GESTIÓN DE GRUPOS DE USUARIO

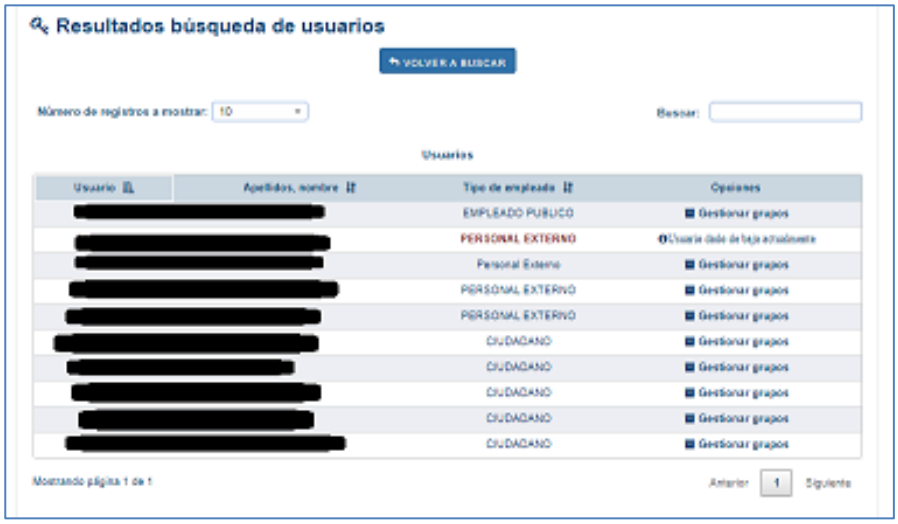
Esta funcionalidad permitirá al administrador gestionar los grupos a los que pertenece un usuario, en el LDAP de AutenticA.

Cuando el administrador acceda a la gestión de grupos de usuario, se le mostrará un formulario para realizar la búsqueda de usuarios.

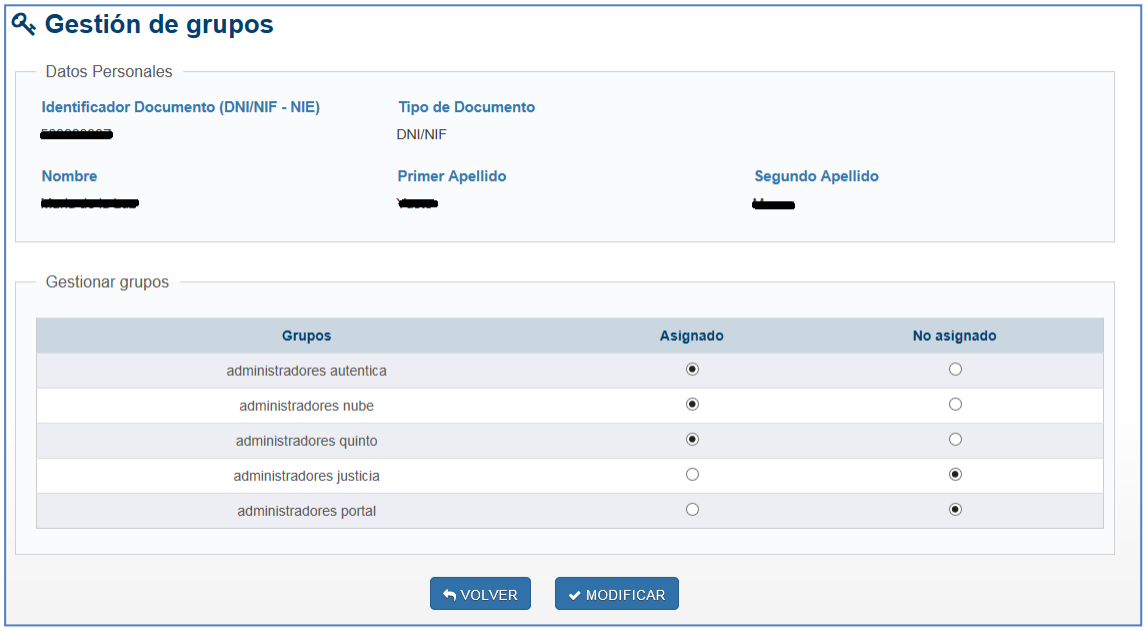


En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Una vez realizada la búsqueda se mostrará un listado con los usuarios que cumplan las condiciones.



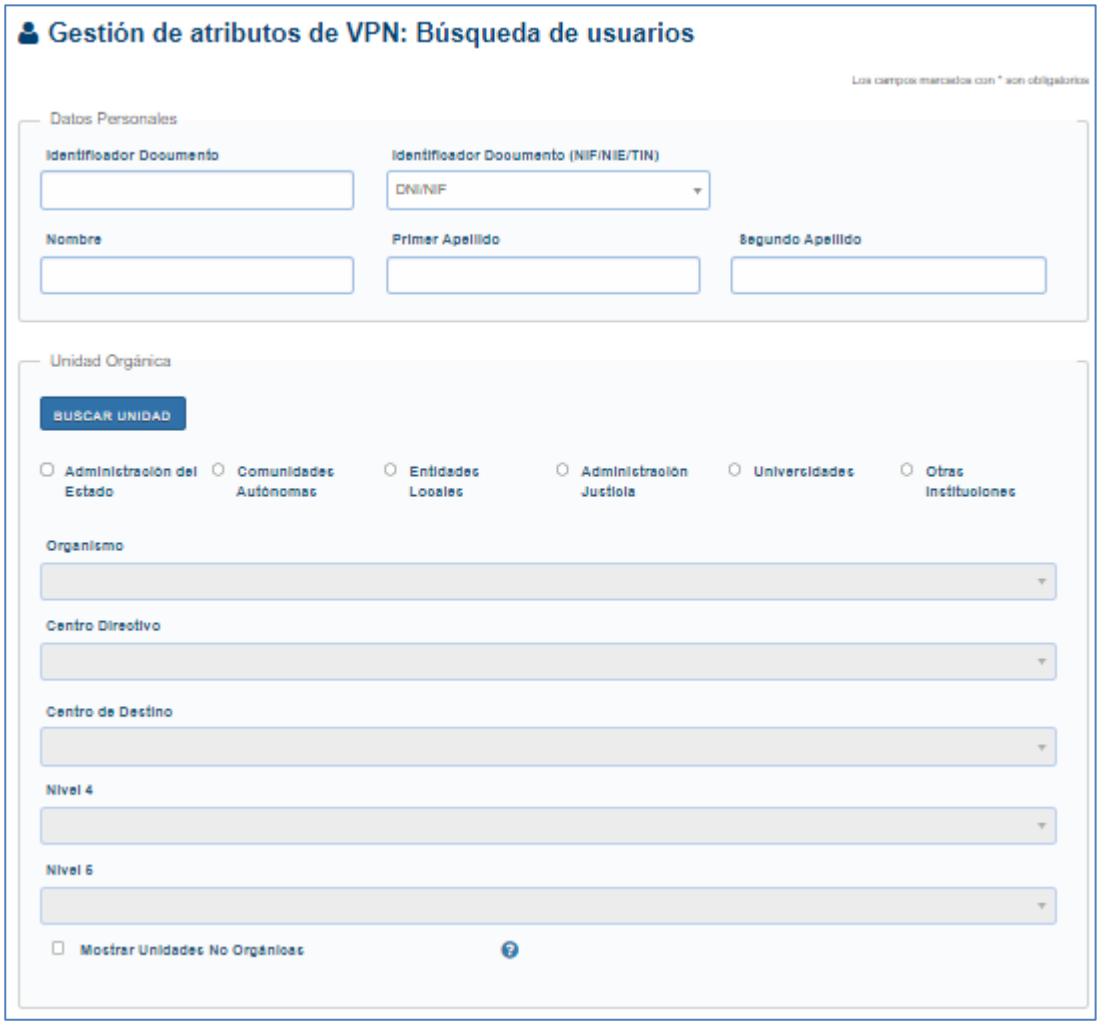
Deberá seleccionar un usuario y se le mostrarán en una pantalla, los grupos que tiene y no tiene asignados. Podrá seleccionar y deseleccionar los que desee. Los grupos no seleccionados se desasignarán y los seleccionados se asignarán.



2.3.3. GESTIÓN DE ATRIBUTOS DE VPN

Esta funcionalidad permitirá al administrador gestionar los atributos de VPN correspondientes a un usuario, almacenados en el LDAP de AutenticA.

Cuando el administrador acceda a la gestión de atributos de VPN, se le mostrará un formulario para realizar la búsqueda de usuarios.



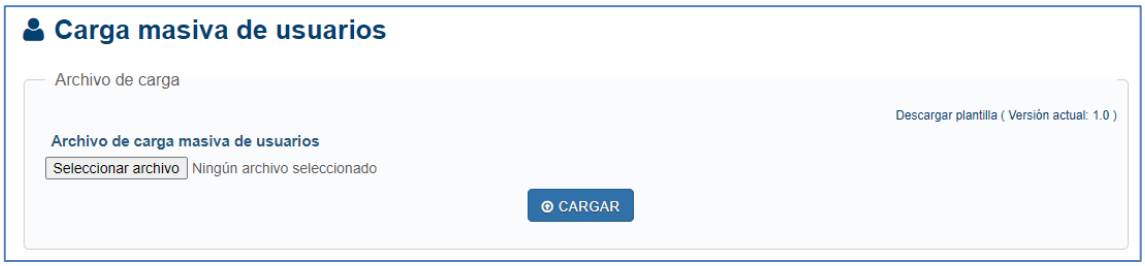
En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Una vez realizada la búsqueda se mostrará un listado con los usuarios que cumplan las condiciones.

Deberá seleccionar un usuario y se le mostrarán en una pantalla, los atributos de VPN que tiene asignados. Podrá rellenar o borrar los valores de los campos de atributos VPN, que se almacenarán en el LDAP al pulsar en el botón “Modificar”.

2.3.4. CARGA MASIVA DE USUARIOS

Se permitirá a los administradores hacer una carga masiva de usuarios utilizando un fichero .xls para ello.



A la derecha de la pantalla habrá un link para descargar un fichero plantilla en el que vendrán especificados los campos a rellenar por línea de usuario.

La primera línea de cabecera se dejará como viene en la plantilla y los datos de cada usuario se rellenarán en las siguientes filas.

Dicho fichero contendrá los siguientes datos:

- ***version_#*** *(Obligatorio): Versión de la plantilla para la carga. El símbolo # se sustituye en la plantilla descargable por la última versión. El valor del campo no se debe modificar ni eliminar y no se debe rellenar la columna correspondiente.*

  Ejemplo: version_1.0

- ***DOCUMENTO_IDENTIFICATIVO*** *(Obligatorio):*
  - *NIF: Formado por nueve caracteres con la siguiente composición: 00000000T*
  - *NIE: Formado por nueve caracteres con la siguiente composición: X0000000T*
- ***TIPO_DOCUMENTO*** *(Opcional): Permite identificar el tipo de documento identificativo:*

- *NIF = 01*
- *NIE = 04*

- ***CODIGO_DIR3*** *(Obligatorio): Código de unidad orgánica DIR3 del usuario, alfanumérico de 9 posiciones, con la siguiente composición: E00000000, si es erróneo no se insertará el usuario.*
- ***NOMBRE*** *(Obligatorio): Nombre del usuario*
- ***APELLIDO1*** *(Obligatorio): Primer apellido del usuario*
- ***APELLIDO2*** *(Obligatorio): Segundo apellido del usuario*
- ***TIPO_EMPLEADO***
  - *Si es administrador central (Obligatorio): El campo tipo de empleado deberá encontrarse en la tabla SAG_REP_TIPO_EMPLEADO. Si el registro no se encuentra en la tabla o se omite, no se insertará el usuario.*
  - *Si es administrador delegado (Opcional): El campo tipo de empleado se omitirá y se guardará como "Desconocido"*
- ***EMAIL*** *(Opcional): Correo electrónico*
- ***CARGO*** *(Opcional): Puesto o cargo del usuario*
- ***TELEFONO*** *(Opcional): Teléfono del usuario*
- ***FECHA_NACIMIENTO*** *(Opcional): Fecha de nacimiento*
- ***ID_COMUNIDAD*** *(Opcional): Código de Comunidad autónoma de nacimiento*
- ***ID_PROVINCIA*** *(Opcional): Código de Provincia de nacimiento*
- ***ID_LOCALIDAD*** *(Opcional): Código de Localidad de nacimiento*
- ***ID_PAIS*** *(Obligatorio): Código del País de nacimiento*
- ***EASYVISTA*** *(Opcional): SI/NO - Volcado de los datos del usuario en easyvista*
- ***CODIGO_CIBI*** *(Opcional): Código del bien inmueble asociado al usuario.*
- ***PLANTA_CIBI*** *(Opcional): Planta del bien inmueble asociado al usuario.*
- ***SALA*** *(Opcional): Sala en la que se ubica el usuario.*
- ***PUESTO_FISICO*** *(Opcional): Puesto físico en el que se ubica el usuario.*
- ***EDITAR ON/OFF*** *(Opcional): Campo representativo a la funcionalidad de "on-off" de la pantalla de datos de usuarios*
- ***RESTRINGIDO*** *(Obligatorio): SI/NO – define la carga de los datos del usuario en la rama restringida. Si el campo se define con valor distinto de "SI" o "NO" o no se define, no se insertará el usuario.*

Serán obligatorios al menos los campos de NIF, Código DIR3, Nombre, Apellidos, Tipo de empleado e ID_PAIS. El resto son recomendables para por lo menos rellenar los datos mínimos identificativos del usuario. Los datos de nacimiento servirán para corroborar que es el propio usuario el que intenta acceder a cambiar su contraseña en la aplicación en caso de que no tenga certificado electrónico.

Si se quiere modificar el tipo de empleado de un usuario ya existente a través de carga masiva de usuarios, deberá estar previamente dado de alta en LDAP como “CIUDADANO” o “PERSONAL EXTERNO”. Para ello, en la plantilla antes de subirla deberá figurar en el campo tipo de empleado como “EMPLEADO PUBLICO”. Si el resto de los campos de la plantilla presentan algún cambio respeto a LDAP solo se cambiaran aquellos datos que tengan una finalidad profesional.

Una vez editado el fichero que se quiere cargar, se selecciona y se pulsa el botón “Cargar” para proceder a la carga de los datos.

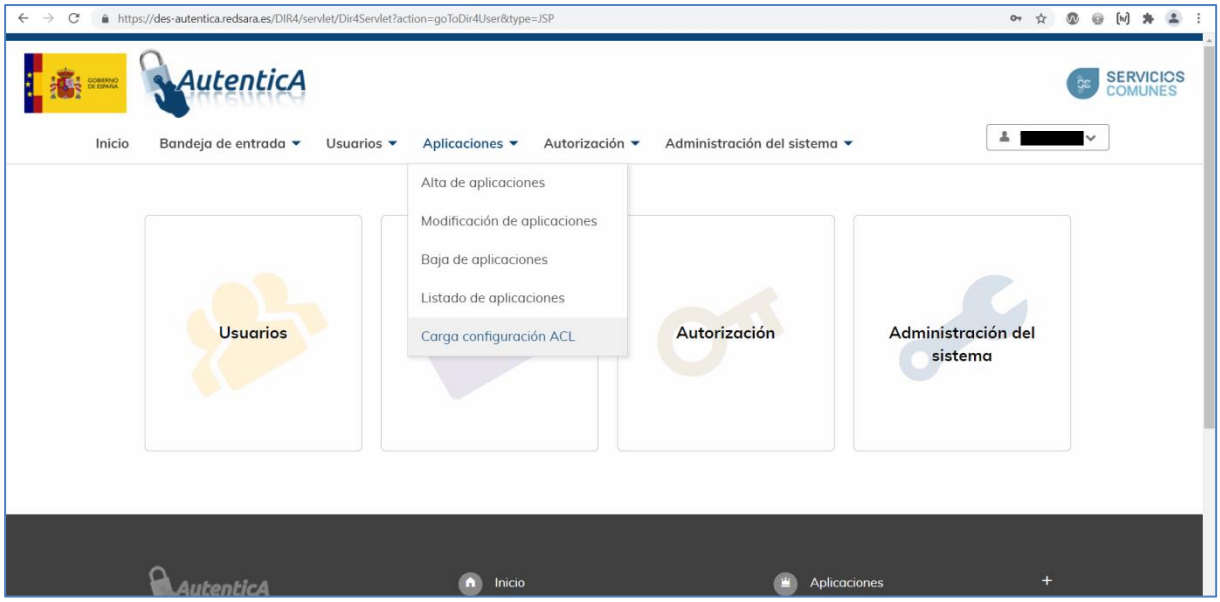
Se contrasta que la versión empleada en la plantilla es la más actual para la carga masiva de usuarios.

Cuando se termine de realizar el proceso, se mostrará una pestaña con el estado del proceso y un botón para descargárselo en un documento de texto.

Después de terminar la carga, saldrá por pantalla el resultado de esta, junto con una opción para poder descargarse un fichero con esta información.

2.4. APLICACIONES

En el menú superior, desde la pestaña de “Aplicaciones” estarán disponibles las opciones para la gestión de las mismas. El objetivo de esta funcionalidad es ofrecer más seguridad a las aplicaciones que se conectan con Autentica. Sólo tendrán acceso a esta pestaña los administradores centrales y los administradores delegados con permiso de aplicaciones solo lectura.



2.4.1. ALTA DE APLICACIONES

Se selecciona la opción de Alta de aplicaciones.

En el formulario de alta, se rellenarán al menos los datos obligatorios (marcados con un asterisco)

En la pantalla se manejarán tres pestañas que agruparán toda la funcionalidad actual del alta, las cuales contendrán la siguiente información: En la pestaña “Datos básicos”:

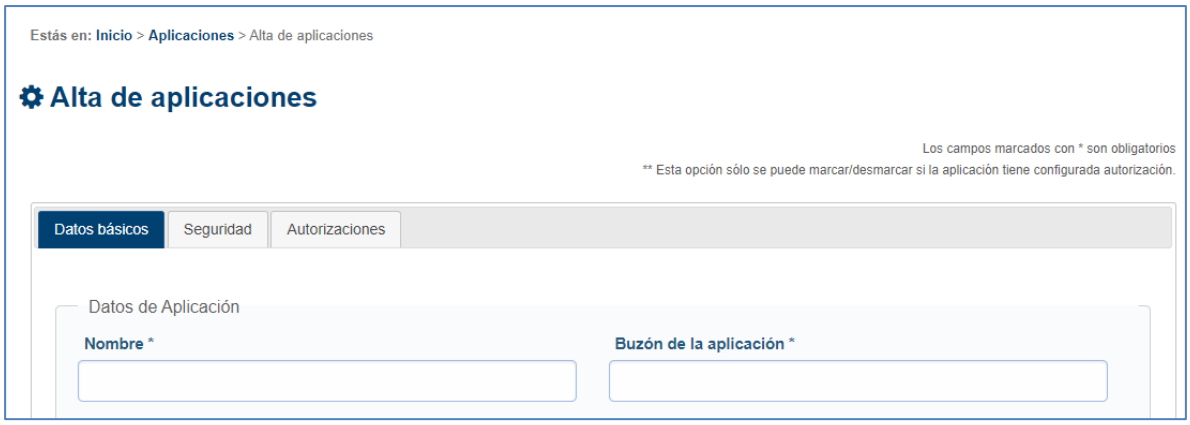
- Datos generales de la aplicación
- Administradores
- Cambio DIR3 Asociada
- Firma no criptográfica

En la pestaña “Seguridad”:

- Métodos de autenticación
- Configuración SAML
- Descarga IdP Metadata
- Datos de seguridad
- Niveles de seguridad
- Algoritmos de firma
- Autenticación con doble factor
- Autenticación mediante QR
- Certificado de perfil de seudónimo
- Servicios web

En la pestaña “Autorizaciones”:

- Configuración de autorizaciones (Activar autorizaciones y autorizaciones)



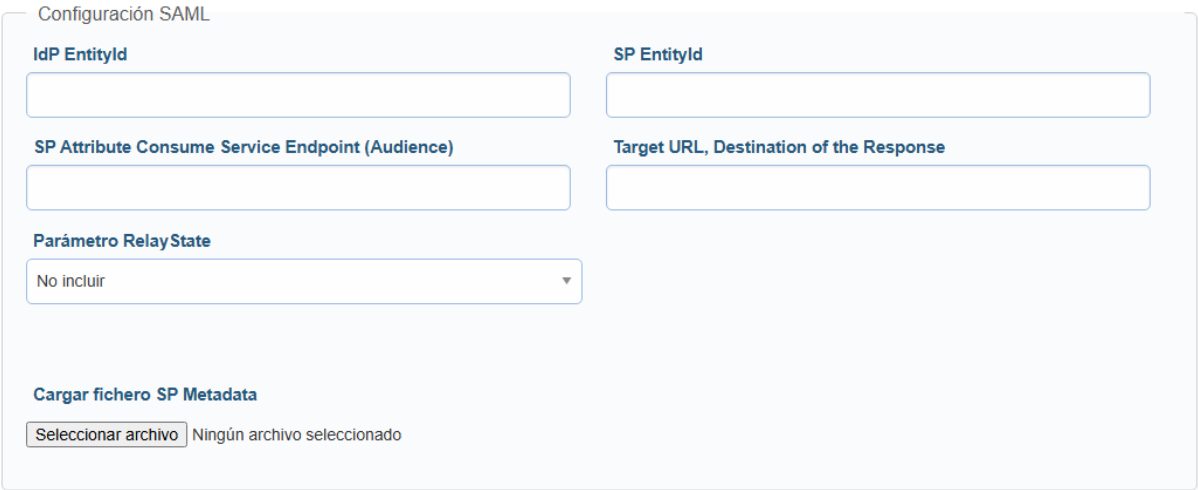
Por defecto vendrán marcados las siguientes opciones:

- check ‘CAS Autentica’, como método de autenticación.
- ‘IP activa’ para verificar la IP de la aplicación.
- ‘Single Sign On’ para permitir acceder a varios sistemas con una sola instancia de identificación.

- ‘Nivel 2’ de seguridad con las opciones
    - ‘Permitir contraseña débil’
    - ‘Acceso automático’
- ‘No realizar ninguna acción’ en el apartado ‘Cambio Unidad DIR3 asociada’.

Se podrá elegir el método de autenticación, teniendo disponibles tres tipos de protocolo:

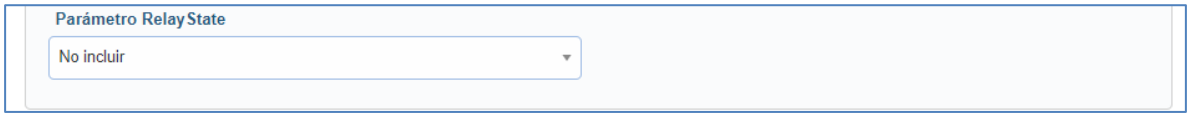
- CAS Autentica: opción seleccionada por defecto, tal como se ha indicado con anterioridad. Seleccionando esta opción, la autenticación se realizará por medio del protocolo SSO Central Authentication Service
- SAML Autentica: seleccionando esta opción, la autenticación se realizará por medio del protocolo SAML2.0 modificado para que sea Autentica el intermediario. Se podrán establecer los siguientes parámetros del estándar, no siendo obligatorios sus datos:
    - IdP EntityId: identificador único global para entidad SAML, como un Proveedor de Identidad (IdP).
    - SP EntityId: identificador único global para un Proveedor de Servicios (SP), URL que identifica a la entidad.
    - SP Attribute Consume Service Endpoint: Punto de acceso de la entidad.
    - Target URL, Destination of the Response: URL de la respuesta en Proveedor de Servicios (SP) para el envío del mensaje saml.
    - Parámetro RelayState: se podrá incluir o no el parámetro con o sin ampersand.



Además, se podrá realizar la carga de los atributos mediante el fichero SpMetadata.

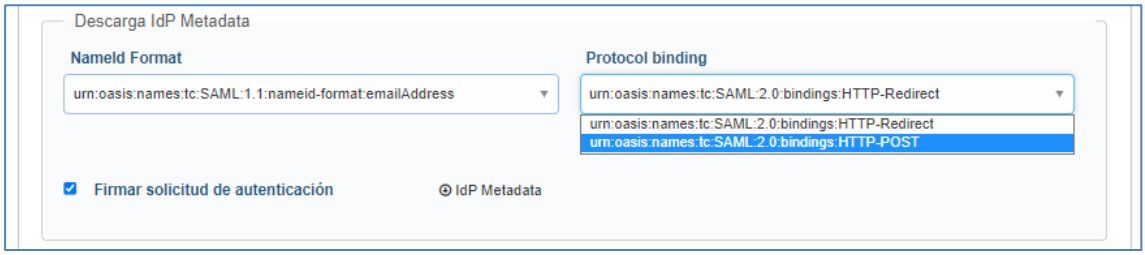
- SAML Estándar: seleccionando esta opción, la autenticación se realizará por medio del protocolo SAML2.0 estándar, requiriéndose, de forma obligatoria, que se complete la siguiente información adicional:
    - IdP EntityId: identificador único global para entidad SAML, como un Proveedor de Identidad (IdP).

- SP EntityId: identificador único global para un Proveedor de Servicios (SP), URL que identifica a la entidad.
- SP Attribute Consume Service Endpoint: Punto de acceso de la entidad.
- Target URL, Destination of the Response: URL de la respuesta en Proveedor de Servicios (SP) para el envío del mensaje saml.
- Parámetro RelayState: se podrá incluir o no el parámetro con o sin ampersand.



Además, se podrá realizar la carga de los atributos mediante el fichero SpMetadata.

Así mismo, se podrá descargar un fichero IdPMetadata.xml que se generará a partir de la información con la que se ha configurado una determinada aplicación y que será distribuido a los responsables de la aplicación.



También se podrán seleccionar las siguientes opciones:

- Si se marca la opción 'No se consulta en LDAP para esta aplicación', sólo se tendrán en cuenta los datos del certificado.
- Si se marca la opción 'Acceso con certificado de representante, se permitirá acceder a la aplicación con este tipo de certificado. Se deberá marcar previamente en la pestaña Aplicaciones > Listado > Modificación de aplicaciones.

- Si se marca la opción 'XML de respuesta en base 64', el XML de respuesta que se devolverá será menos legible que de la manera ordinaria.
- Si se marca la opción 'Permitir certificado de perfil de seudónimo', se permitirá el acceso a la aplicación con certificados de perfil de seudónimo.
    - Si se marca la opción 'Permitir solo certificados incluidos en la lista blanca', se permitirá el acceso a la aplicación con certificados de perfil de seudónimo que estén permitidos en el listado de autoridades de certificación.
- Si se marca la opción 'Activar servicio notificación de autorizaciones' podrán ser notificados aquellos administradores delegados de cierta aplicación podrán recibir notificaciones mediante correos si se marca la opción 'Envío de correo electrónico de

notificaciones de autorización' o si se marca la opción 'Envío de notificaciones correo electrónico específico' se mandará al que se guarda en la caja de texto.

- Si se marca la opción 'Activar autorización para representantes' se permitirá gestionar las autorizaciones sobre la aplicación a los administradores delegados representantes.
    - Si se marca la opción 'Permitir solo certificados incluidos en la lista blanca', se permitirá el acceso a la aplicación con certificados de representantes que estén permitidos en el listado de autoridades de certificación.

Se podrá elegir entre distintos niveles de seguridad de autenticación para la aplicación que se esté dando de alta. Actualmente el nivel 1 está deshabilitado.

- Nivel 1 (desaconsejado), este método permitirá el acceso a la rama de ciudadanos.
- Nivel 2 (básico), Cualquier certificado y contraseña fuerte.
    a. Cualquier contraseña (sí o no) (incluiría también contraseña débil)
    b. Consultar método (sí o no) (por defecto automático).
    c. Acceso a internet con contraseña.
    d. Permitir búsqueda en otros repositorios sindicados.
    e. Permitir repositorio externo sin LDAP.
    f. Permitir solo certificados incluidos en la lista blanca.
    g. Permitir nombres de usuario no nominales
- Nivel 3 (medio/sustancial), cualquier certificado
    - Permitir solo certificados incluidos en la lista blanca.
- Nivel 4 (alto), sólo certificado con soporte en tarjeta criptográfica o eDNI.

Se podrá permitir la autenticación con doble factor en función de las necesidades de la aplicación que se esté dando de alta. Este mecanismo se podrá combinar con los niveles de seguridad disponibles que permitan el uso de contraseña en el acceso, excepto con el nivel 1, con el cual no será compatible. Se puede configurar:

- Omitir la verificación con certificado.
- Omitir la verificación con código QR.

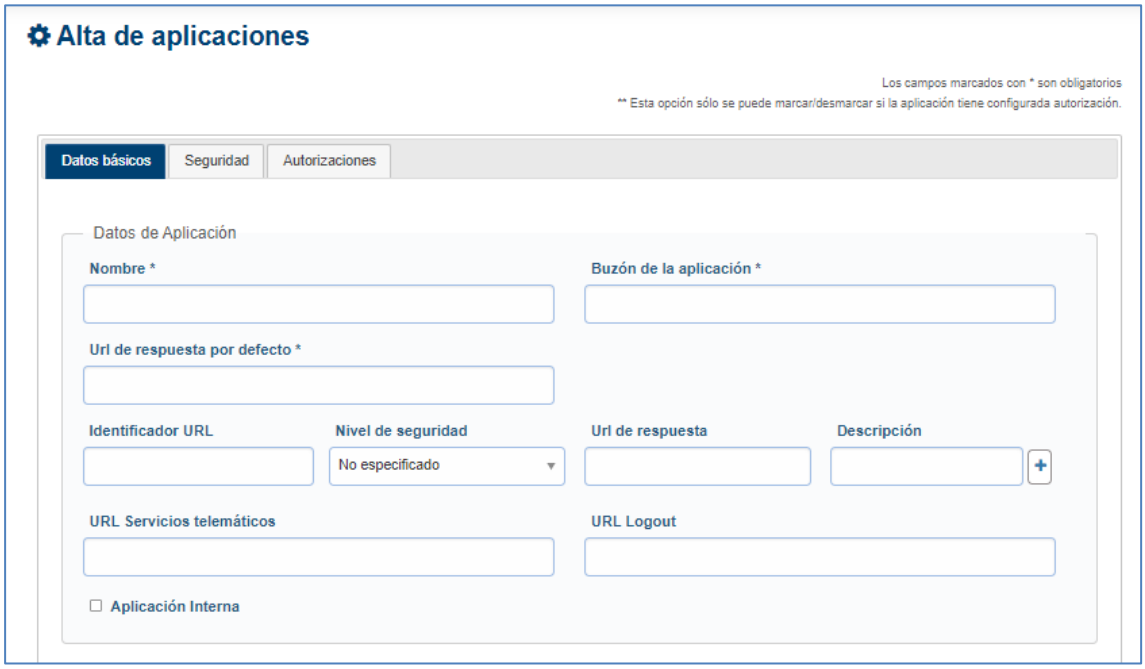
- Tipo de envío del código de seguridad: ya sea solo a través de correo electrónico, solo a través de mensaje corto SMS o a través de ambas opciones a selección del usuario en el acceso.
- La duración en minutos destinada a la caducidad del código
- La cantidad de caracteres que componen el código de verificación.

En el campo obligatorio “Url de respuesta por defecto” se indicará la URL a la que se redirigirá Autentica en el caso de que la autenticación del usuario haya sido satisfactoria. Es posible añadir más URLs de respuesta asociándolos con el valor introducido en el campo “Identificador URL”, cuyo contenido debe ser numérico, de tal forma que en el caso de que un usuario se autentique de forma satisfactoria, y la aplicación haya invocado el acceso con Autentica añadiendo este valor numérico en un parámetro de nombre “appParam”, se redirigirá a la URL asociada.

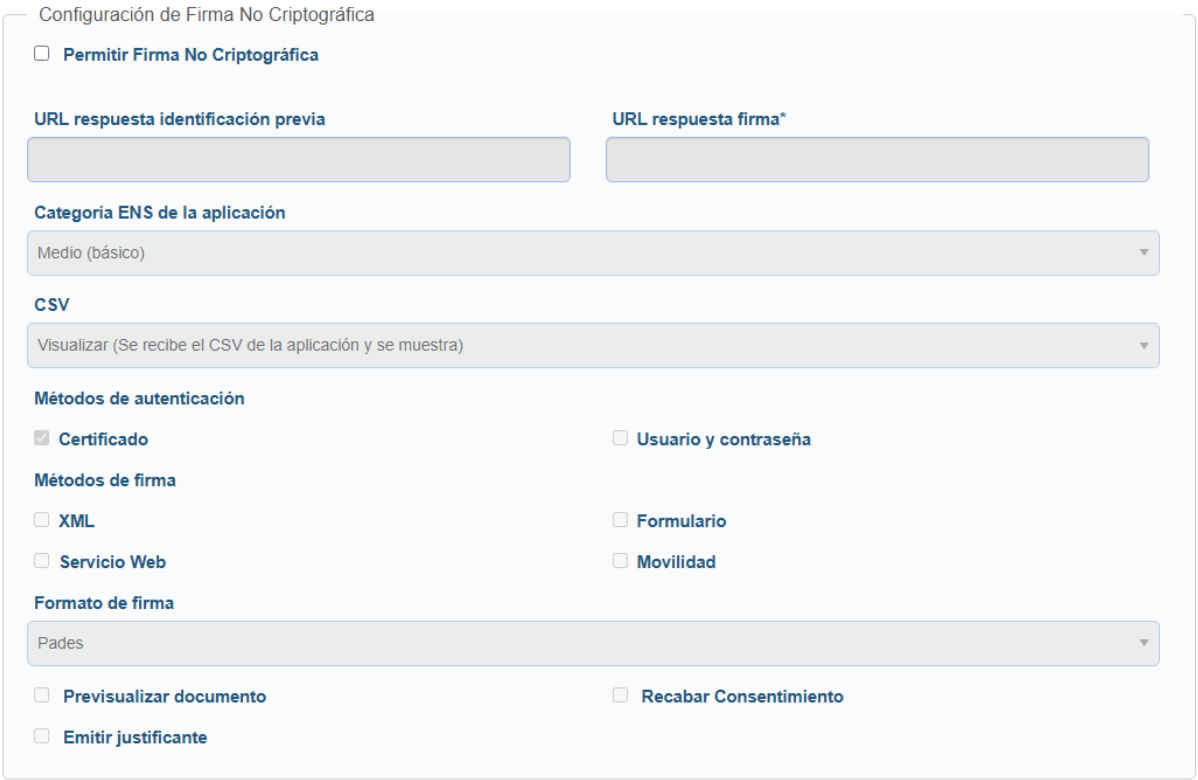
Así mismo, para cada identificador URL se puede especificar un nivel de seguridad diferente al definido para la aplicación, teniendo en cuenta lo siguiente:

- No se puede especificar un nivel de seguridad inferior al definido para la aplicación; en el caso de que, por algún motivo, quede registrado un nivel inferior, será modificado automáticamente por el nivel “No especificado”.
- En el caso de alta de aplicación, se muestran las cuatro opciones disponibles, en el caso de modificación de una aplicación, se muestran siempre las opciones “No especificado” y “Nivel 3 (medio/sustancial)”, y que las opciones “Nivel 1 (no recomendado)” y “Nivel 2 (básico)”, dependerán del nivel de seguridad indicado en la aplicación.
- El nivel “No especificado” indica que el identificador URL toma el nivel de seguridad genérico definido para la aplicación.
- En el caso de que se invoque Autentica con un parámetro *appParam* que no sea válido (ya sea porque no sea numérico o porque no se trate de un valor registrado en la ficha de la aplicación) y la autenticación sea correcta, se redirigirá a la URL de respuesta por defecto de la aplicación.
- En el caso de que se configure un nivel de seguridad 2 tanto para la aplicación como para el identificador URL:
    a. El acceso por identificador URL requerirá contraseña fuerte.
    b. El acceso por identificador URL mostrará la pantalla de opciones de acceso, se haya marcado o no el acceso automático en la definición del nivel de seguridad 2 por parte de la aplicación.

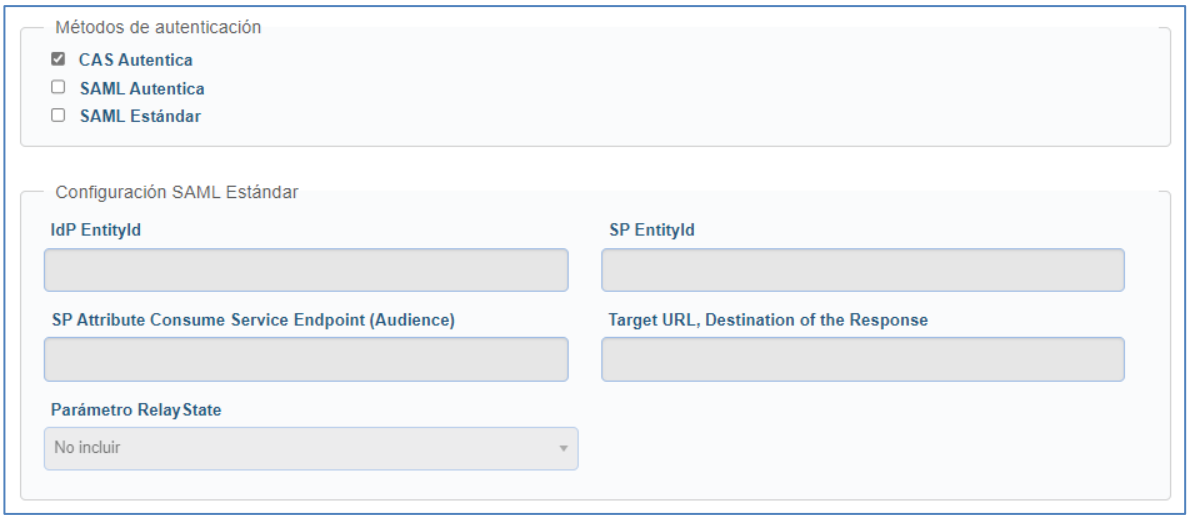
Se podrá definir la aplicación como interna.



En el apartado de firma no criptográfica se podrá definir las urls de identificación previa y la de respuesta de la firma; así mismo, se podrá la categoría, el tipo de csv para la firma con dicha aplicación, el método de autenticación permitido, el método de firma, el formato y las opciones de previsualización del documento, aceptar el consentimiento o la generación del justificante.



Se podrá configurar el responsable y los gestores (hasta 5 gestores) de dicha aplicación.



Algoritmos de firma

Algoritmo

SHA1

Niveles de seguridad

- [ ] **Nivel 4 (alto)**
- [ ] **Nivel 3 (medio/sustancial)**
  - [ ] **Permitir solo certificados incluidos en la lista blanca**
- [x] **Nivel 2 (básico)**
  - [x] **Permitir contraseña débil**
  - [x] **Acceso automático**
  - [ ] **Acceso a internet con contraseña**
  - [ ] **Permitir búsqueda en otros repositorios sindicados**
  - [ ] **Permitir repositorio externo sin LDAP**
  - [ ] **Acceso mediante proveedor de identidad**
  - [ ] **Permitir solo certificados incluidos en la lista blanca**
  - [ ] **Permitir nombres de usuario no nominales**
- [ ] **Nivel 1 (desaconsejado)**

Autenticación con doble factor

- [ ] **Permitir autenticación con doble factor**
  - [ ] **Omitir doble factor en autenticación con certificado electrónico**
  - [ ] **Omitir doble factor en autenticación con código QR**

Envío de verificación mediante:

- [ ] **Correo electrónico**
- [ ] **Mensaje de texto (SMS)**
- [ ] **Notificación en aplicación móvil**

Duración del código en minutos: min

Cantidad de dígitos:

Autenticación con código QR

- [x] **Permitir autenticación con código QR**

Duración del código en minutos:

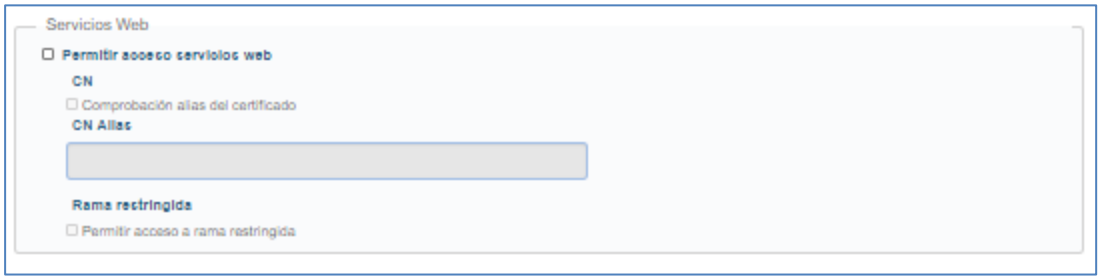
9 min

Cantidad de dígitos:

5

Tipos de certificados permitidos

- [ ] **Permitir certificado de perfil de seudónimo**
  - [ ] **Permitir solo certificados incluidos en la lista blanca**
- [ ] **Permitir acceso con certificado de representante**
  - [ ] **Permitir solo certificados incluidos en la lista blanca**



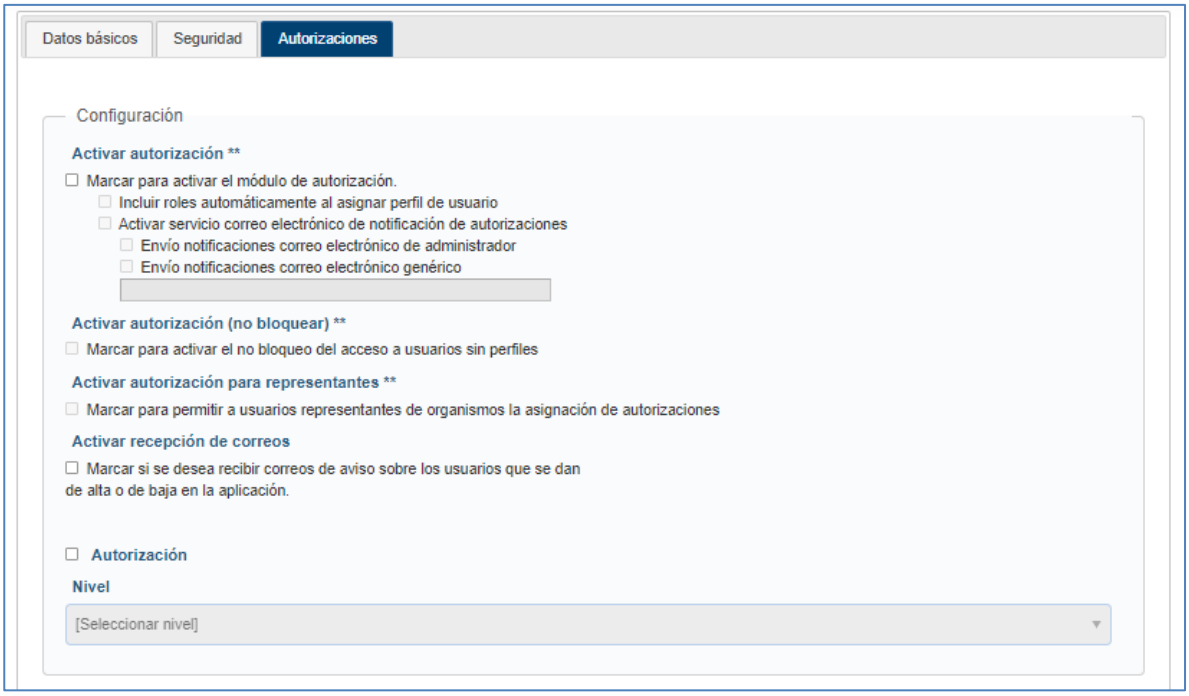
El apartado Servicios Web, está relacionado con los permisos de accesos a los servicios web; en el cual, se podrá permitir marcando la opción de servicios web. Además, se podrá seleccionar la comprobación del alias del certificado definiendo el CN a utilizar por la aplicación. Por otro lado, se podrá habilitar la opción de permiso de acceso al servicio web de rama restringida, para habilitar el mismo, debe estar habilitado la ip activa y el alias del certificado.

El campo Activar autorización, está relacionado con el módulo de autorización, que se explicará en el punto 2.4

Al dar de alta la aplicación llevará a su detalle, desde donde se podrá asignar una autorización a la aplicación.

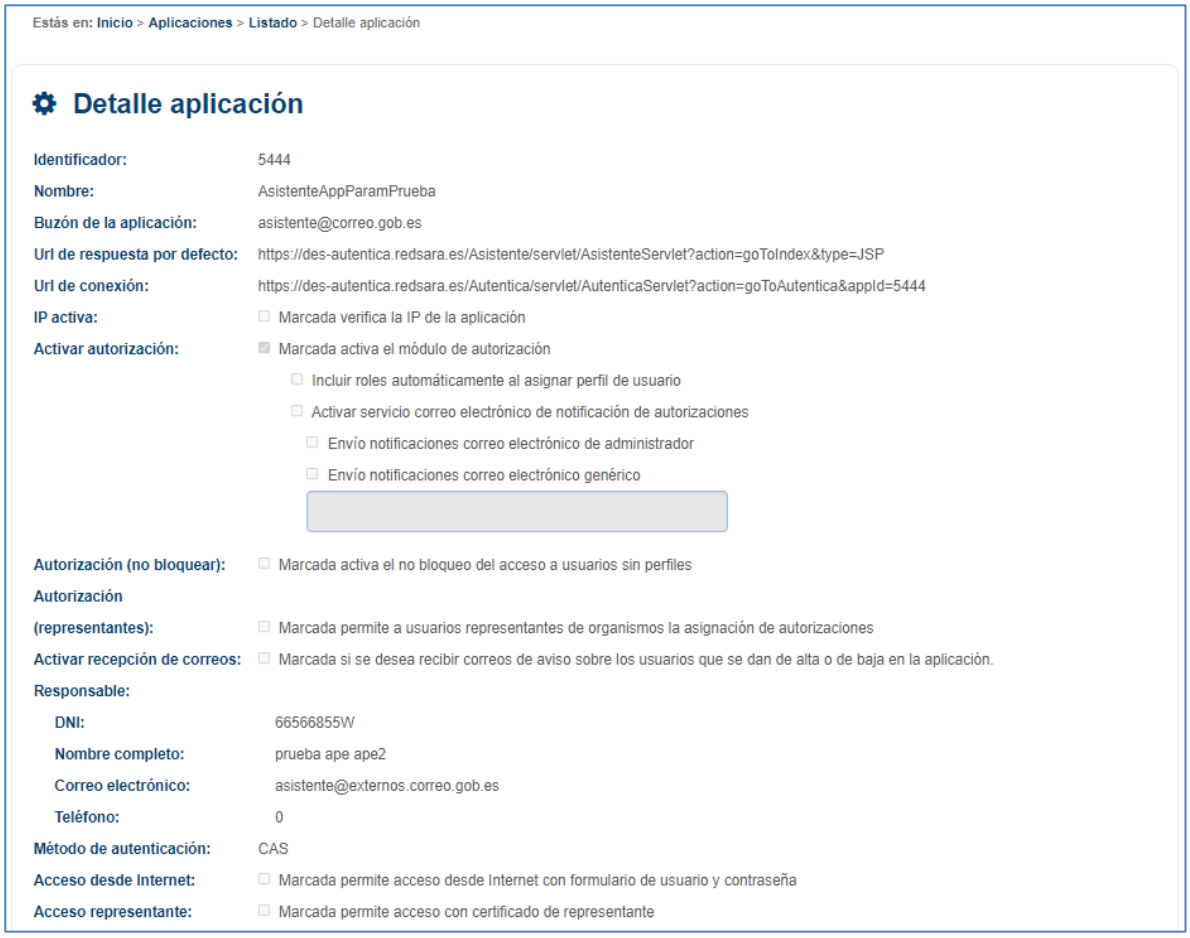
En el apartado “Configuración de autorización” se configura si un usuario podrá realizar solicitudes de autorización sobre la aplicación desde su ficha de usuario en “Estoy dado de alta”. Para ello, se deberá:

- Marcar la casilla “Autorización”.
- Indicar el nivel de autorización (1 o 2) de las autorizaciones que se podrán solicitar.



De esta forma, en la ficha de usuario de “Estoy dado de alta”, un usuario podrá realizar una solicitud de autorización sobre una aplicación que tenga la casilla “Autorización” marcada, así como realizar una solicitud de modificación sobre aquellas autorizaciones cuyo nivel sea el mismo que está configurado en este apartado.

Respecto a las solicitudes de autorizaciones que se realicen, estas se podrán ver en la bandeja de entrada de solicitudes de autorización.



URL servicios telemáticos:	ua
URL Logout:	pruebaUrlLogout
SSO:	☐ Permitir Single Sign On en el acceso a la aplicación
CN:	☑ Marcada para seguridad de Servicios Web
CN Alias:	SELLO ENTIDAD SGAD PRUEBAS
Rama restringida:	☑ Marcada permite acceso a servicio web de rama restringida
Ip de servicios web:	10.1.109.84,10.1.109.85,10.1.110.28,10.253.114.163,10.118.85.150,10.1.110.72
Codificación base 64:	☐ Marcada para codificación en base64 del XML de respuesta
Algoritmo de firma	sha1
Mensaje conexión:	☐ Marcada para mostrar mensaje de última conexión
Nivel de seguridad:	Nivel 2 de seguridad - No se permiten todas las contraseñas - Se permite el acceso automático - No se busca en otros repositorios - Se permite solo certificados incluidos en la lista blanca
Patrón repositorio externo:	☑ Marcada permite acceso a repositorio externo sin LDAP
Autenticación con doble factor:	☐ Permite autenticación con doble factor
Autenticación con código QR:	☐ Permite autenticación con código QR
Certificado de seudónimo:	☑ Marcada permite certificado de perfil de seudónimo ☑ Marcada permite solo certificados incluidos en la lista blanca
Usuario LDAP:	☐ Marcada indica que no se consulta en LDAP para esta aplicación
Tratamiento Unidad DIR3:	No realizar ninguna acción

✔ ASIGNAR AUTORIZACIÓN DESCARGAR FICHERO ACL

Se podrá descargar el fichero de configuración ACL para la aplicación desde el botón habilitado para la descarga.

2.4.2. MODIFICACIÓN DE APLICACIONES

Se seleccionará la aplicación que se desee modificar del listado que se muestra

Se podrá realizar la búsqueda de aplicaciones según los criterios que se muestran o descargar el listado que se visualiza.

Una vez se muestre el formulario, se podrá modificar cualquier dato de la aplicación.

En la pantalla se manejarán tres pestañas que agruparán toda la funcionalidad actual de la modificación, las cuales contendrán la siguiente información:

En la pestaña “Datos básicos”:

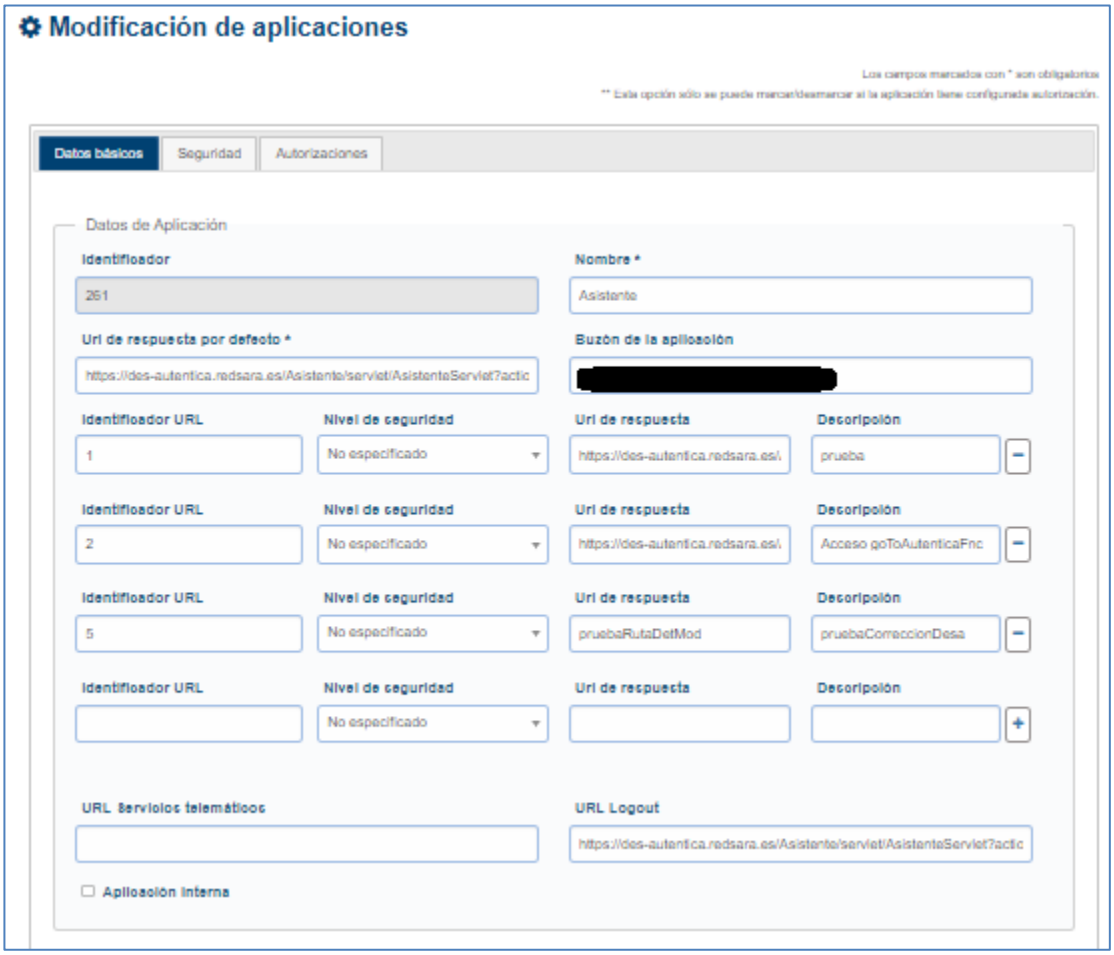
- Datos generales de la aplicación
- Administradores
- Cambio DIR3 Asociada
- Firma no criptográfica

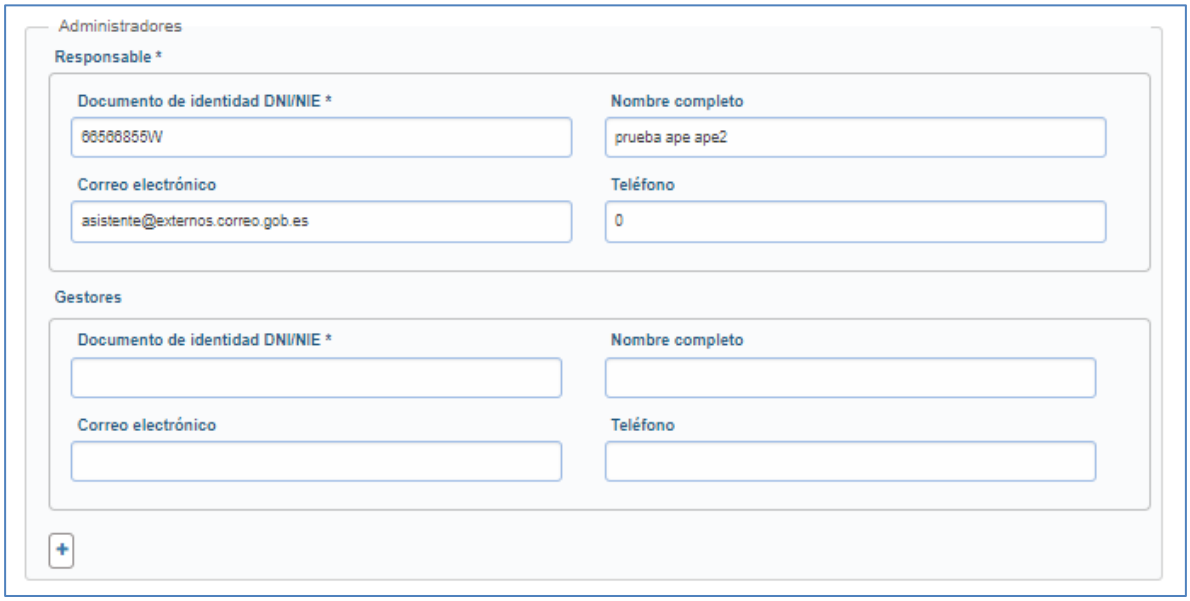
En la pestaña “Seguridad”:

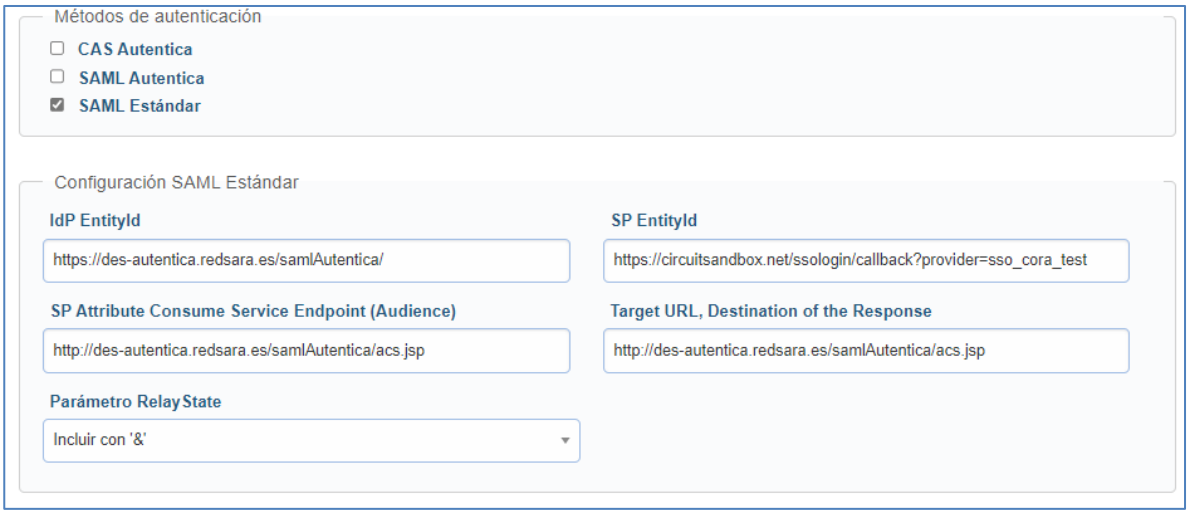
- Métodos de autenticación
- Configuración SAML
- Descarga IdP Metadata
- Datos de seguridad
- Niveles de seguridad
- Autenticación con doble factor
- Autenticación mediante QR
- Certificado de perfil de seudónimo
- Servicios web

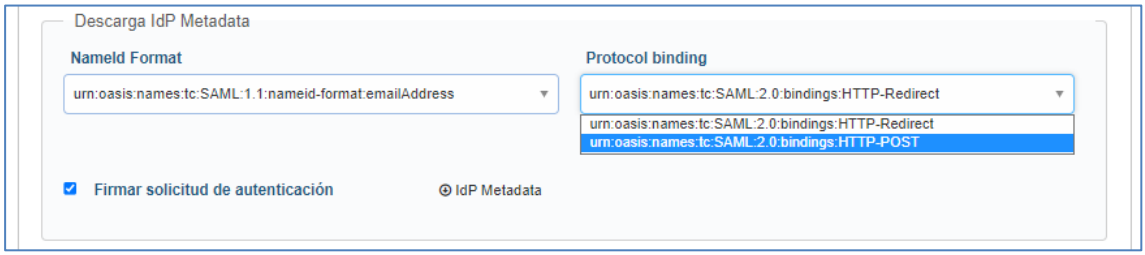
En la pestaña “Autorizaciones”:

- Configuración de autorizaciones (Activar autorizaciones y autorizaciones)




Administradores
Responsable *
Documento de identidad DNI/NIE *
66566855W
Nombre completo
prueba ape ape2
Correo electrónico
asistente@externos.correo.gob.es
Teléfono
0
Gestores
Documento de identidad DNI/NIE *
Nombre completo
Correo electrónico
Teléfono


Métodos de autenticación
CAS Autentica
SAML Autentica
SAML Estándar
Configuración SAML Estándar
IdP EntityId
https://des-autentica.redsara.es/samlAutentica/
SP EntityId
https://circuitsandbox.net/ssologin/callback?provider=sso_cora_test
SP Attribute Consume Service Endpoint (Audience)
http://des-autentica.redsara.es/samlAutentica/acs.jsp
Target URL, Destination of the Response
http://des-autentica.redsara.es/samlAutentica/acs.jsp
Parámetro RelayState
Incluir con '&'


Descarga IdP Metadata
NameId Format
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Protocol binding
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
Firmar solicitud de autenticación
IdP Metadata

Niveles de seguridad

- [ ] Nivel 4 (alto)
- [ ] Nivel 3 (medio/sustancial)
  - [ ] Permitir solo certificados incluidos en la lista blanca
- [x] Nivel 2 (básico)
  - [x] Permitir contraseña débil
  - [x] Acceso automático
  - [ ] Acceso a internet con contraseña
  - [ ] Permitir búsqueda en otros repositorios sindicados
  - [ ] Permitir repositorio externo sin LDAP
  - [ ] Acceso mediante proveedor de identidad
  - [ ] Permitir solo certificados incluidos en la lista blanca
  - [ ] Permitir nombres de usuario no nominales
- [ ] Nivel 1 (desaconsejado)

Autenticación con doble factor

- [ ] Permitir autenticación con doble factor
  - [ ] Omitir doble factor en autenticación con certificado electrónico
  - [ ] Omitir doble factor en autenticación con código QR

Envío de verificación mediante:

- [ ] Correo electrónico
- [ ] Mensaje de texto (SMS)
- [ ] Notificación en aplicación móvil

Duración del código en minutos: min

Cantidad de dígitos:

Autenticación con código QR

- [x] Permitir autenticación con código QR

Duración del código en minutos: 9 min

Cantidad de dígitos: 5

Tipos de certificados permitidos

- [ ] Permitir certificado de perfil de seudónimo
  - [ ] Permitir solo certificados incluidos en la lista blanca
- [ ] Permitir acceso con certificado de representante
  - [ ] Permitir solo certificados incluidos en la lista blanca

Servicios Web

- [ ] Permitir acceso servicios web

CN

- [ ] Comprobación alias del certificado

CN Alias

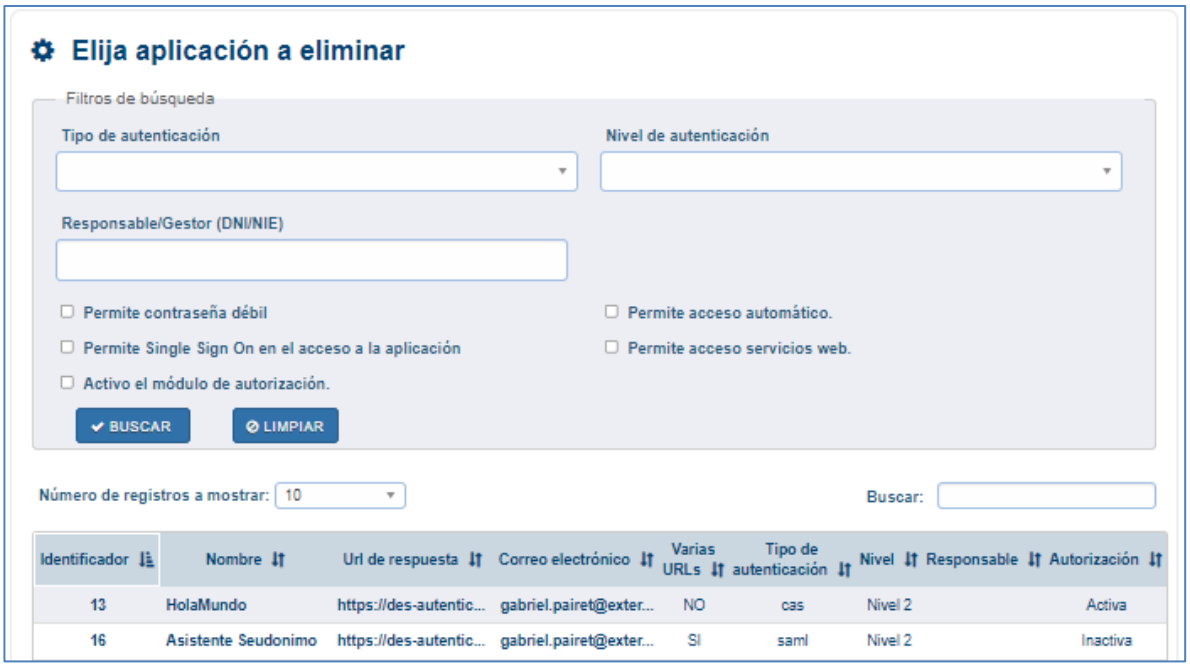
Rama restringida

- [ ] Permitir acceso a rama restringida

Se mostrará una pantalla donde se podrá Asignar, Eliminar o Modificar las autorizaciones de la aplicación.

2.4.3. BAJA DE APLICACIONES

Se seleccionará la aplicación que se desee eliminar del listado que se muestra.

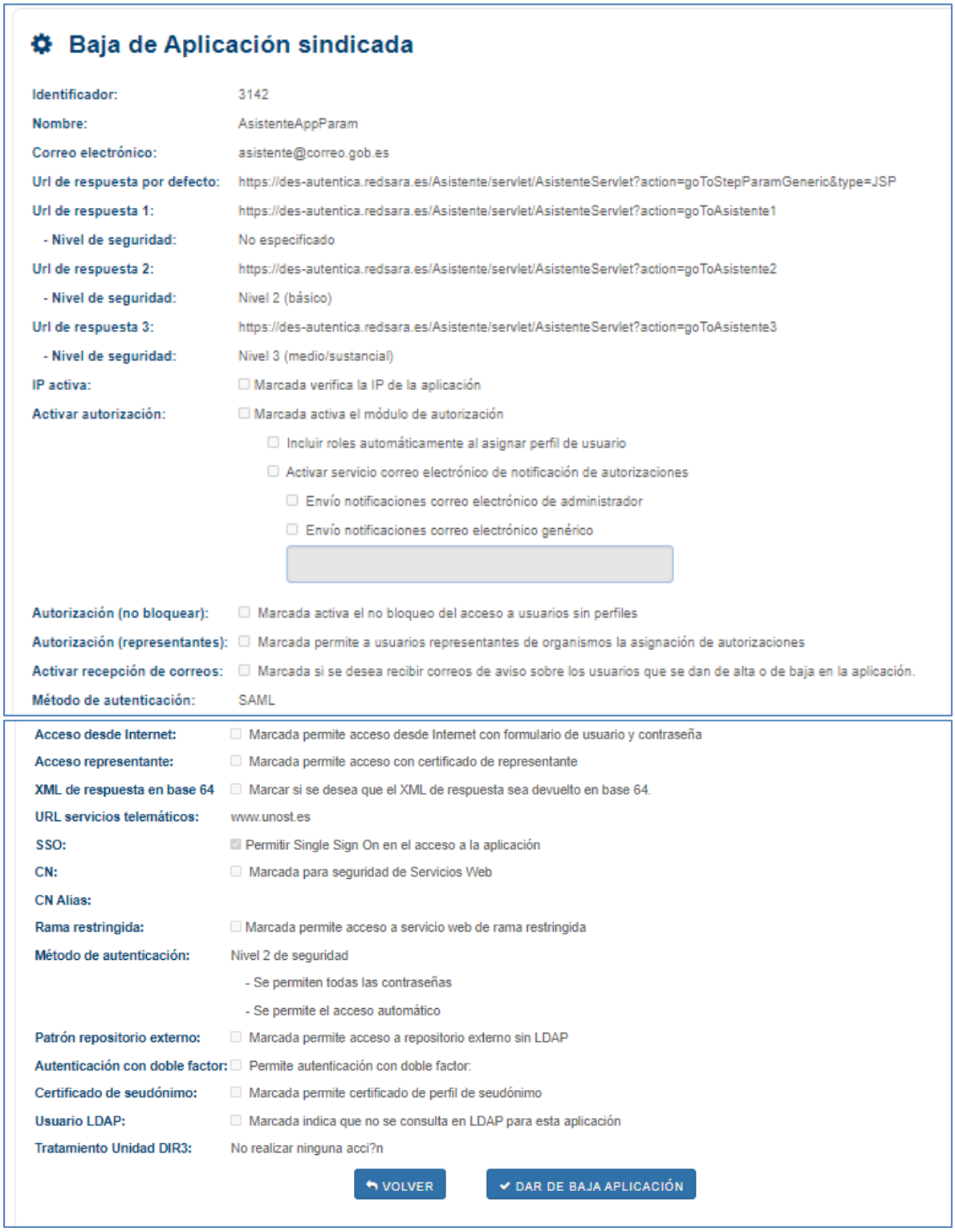


Se podrá realizar la búsqueda de usuarios por los criterios que se muestran.

Se mostrará el detalle de la aplicación a eliminar

Baja de Aplicación sindicada

Identificador:	5444
Nombre:	AsistenteAppParamPrueba
Buzón de la aplicación:	asistente@correo.gob.es
Url de respuesta por defecto:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToIndex&type=JSP
IP activa:	☐ Marcada verifica la IP de la aplicación
Activar autorización:	☑ Marcada activa el módulo de autorización
	☐ Incluir roles automáticamente al asignar perfil de usuario
	☐ Activar servicio correo electrónico de notificación de autorizaciones
	☐ Envío notificaciones correo electrónico de administrador
	☐ Envío notificaciones correo electrónico genérico
Autorización (no bloquear):	☐ Marcada activa el no bloqueo del acceso a usuarios sin perfiles
Autorización (representantes):	☐ Marcada permite a usuarios representantes de organismos la asignación de autorizaciones
Activar recepción de correos:	☐ Marcada si se desea recibir correos de aviso sobre los usuarios que se dan de alta o de baja en la aplicación.
Responsable:	
DNI:	66666855W
Nombre completo:	prueba ape ape2
Correo electrónico:	asistente@externos.correo.gob.es
Teléfono:	0
Método de autenticación:	CAS
Acceso desde Internet:	☐ Marcada permite acceso desde Internet con formulario de usuario y contraseña
Acceso representante:	☐ Marcada permite acceso con certificado de representante
XML de respuesta en base 64	☐ Marcar si se desea que el XML de respuesta sea devuelto en base 64.



Baja de Aplicación sindicada

Identificador:	3142
Nombre:	AsistenteAppParam
Correo electrónico:	asistente@correo.gob.es
Url de respuesta por defecto:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToStepParamGeneric&type=JSP
Url de respuesta 1:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente1
- Nivel de seguridad:	No especificado
Url de respuesta 2:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente2
- Nivel de seguridad:	Nivel 2 (básico)
Url de respuesta 3:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente3
- Nivel de seguridad:	Nivel 3 (medio/sustancial)
IP activa:	Marcada verifica la IP de la aplicación
Activar autorización:	Marcada activa el módulo de autorización
	Incluir roles automáticamente al asignar perfil de usuario
	Activar servicio correo electrónico de notificación de autorizaciones
	Envío notificaciones correo electrónico de administrador
	Envío notificaciones correo electrónico genérico
Autorización (no bloquear):	Marcada activa el no bloqueo del acceso a usuarios sin perfiles
Autorización (representantes):	Marcada permite a usuarios representantes de organismos la asignación de autorizaciones
Activar recepción de correos:	Marcada si se desea recibir correos de aviso sobre los usuarios que se dan de alta o de baja en la aplicación.
Método de autenticación:	SAML
Acceso desde Internet:	Marcada permite acceso desde Internet con formulario de usuario y contraseña
Acceso representante:	Marcada permite acceso con certificado de representante
XML de respuesta en base 64	Marcar si se desea que el XML de respuesta sea devuelto en base 64.
URL servicios telemáticos:	www.unost.es
SSO:	Permitir Single Sign On en el acceso a la aplicación
CN:	Marcada para seguridad de Servicios Web
CN Alias:	
Rama restringida:	Marcada permite acceso a servicio web de rama restringida
Método de autenticación:	Nivel 2 de seguridad
	- Se permiten todas las contraseñas
	- Se permite el acceso automático
Patrón repositorio externo:	Marcada permite acceso a repositorio externo sin LDAP
Autenticación con doble factor:	Permite autenticación con doble factor:
Certificado de seudónimo:	Marcada permite certificado de perfil de seudónimo
Usuario LDAP:	Marcada indica que no se consulta en LDAP para esta aplicación
Tratamiento Unidad DIR3:	No realizar ninguna acci?n

VOLVER DAR DE BAJA APLICACIÓN

2.4.4. CONSULTA DE APLICACIONES

Se seleccionará la aplicación que se desee consultar del listado que se muestra.

Se podrá realizar la búsqueda de aplicaciones por los criterios que se muestran.

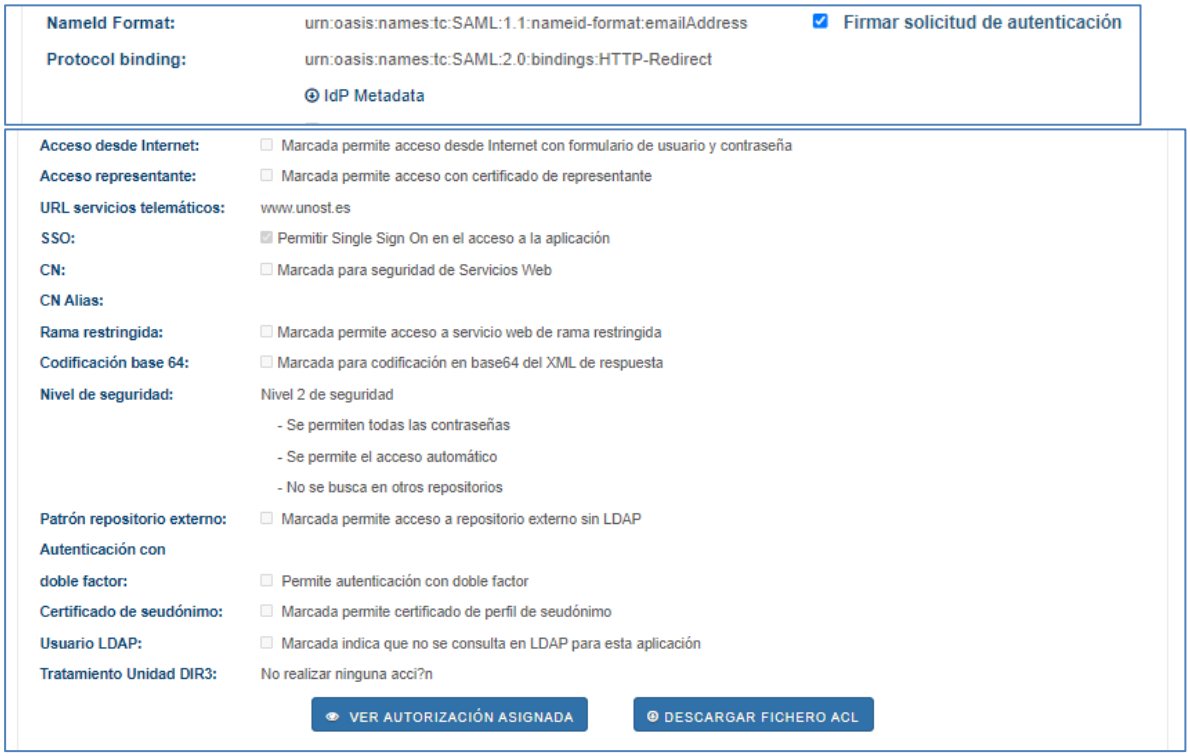
Se mostrará el detalle de la aplicación seleccionada, pudiendo ver también las autorizaciones asignadas a ella.

Detalle aplicación

Identificador:	3142
Nombre:	AsistenteAppParam
Buzón de la aplicación:	asistente@correo.gob.es
Url de respuesta por defecto:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToStepParamGeneric&type=JSP
Url de respuesta 1:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente1
- Descripción:	No especificado
- Nivel de seguridad:	No especificado
Url de respuesta 2:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente2
- Descripción:	No especificado
- Nivel de seguridad:	Nivel 2 (b?sico)
Url de respuesta 3:	https://des-autentica.redsara.es/Asistente/servlet/AsistenteServlet?action=goToAsistente3
- Descripción:	No especificado
- Nivel de seguridad:	Nivel 3 (medio/sustancial)
Url de conexión:	https://des-autentica.redsara.es/Autentica/servlet/AutenticaServlet?action=goToAutentica&appId=3142
IP activa:	☐ Marcada verifica la IP de la aplicación

Activar autorización:	☑ Marcada activa el módulo de autorización ☐ Incluir roles automáticamente al asignar perfil de usuario ☐ Activar servicio correo electrónico de notificación de autorizaciones ☐ Envío notificaciones correo electrónico de administrador ☐ Envío notificaciones correo electrónico genérico
Autorización (no bloquear):	☐ Marcada activa el no bloqueo del acceso a usuarios sin perfiles
Autorización (representantes):	☐ Marcada permite a usuarios representantes de organismos la asignación de autorizaciones
Activar recepción de correos:	☐ Marcada si se desea recibir correos de aviso sobre los usuarios que se dan de alta o de baja en la aplicación.
Responsable:	
DNI:	
Nombre completo:	

Método de autenticación:	SAML Estándar
Configuración de SAML:	
IdP EntityId:	https://des-autentica.redsara.es/samlAutentica/
SP EntityId:	https://circuitsandbox.net/ssologin/callback?provider=sso_cora_test
Service Endpoint:	http://des-autentica.redsara.es/samlAutentica/acs.jsp
Target URL:	http://des-autentica.redsara.es/samlAutentica/acs.jsp
	☑ Marcada si se permite incluir parámetro RelayState
	☑ Marcada si se permite incluir ampersand con parámetro RelayState

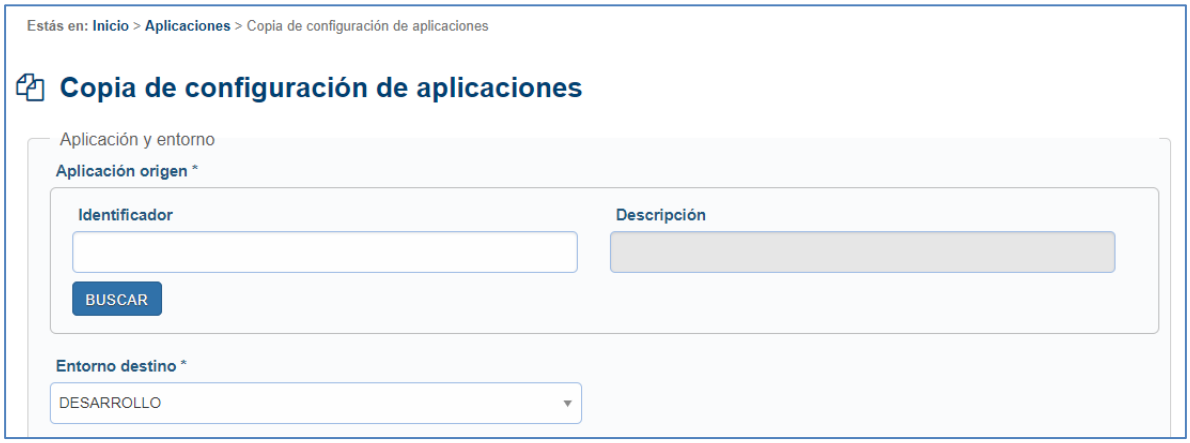


2.4.5. CARGA CONFIGURACIÓN ACL

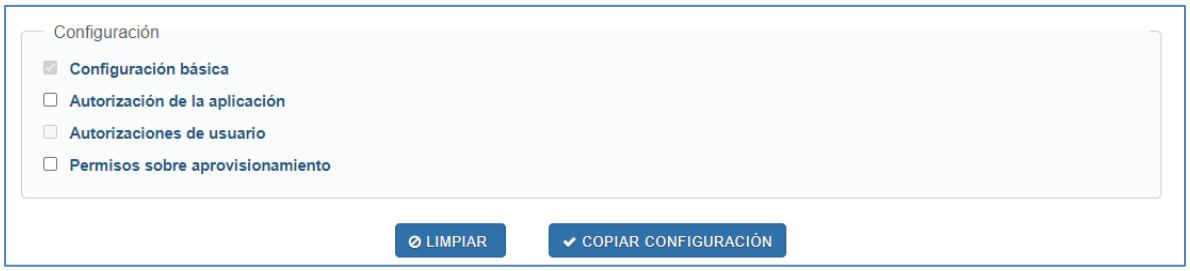
Se seleccionará el fichero de configuración ACL para la carga de datos de la aplicación de manera automática.

2.4.6. COPIA DE APLICACIÓN

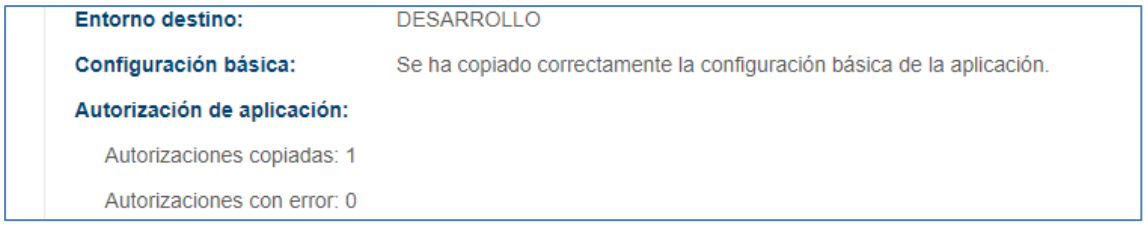
Se seleccionará la aplicación origen indicando el identificador o mediante el botón “Buscar”. Además se debe seleccionar el entorno destino.



Se añadirá el nombre de la aplicación a copiar en destino, en caso de no estar definido, se insertará en destino con nombre aplicación origen terminado en "_Copia". Se seleccionará la aplicación destino en caso que se quiera copiar la configuración sobre la misma y se marcarán los tipos de configuración a copiar.



Una vez seleccionado los datos se copiará la configuración indicada en el entorno destino y se mostrará un resumen de los datos copiados.



Autorización de aplicación:

Autorizaciones copiadas: 1

Autorizaciones con error: 0

Autorización de usuario:

Autorizaciones copiadas: 1

Autorizaciones con error: 0

Permisos sobre aprovisionamiento: Permisos copiados: 2

Permisos con error: 0

2.5. AUTORIZACIÓN

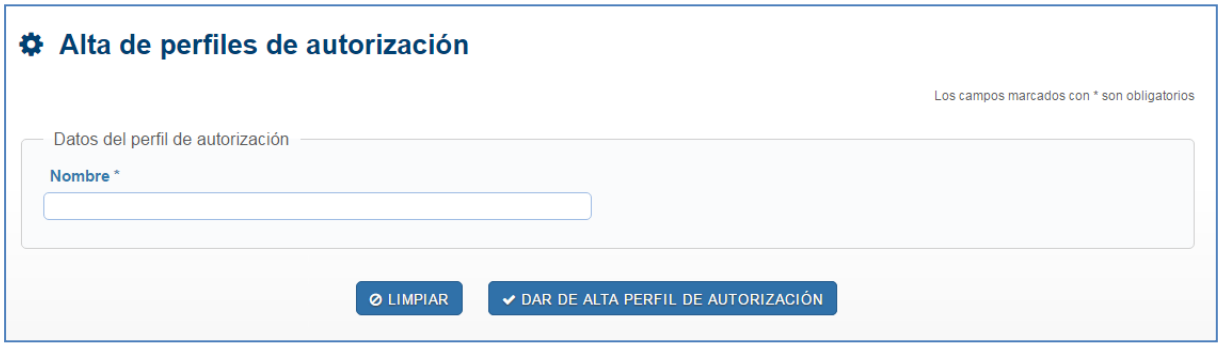
Toda la gestión de autorización por parte de los administradores se hará a través de las opciones accesibles desde la pestaña “Autorización”. Sólo tendrán acceso a esta pestaña los administradores (tanto central como delegado con permiso de autorización)

2.5.1. GESTIÓN DE PERFILES

2.5.1.1. Alta de perfil

En este mantenimiento se dará de alta un perfil, asignándose un nombre descriptivo.

La descripción del perfil no debe ser igual a uno ya existente.

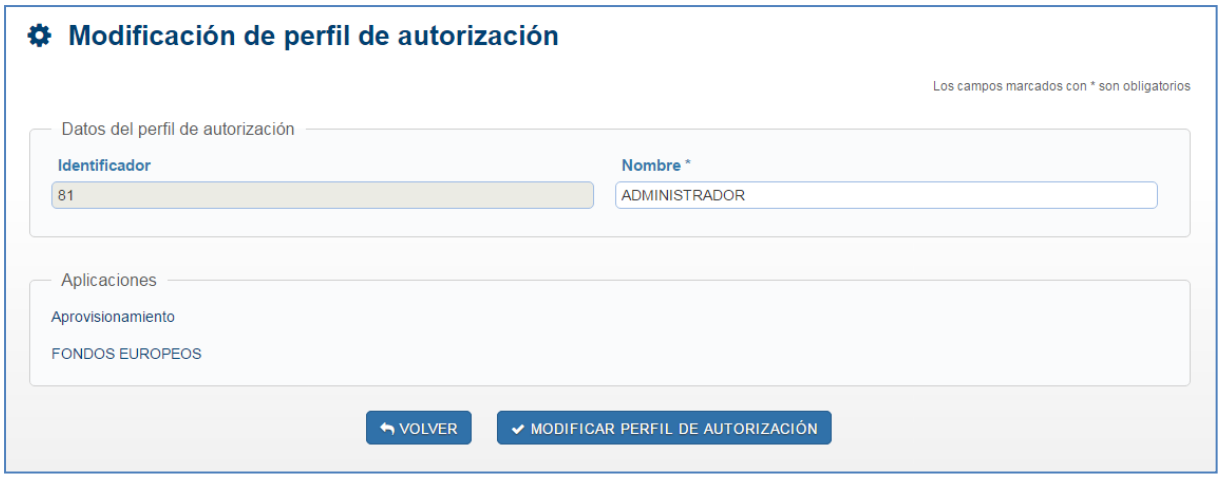


2.5.1.2. Modificación de perfil

El usuario administrador accederá a un listado de perfiles y seleccionará uno para ser modificado.

Para realizar esta modificación tendrá algunos límites:

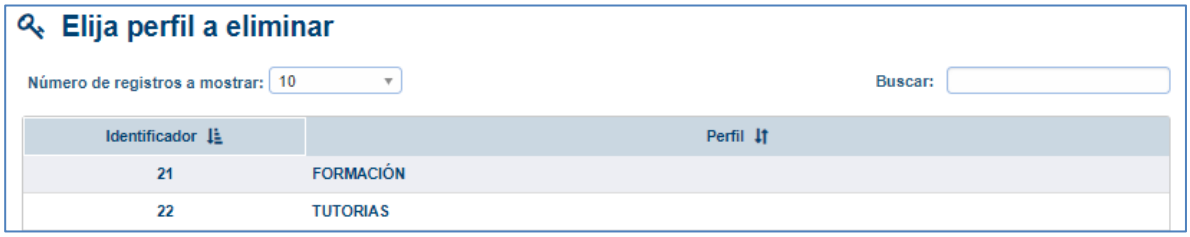
- No podrá modificar el nombre del perfil si el nuevo nombre coincide con el de un perfil ya existente.
- No podrá modificar un perfil que esté siendo utilizado por alguna aplicación.



Desde aquí podrá acceder al detalle de las aplicaciones relacionadas.

2.5.1.3. Baja de perfil

El usuario administrador accederá a un listado de perfiles y seleccionará uno para ser dado de baja.



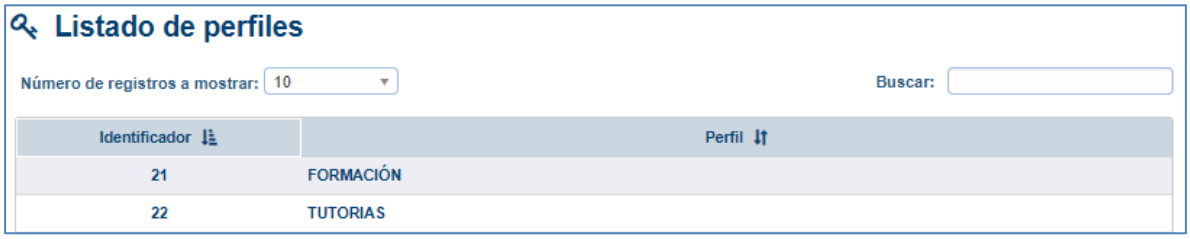
Para realizar una baja de perfil, se tendrán en cuenta las siguientes condiciones:

- Si el perfil que se desea eliminar está siendo utilizado por alguna aplicación, se mostrará al usuario un mensaje indicando que no es posible realizar la baja de ese perfil, indicando las aplicaciones que lo están utilizando así como los responsables de las mismas.

Desde aquí se podrá acceder al detalle de las aplicaciones relacionadas.

2.5.1.4. Listado de perfiles

Se mostrará una opción para acceder al listado de perfiles existentes.



Al pulsar sobre un perfil determinado, se mostrará el detalle del mismo, indicando las aplicaciones que lo están usando y pudiendo acceder a su detalle.

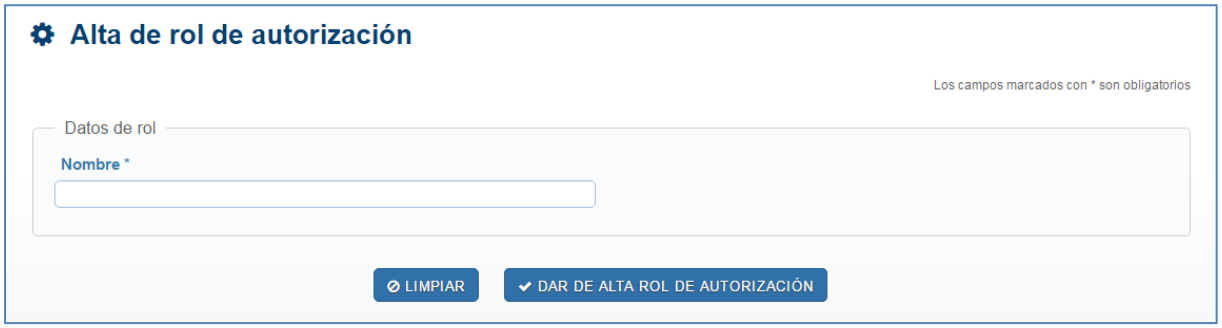
2.5.2. GESTIÓN DE ROLES

El mantenimiento de los roles de autorización se llevará a cabo desde la opción “Gestión de roles”.

2.5.2.1. Alta de rol

En este mantenimiento se dará de alta un rol, asignándose un nombre descriptivo.

La descripción del rol no debe ser igual a uno ya existente.

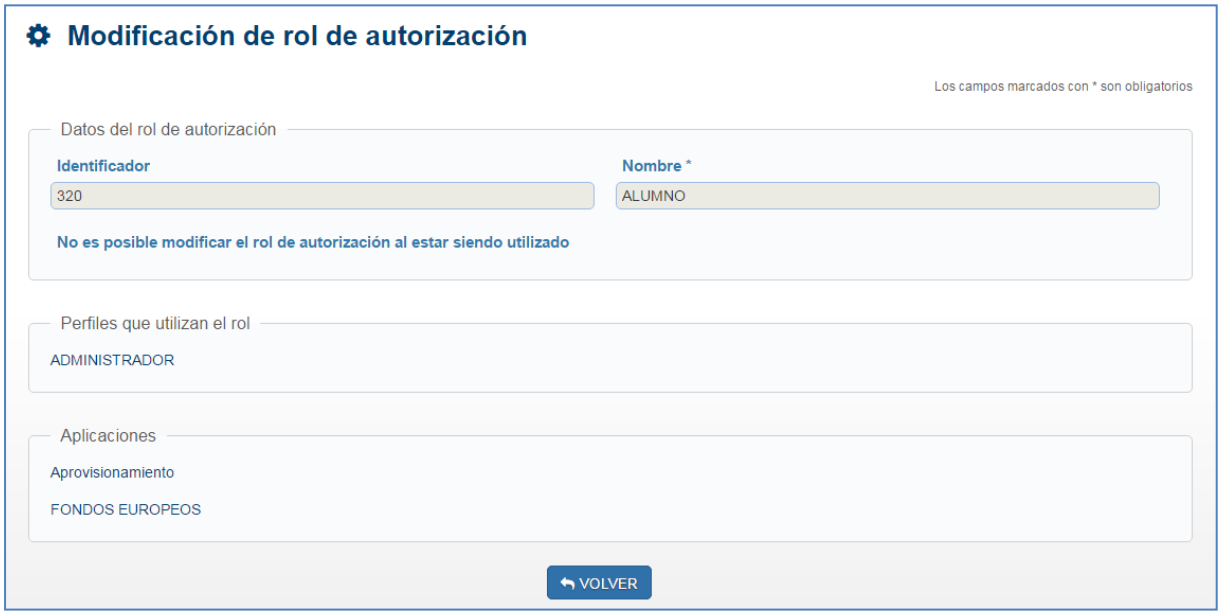


2.5.2.2. Modificación de rol

El usuario administrador accederá a un listado de roles y seleccionará uno para ser modificado.

Para realizar esta modificación tendrá algunos límites:

- No podrá modificar el nombre del rol si el nuevo nombre coincide con el de un rol ya existente.
- No podrá modificar un rol que esté siendo utilizado por alguna aplicación.



Desde aquí podrá acceder al detalle de los roles y las aplicaciones relacionadas.

2.5.2.3. Baja de rol

El usuario administrador accederá a un listado de roles y seleccionará uno para ser dado de baja.

Para realizar una baja de rol, se tendrán en cuenta las siguientes condiciones:

- Si el rol que se desea eliminar está siendo utilizado por alguna aplicación, se mostrará al usuario un mensaje indicando que no es posible realizar la baja de ese rol, indicando las aplicaciones que lo están utilizando así como los responsables de las mismas.

2.5.2.4. Listado de roles

Se mostrará una opción para acceder al listado de roles existentes.

Al pulsar sobre un rol determinado, se mostrará el detalle del mismo, indicando los perfiles y aplicaciones que lo están usando y pudiendo acceder a su detalle.

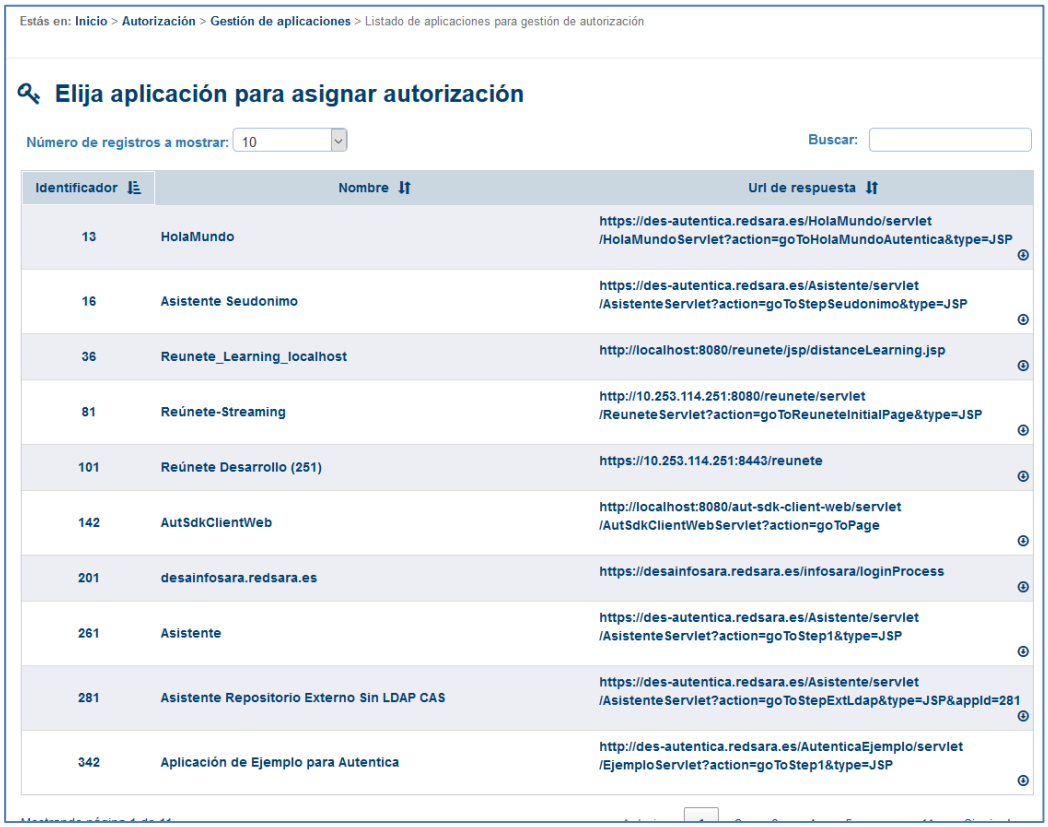
2.5.3. GESTIÓN DE APLICACIONES

El mantenimiento de las aplicaciones se llevará a cabo desde la opción “Gestión de aplicaciones”.

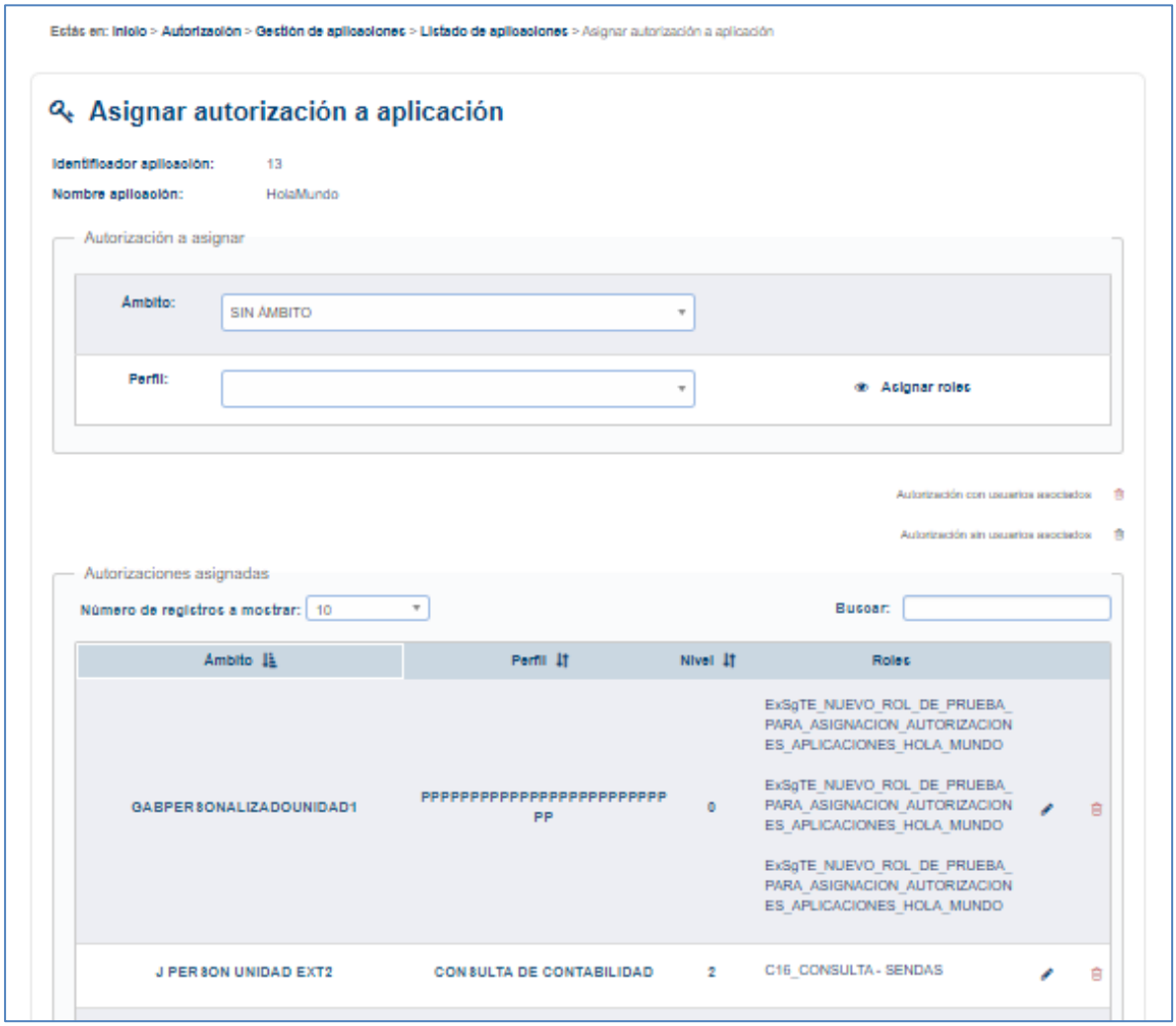
2.5.3.1. Asignar autorización para una aplicación

Un usuario administrador podrá acceder a la opción “Asignar autorización”; para ello, realizará los siguientes pasos:

- Se mostrará el listado de aplicaciones para seleccionar a cual se le quiere asignar una autorización.



- Se accederá a una pantalla donde se muestra en una tabla las autorizaciones que ya tiene asignadas la aplicación con sus niveles y el formulario para asignar autorización.

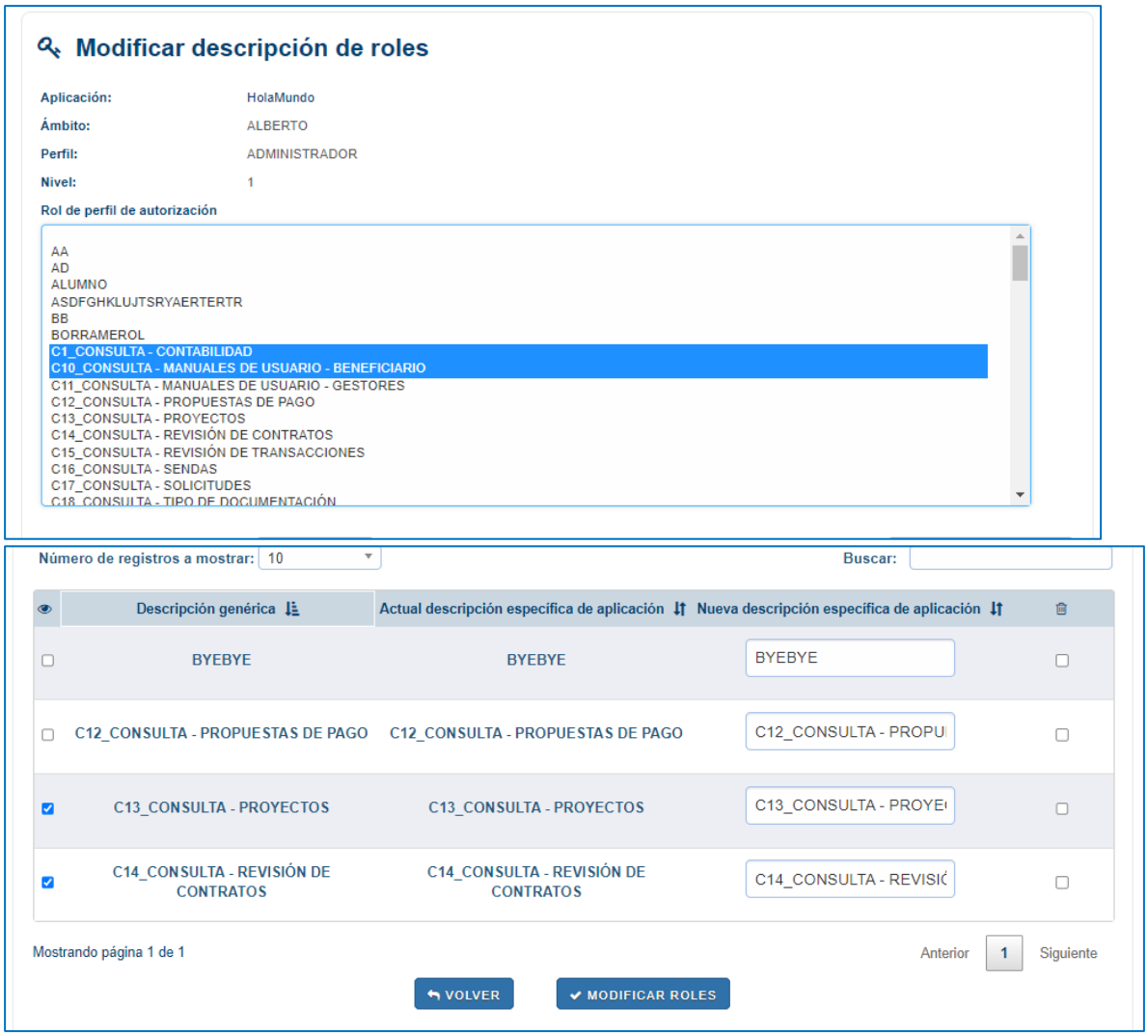


- En el formulario para asignar autorización, se encontrará
  - un desplegable con el ámbito a seleccionar, disponiendo de las siguientes opciones:
    - ÁMBITO PERSONALIZADO: aparecerá una nueva caja para escribir el nuevo ámbito que se quiere dar de alta.
    - ÁMBITO PERSONALIZADO CON UNIDAD: aparecerá una nueva caja para escribir el nuevo ámbito que se quiere dar de alta y se elegirá una unidad orgánica que quedará asociada al ámbito creado.
    - ÁMBITO GEOGRÁFICO: indica que el ámbito de la autorización estará formado por al menos un país, pudiendo añadir provincia_comunidad_localidad.
    - ÁMBITO UNIDAD: indica que el ámbito de la autorización será la unidad organizativa de un usuario.
    - SIN ÁMBITO
    - La lista de ámbitos personalizados ya creados
  - un desplegable con el perfil a seleccionar

- un acceso “Asignar roles” a la página para la asignación de roles de autorización a la aplicación. Antes de acceder a esta página se comprobará que la relación entre el ámbito y perfil seleccionado no existan ya para la aplicación sobre la que se está asignando autorización.

Dentro de la tabla de autorizaciones asignadas podrá realizar 3 acciones:

- Modificar autorización para una aplicación: Se accederá a un formulario donde se podrá cambiar la descripción específica de los roles para esa autorización de la aplicación.
- Se podrán añadir nuevos roles para ese perfil de autorización. Seleccionándolos de la tabla y pulsando el botón de modificar.
- Se pueden eliminar las autorizaciones seleccionando los checks en la columna de la papelera. Y pulsando el botón modificar.
- Se podrá modificar la visibilidad de los roles para la sección de Mis datos y autorizaciones seleccionando los check correspondientes en la columna de visibilidad.



2.5.3.2. Listado de autorizaciones para una aplicación

Un usuario administrador accederá a la opción “Listado de autorizaciones”; para ello, se realizarán los siguientes pasos:

- Se muestra el listado de aplicaciones que tienen configurada alguna autorización.

- Se seleccionará la aplicación a la que se le quiere ver el detalle de la autorización.
- Se accederá a una pantalla donde se muestra en una tabla la autorización que ya tiene asignada la aplicación en modo lectura con sus niveles, con una opción “Ver roles” para cada perfil de autorización.

Al seleccionar la opción “Ver roles” se muestra la descripción de roles y la opción de modificar el nivel de la autorización.

En el desplegable de nivel se podrá seleccionar el nivel a modificar, siendo el nivel 1 el más bajo y el nivel 2 el más alto.

2.5.3.3. Eliminar ámbitos sin utilizar

Con esta funcionalidad se permitirá eliminar los ámbitos que ya no se utilicen y poder limpiar así los ámbitos que se hayan dado de alta y no estén asignados a ninguna aplicación.

2.5.3.4. Carga masiva de autorizaciones de aplicación

Se permitirá a los administradores asignar una relación entre aplicación, ámbito, perfil y rol de manera masiva utilizando un fichero en formato CSV para ello.

A la derecha de la pantalla habrá un link para descargar un fichero plantilla en el que vendrán especificados los campos a rellenar por línea de usuario.

Dicho fichero contendrá los siguientes datos:

- ***version_#*** *(Obligatorio): Versión de la plantilla para la carga. El símbolo # se sustituye en la plantilla descargable por la última versión. El valor del campo no se debe modificar ni eliminar y no se debe rellenar la columna correspondiente.*

  Ejemplo: version_1.0

- ***ID_APLICACION*** *(Obligatorio): Código de aplicación en el entorno donde se haga la carga*
- ***PERFIL*** *(Obligatorio): Nombre del perfil*
- ***ROL*** *(Obligatorio): Nombre del rol*
- ***AMBITO*** *(Obligatorio): Nombre o descripción del ámbito*

Ejemplos:

version_1.0	ID_APLICACION	PERFIL	ROL	AMBITO
	101	*AAAAAAA*	*C6_CONSULTA - FONDOS2007*	*J PERSON UNIDAD EXT2*
	13	*PRUEBA22*	BB	*PERDIENDO*
	101	*ASESOR JURÍDICO (REA)*	AA	*SERVINOMINA1*
	13	*BENEFICIARIO*	BB	*GABPERSONALIZADOUNIDAD*

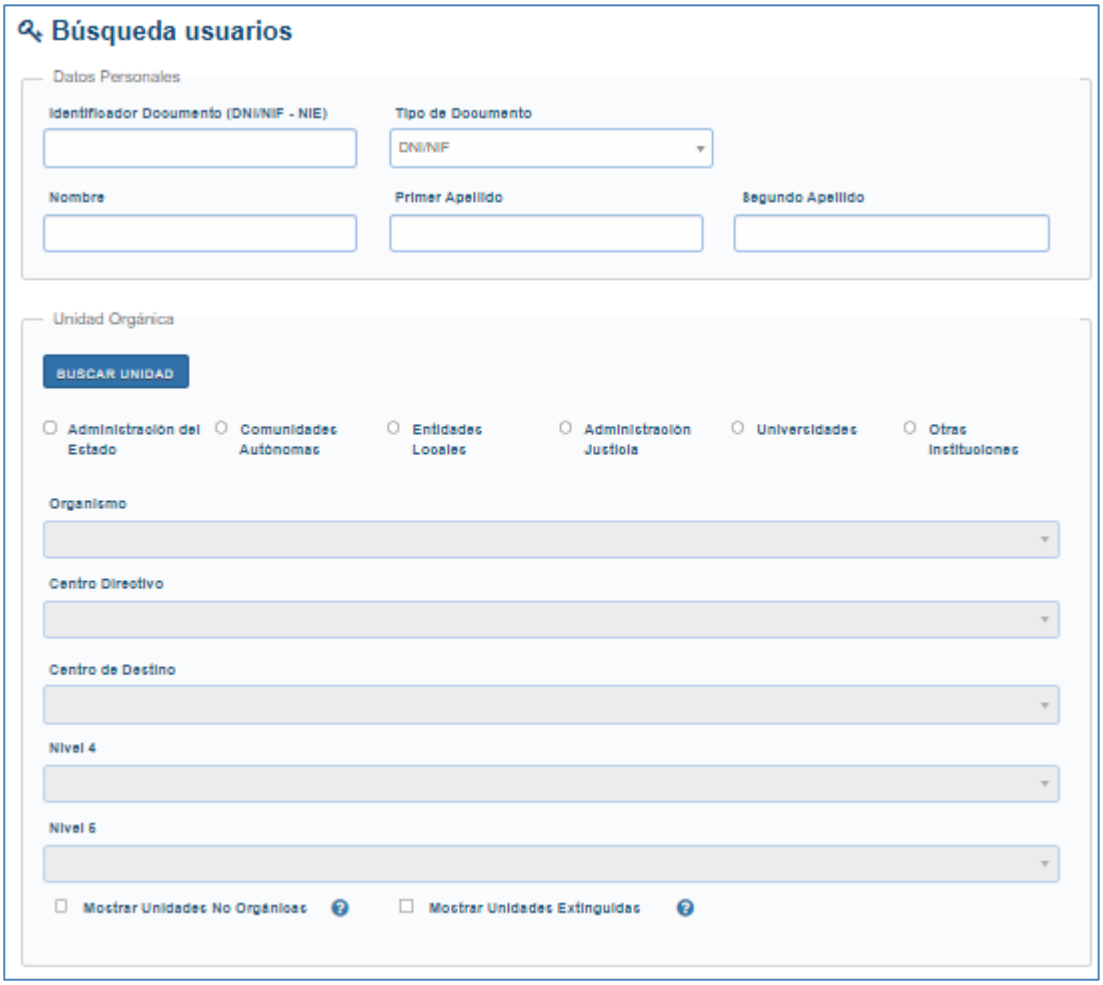
Una vez editado el fichero que se quiere cargar, se selecciona y se pulsa el botón “Cargar” para proceder a la carga de los datos.

Se contrasta que la versión empleada en la plantilla es la más actual para la carga masiva de autorizaciones de aplicación.

Después de terminar la carga, saldrá por pantalla el resultado de esta, junto con una opción para poder descargarse un fichero con esta información.

2.5.4. AUTORIZACIÓN DE USUARIOS

Se podrán dar de alta, modificar y eliminar autorizaciones de usuarios. Para cualquiera de estas opciones, se accede a la opción “Autorización de usuarios” donde se muestra un buscador de usuarios.



En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Marcando el check ‘Permitir unidades extinguidas’, se mostrarán en los combos Unidades orgánicas que ya no tienen estado Vigente sino Extinguido.

Una vez que se hayan buscado, se muestran los resultados en una tabla con los datos DNI, nombre y apellidos y tipo de empleado; para cada usuario se tiene enlace a la asignación de autorizaciones y uno de copia de autorizaciones de usuario.

2.5.4.1. Alta de autorización para un usuario

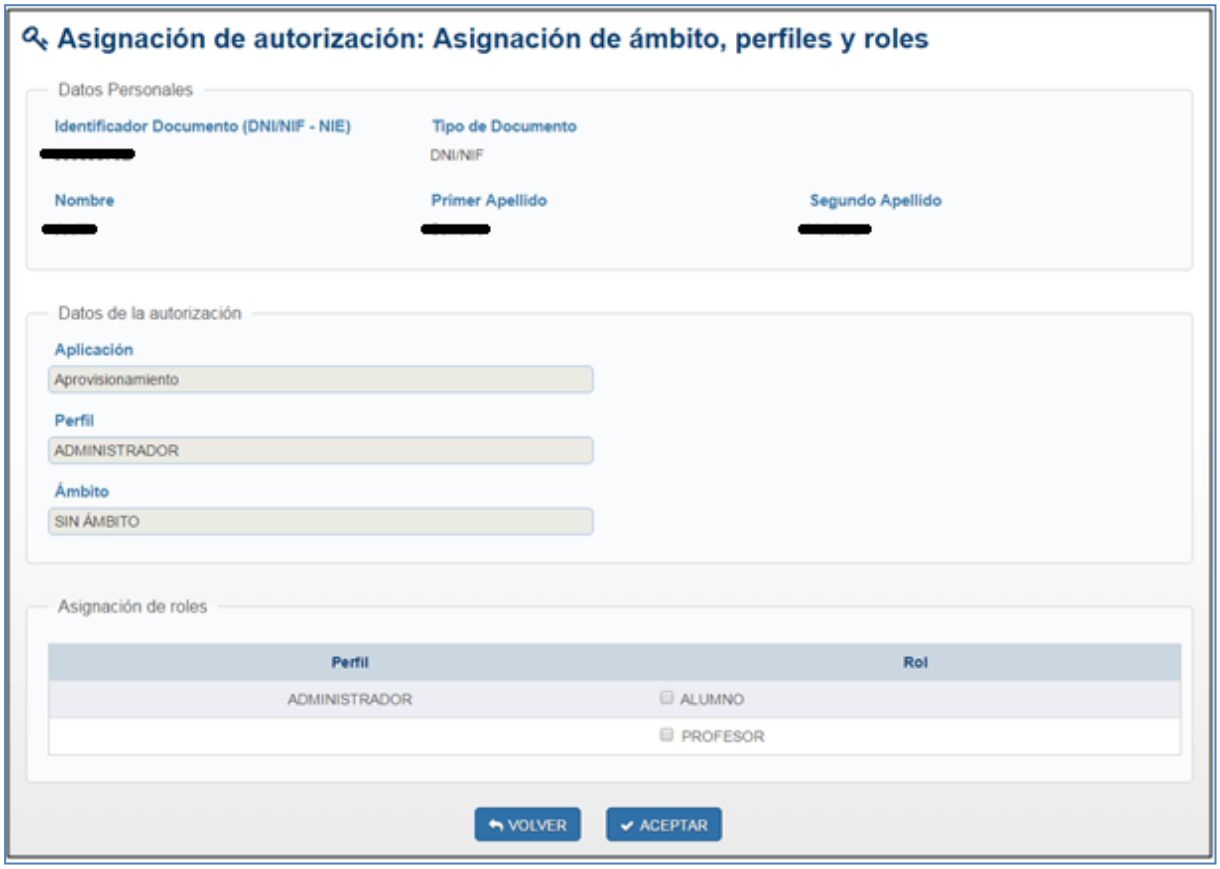
Mediante esta opción, se asigna autorización a un usuario sobre una aplicación de la que no tenga ningún tipo de autorización.

Sobre el listado de usuarios encontrados según el filtro de búsqueda especificado, se pulsa sobre los datos del usuario mostrados en la tabla y se muestran los siguientes datos:

- Una tabla con las aplicaciones sobre las que ya tiene asignada autorización el usuario.
- Una tabla con las aplicaciones que tienen definida autorización y sobre las cuáles el usuario no dispone ningún tipo de autorización

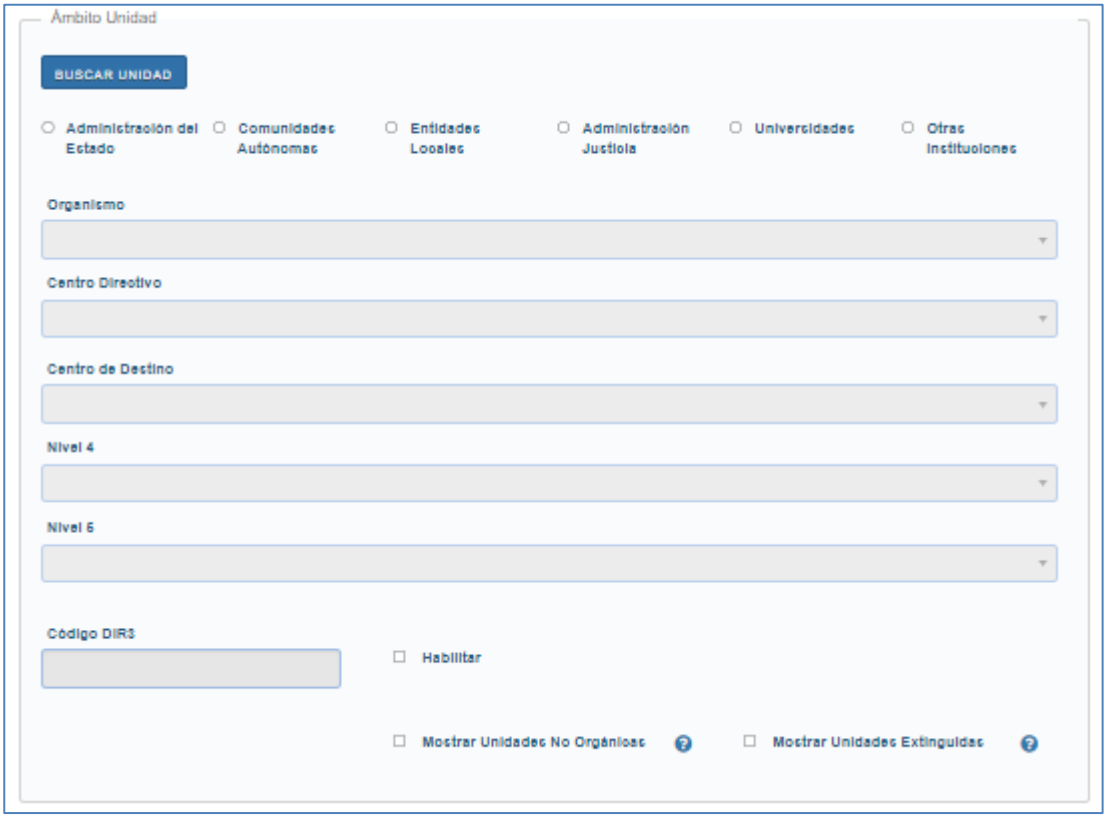
Se pulsa sobre la aplicación a la que se quiere asignar autorización y se muestra una tabla con la autorización que se puede seleccionar para un usuario. En el caso de que alguna autorización esté definida con el ámbito unidad, se muestran una autorización para cada unidad a la que pertenezca el usuario.

La pantalla será distinta dependiendo el tipo de ámbito que se haya elegido. En todos los casos se tendrá que elegir el Rol.

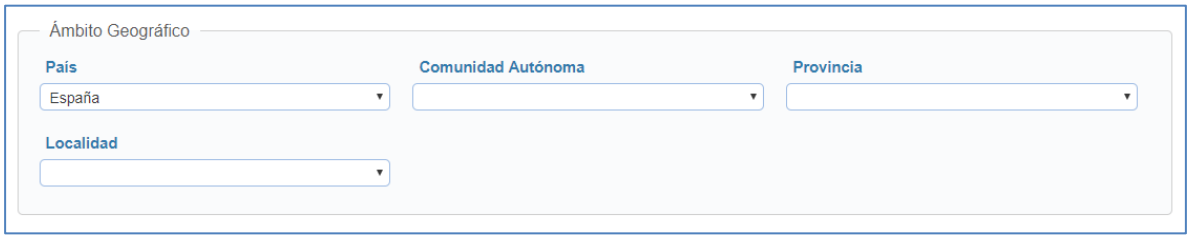


Para ámbito Unidad, se tendrá que elegir una unidad desde los desplegables o directamente poniendo el código DIR3. Se podrá seleccionar o introducir el código de una unidad con nivel de profundidad superior al nivel 5; los desplegables para niveles superiores a nivel 5 se muestran al seleccionar una unidad de nivel inferior. Marcando el check 'Permitir Unidades Extinguidas', se podrá hacer la autorización sobre unidades en estado Extinguido.

En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Para ámbito Geográfico, se tendrá que elegir desde los desplegables la Comunidad, Provincia o Localidad de la autorización.



Una vez que se seleccione autorización, se pulsa sobre el botón “Aceptar”, se muestra un mensaje de confirmación y se confirma la asignación.

2.5.4.2. Modificación de autorización para un usuario

Mediante esta opción, se modifica autorización a un usuario sobre una aplicación de la que ya disponga algún tipo de autorización.

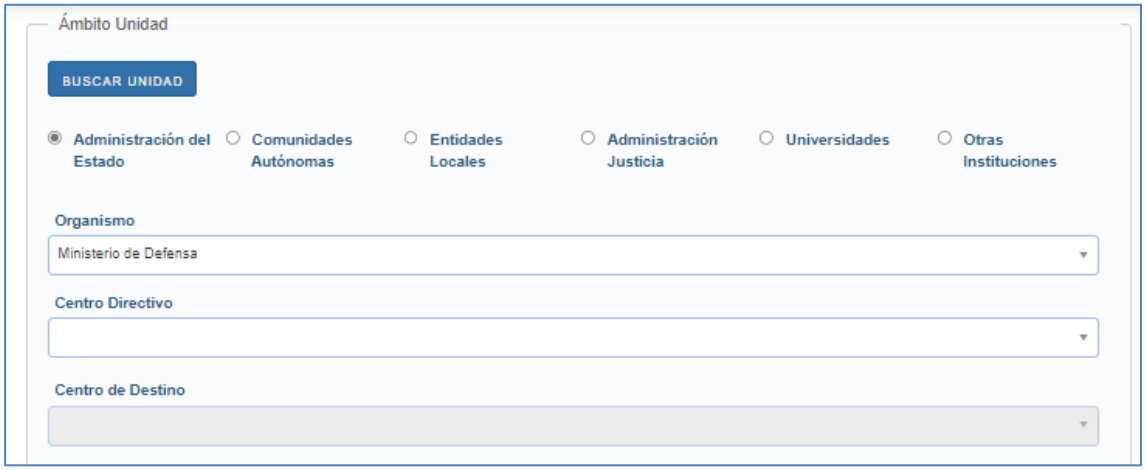
Sobre la pantalla de asignación de autorizaciones correspondiente a una aplicación determinada se pulsa sobre el ícono de modificación que se muestra en la tabla con las autorizaciones. Se mostrara un check marcado en caso de que sea recursiva la autorización.

Se muestra una tabla con la autorización ya definida para ese usuario y aplicación. En el caso de que alguna autorización esté definida con el ámbito unidad, se muestra una autorización para cada unidad a la que pertenezca el usuario.

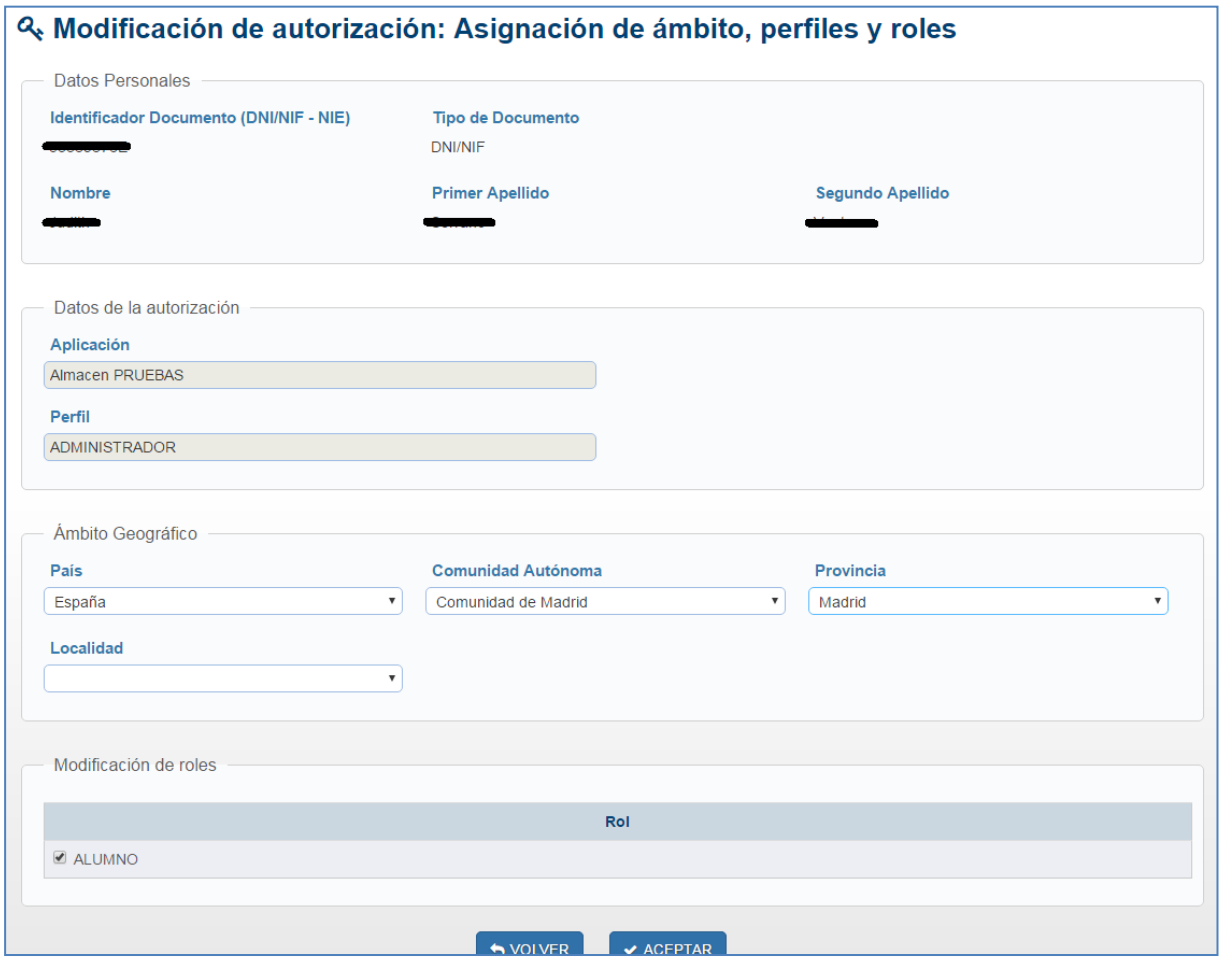
La pantalla variará dependiendo del ámbito de la autorización.

En ámbito unidad se cargará la unidad definida con los niveles superiores a la misma. Se podrá seleccionar una unidad con nivel de profundidad superior al nivel 5; los desplegables para niveles superiores a nivel 5 se muestran al seleccionar una unidad de nivel inferior.

En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Una vez que se seleccione la nueva autorización definida para el usuario y aplicación, se pulsa sobre el botón “Aceptar”. Se muestra un mensaje de confirmación y se confirma la modificación.



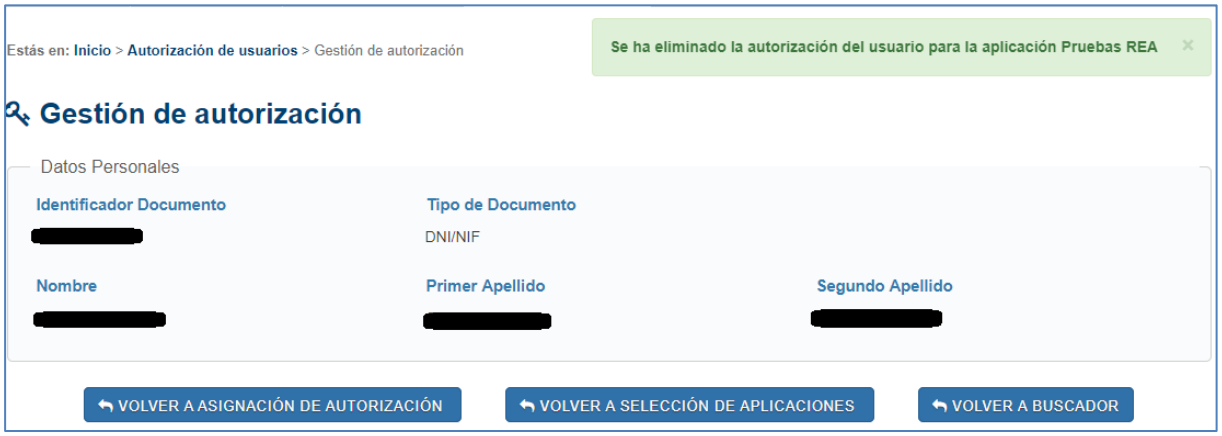
2.5.4.3. Eliminación de autorización para un usuario

Mediante esta opción, se elimina autorización a un usuario sobre una aplicación de la que ya disponga algún tipo de autorización.

Sobre la pantalla de asignación de autorizaciones correspondiente a una aplicación determinada se pulsa sobre el ícono de eliminación que se muestra en la tabla con las autorizaciones.

Se muestra una tabla con la autorización ya definida para ese usuario y aplicación. En el caso de que alguna autorización esté definida con el ámbito unidad, se muestra una autorización para cada unidad a la que pertenezca el usuario.

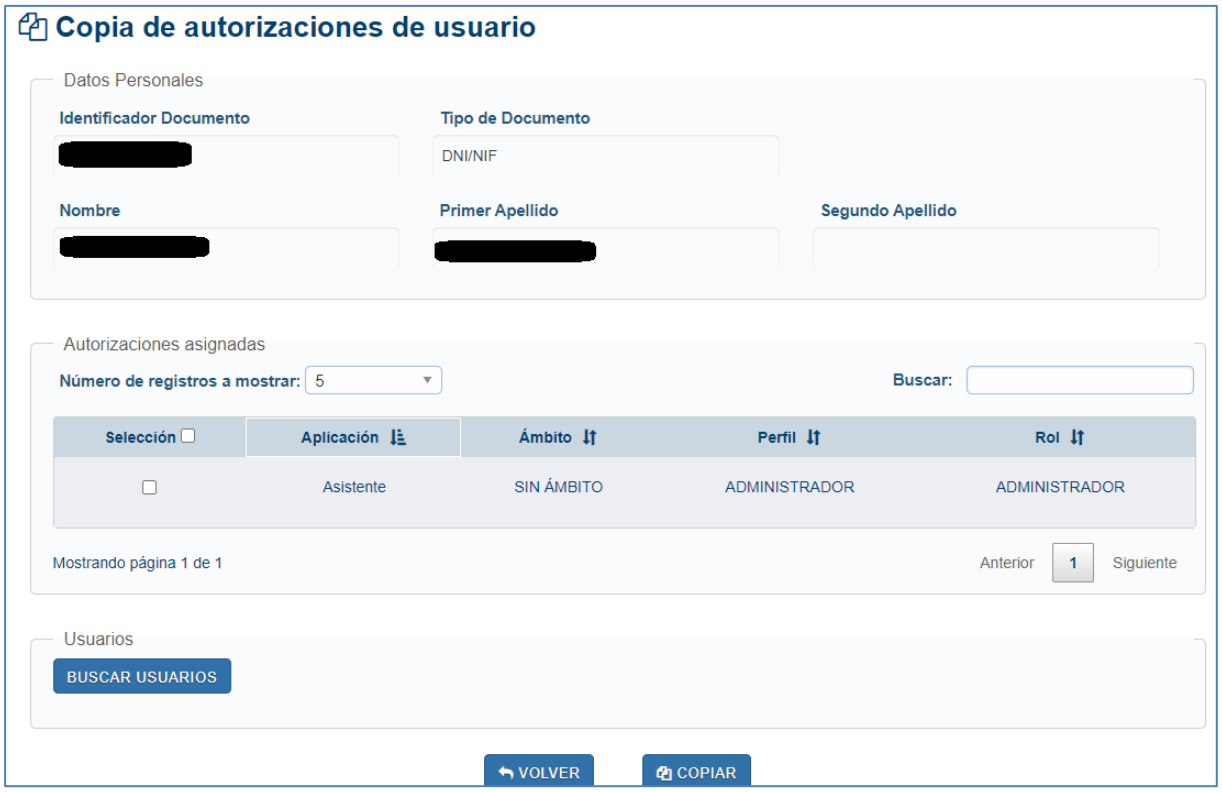
Se selecciona la autorización que se desea eliminar y se pulsa sobre el botón “Aceptar”. Se muestra un mensaje de confirmación y se confirma la eliminación.



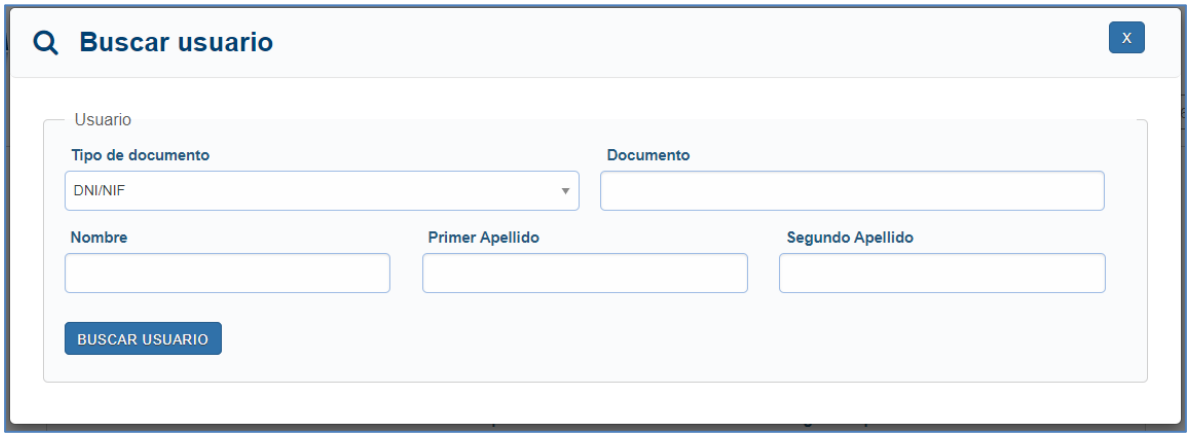
Nos llevará a una pantalla mostrándonos si el resultado ha sido correcto y dándonos la opción de volver a la Asignación de autorización, a la Selección de aplicaciones o al Buscador.

2.5.4.4. Copia de autorizaciones de usuario

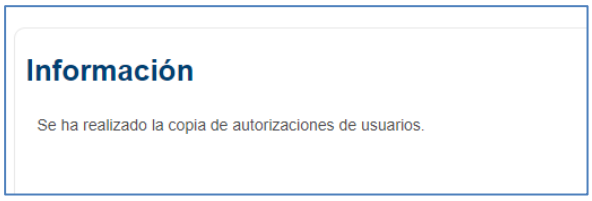
Una vez seleccionada la opción de copia del listado de usuarios se podrá realizar una copia de las autorizaciones seleccionadas a los usuarios deseados. Se mostrará la pantalla de copia, con los datos del usuario de referencia, las autorizaciones asignadas al mismo con la opción de seleccionar las autorizaciones requeridas; así como la búsqueda de usuario a los que se les asignarán las autorizaciones seleccionadas.



Se buscan los usuarios a asignar las autorizaciones mediante la ventana flotante.



Una vez seleccionadas las autorizaciones y los usuarios a asignar, se realiza la copia de las mismas y se muestra el resultado de la copia.

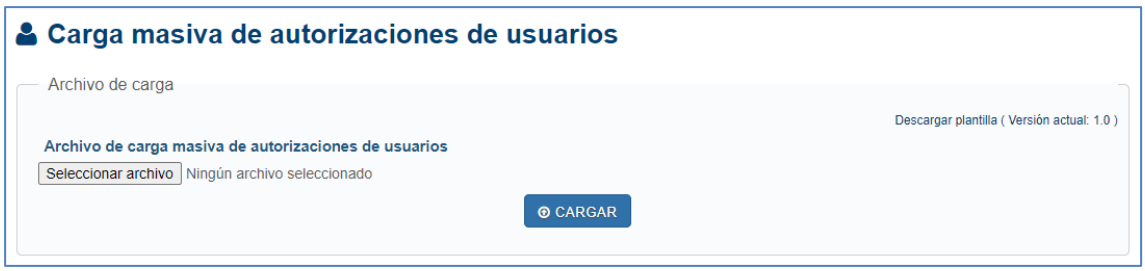


2.5.4.5. Nota importante sobre los identificadores

Los identificadores de Aplicación, Ámbito, Perfil y Rol de una autorización, serán distintos dependiendo del entorno en que se encuentre el usuario

2.5.5. CARGA MASIVA DE AUTORIZACIONES DE USUARIO

Se permitirá a los administradores asignar permisos a usuarios de manera masiva utilizando un fichero en formato CSV para ello.



A la derecha de la pantalla habrá un link para descargar un fichero plantilla en el que vendrán especificados los campos a rellenar por línea de usuario.

Dicho fichero contendrá:

- ***version_#*** *(Obligatorio): Versión de la plantilla para la carga. El símbolo # se sustituye en la plantilla descargable por la última versión. El valor del campo no se debe modificar ni eliminar y no se debe rellenar la columna correspondiente.*

Ejemplo: version_1.0

- ***COD APLICACIÓN*** *(Obligatorio): Código de aplicación para la que se asignaran los permisos. Formato: Numérico 4 caracteres. Si desconoce el código de aplicación, consultar con el responsable de la aplicación*
- ***DNI/NIE*** (*Obligatorio): NIF/NIE con formato 00000000T (sin guión y completando con ceros a la izquierda hasta 9 caracteres) Si desconoce el código de aplicación, consultar con el responsable de la aplicación*
- ***PERFIL*** *(Obligatorio): Nombre del perfil Consulte con el responsable de la aplicación para conocer el valor. Consulte con el responsable de la aplicación para conocer el valor*
- ***ROL*** *(Obligatorio): Nombre del rol. Consulte con el responsable de la aplicación para conocer el valor*
- ***AMBITO*** (*Obligatorio): Nombre o descripción del ámbito sobre el que tendrá efecto la autorización.*

  Valores permitidos y obligatorios:

  - *"SIN ÁMBITO" Indica que no se limitan a una o varias unidades orgánicas. Si se deja en blanco, tendrá el mismo efecto.*
  - *"ÁMBITO UNIDAD" Indica la unidad orgánica sobre la que tendrán efecto la autorización. Será obligatorio cumplimentar el campo UNIDAD con el código DIR3*
  - *"ÁMBITO GEOGRAFICO" Será obligatorio cumplimentar los campos (PAÍS, COMUNIDAD, PROVINCIA, LOCALIDAD, ENTIDAD LOCAL) en función del nivel que deseamos asignar.*
  - *Si es otra descripción, comprobará que coincide con una válida*
- ***COD UNIDAD DIR3*** *(Opcional): Código de unidad orgánica DIR3 del usuario, alfanumérico de 9 posiciones, con la siguiente composición: E00000000*
- ***NOMBRE PAÍS*** *(Opcional): Nombre país. . En caso de que el valor del campo ÁMBITO, sea ÁMBITO GEOGRÁFICO, será obligatorio cumplimentar al menos, los campos PAIS y COMUNIDAD.*
- ***NOMBRE COMUNIDAD AUTÓNOMA*** *(Opcional): Nombre comunidad autónoma. En caso de que el valor del campo ÁMBITO, sea ÁMBITO GEOGRÁFICO, será obligatorio cumplimentar al menos, los campos PAIS y COMUNIDAD.*
- ***NOMBRE PROVINCIA*** *(Opcional): Nombre provincia*
- ***NOMBRE LOCALIDAD*** *(Opcional): Nombre localidad*
- ***ENTIDAD LOCAL*** *(Opcional):*
  - *01 – Si es entidad local*
  - *04 – Si es entidad local menor*

  El valor introducido tendrá que coincidir con el id entidad geográfica de la localidad

- ***CREAR RELACIÓN*** *(Obligatorio):*
    - *0 – Si no existe la relación con la aplicación, no se inserta el usuario*
    - *1 – Si no existe la relación con la aplicación, se crea y se inserta el usuario*

Ejemplos:

version_1.0	*COD APLICACIÓN*	*DNI/NIE*	*PERFIL*	*ROL*	*AMBITO*	*COD UNIDAD DIR3*	*NOMBRE PAÍS*
	1562	*00000000T*	*TUTORIA*	*ALUMNO*			
	1562	*00000000T*	*TUTORIA*	*ALUMNO*	*ÁMBITO UNIDAD*	*EA0008567*	
	1562	*00000000T*	*TUTORIA*	*ALUMNO*	*ÁMBITO GEOGRÁFICO*		*España*
	1562	*00000000T*	*TUTORIA*	*ALUMNO*	*FACTURACIÓN*		

NOMBRE COMUNIDAD AUTÓNOMA	*NOMBRE PROVINCIA*	*NOMBRE LOCALIDAD*	*ENTIDAD LOCAL*	*CREAR RELACION*
				1
				1
Andalucía	*Granada*			*1*
				1

Una vez editado el fichero que se quiere cargar, se selecciona y se pulsa el botón “Cargar” para proceder a la carga de los datos.

Se contrasta que la versión empleada en la plantilla es la más actual para la carga masiva de autorizaciones de usuarios.

2.5.6. SINCRONIZACIÓN DIR3

Se permitirá tramitar los permisos de autorización de usuario, en caso de cambio en su unidad DIR3 asociada y que su aplicación no tenga seleccionado el tratamiento a seguir.

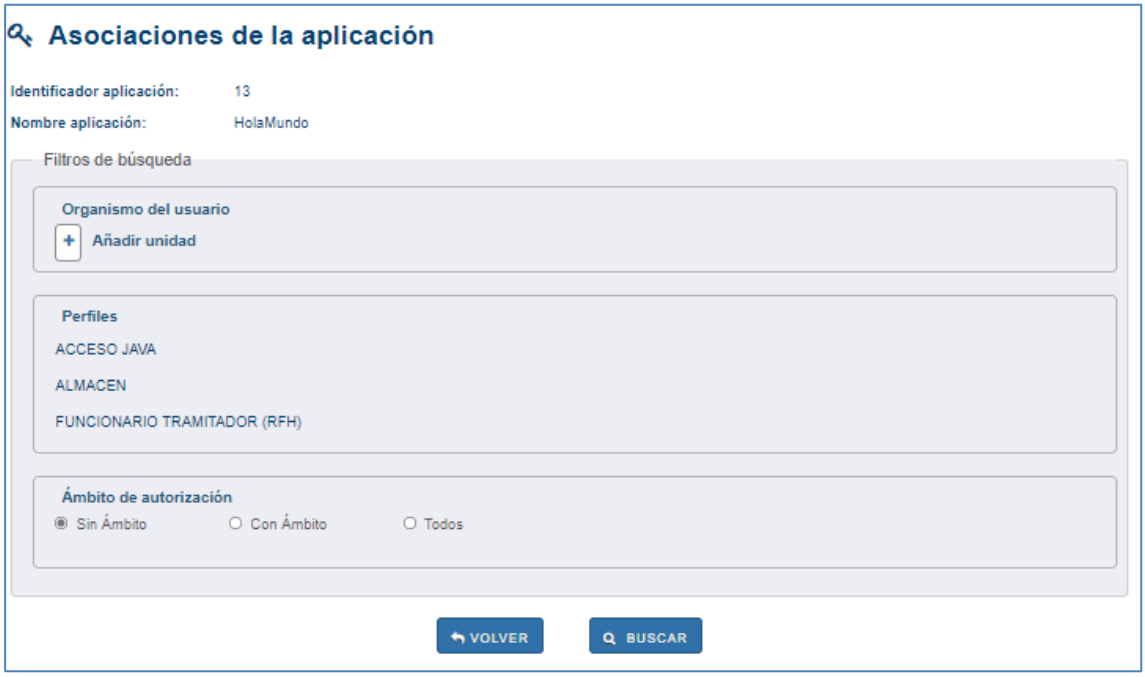
2.5.7. BÚSQUEDA USUARIOS PERFIL

Un usuario administrador, con permiso de autorización avanzada, dentro del apartado de autorización, podrá consultar los roles asociados a los usuarios que a su vez posean una autorización para usar una aplicación; para ello, se realizarán los siguientes pasos:

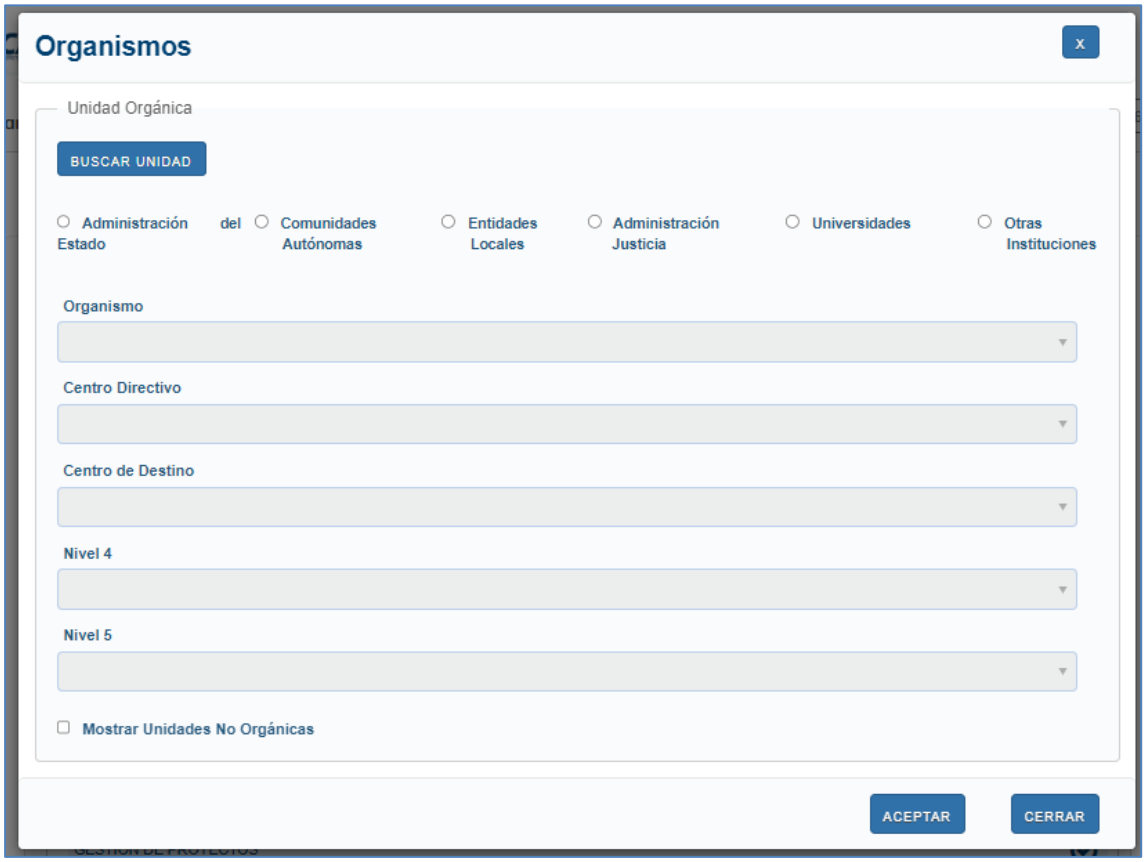
- Se mostrará el listado de aplicaciones que tienen configurada alguna autorización.

- Se seleccionará la aplicación de la que se quieren consultar los roles y se mostrará la pantalla de asociación de la aplicación con los filtros de búsqueda. Dichos filtros están dados por:
    - Organismo del usuario: se podrá seleccionar una unidad DIR3 de modo que únicamente se muestren en los resultados usuarios que pertenezcan a dicha unidad. Se podrá indicar recursividad.
    - Perfiles: se mostrará un multiselect con los perfiles disponibles en la aplicación limitados por el nivel de administración.

Ámbito de autorización: habrá un radio button que permitirá seleccionar Sin Ámbito, Con ámbito o todos. En caso de seleccionar “Con ámbito”, se podrán agregar ámbitos a la consulta, pero únicamente aquellos sobre los que el AD tenga permisos de administración.



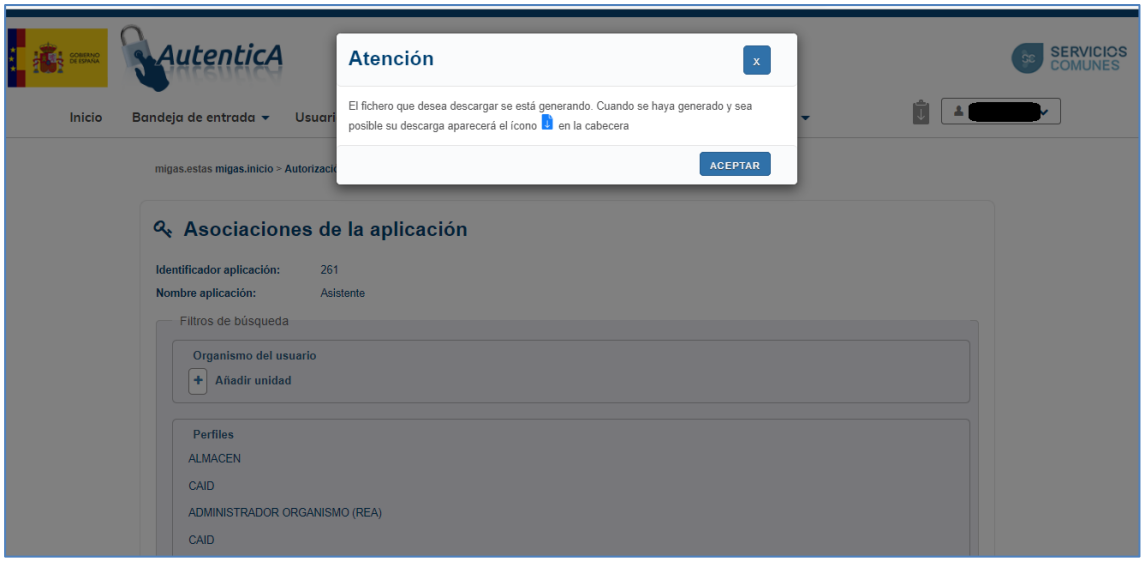
En el apartado “Organismo del usuario”, se podrá añadir unidad que mostrará un cuadro para la selección de la misma. En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Una vez seleccionados los filtros se realiza la consulta, la cual lanzará directamente la generación del informe, sin permitir consulta online por la interfaz de usuario.

Además, se podrá descargar el listado de usuarios desde la pantalla de listado de aplicaciones.

Si el fichero a descargar es pesado se generará de manera asíncrona, se muestra una notificación y un ícono de color gris en la cabecera indicando que se están generando ficheros.

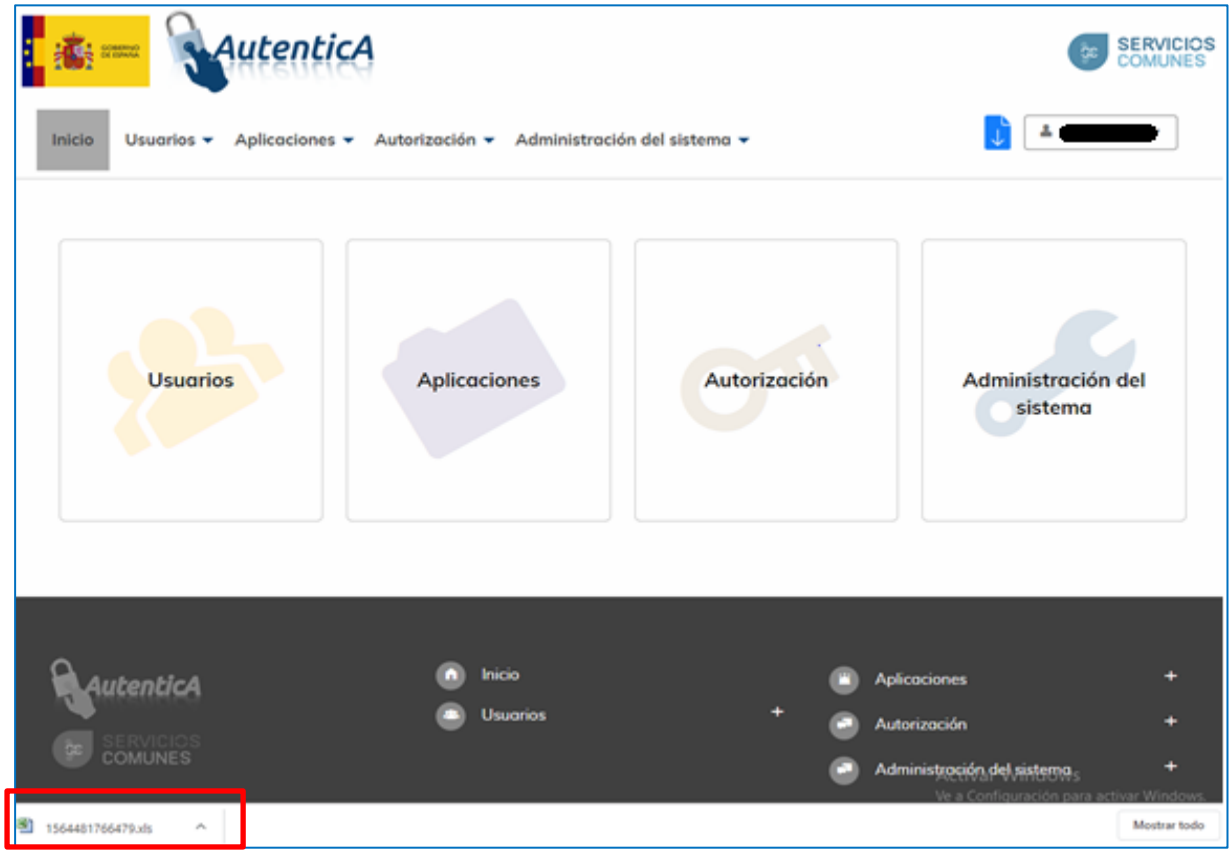


Una vez generado el fichero se muestra en la cabecera un ícono de color azul indicando que se tienen notificaciones pendientes y que el fichero está disponible para la descarga.

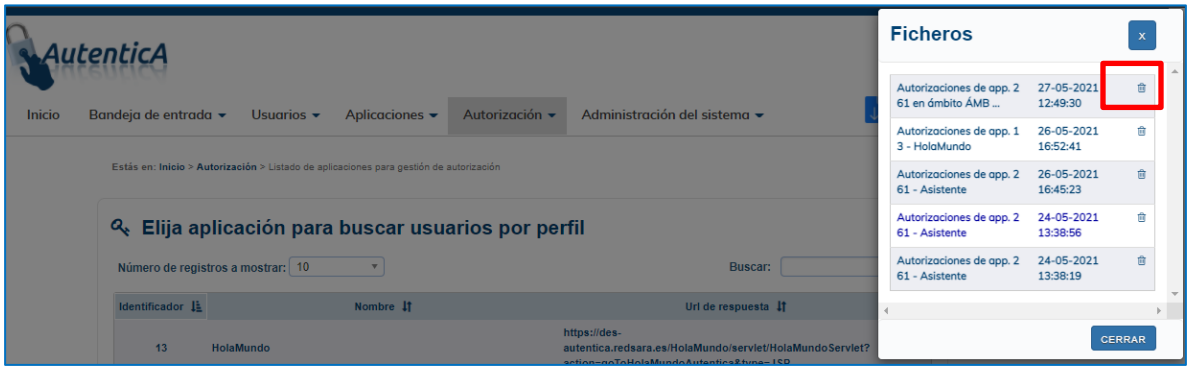
Para gestionar los ficheros disponibles se deben seguir los siguientes pasos:

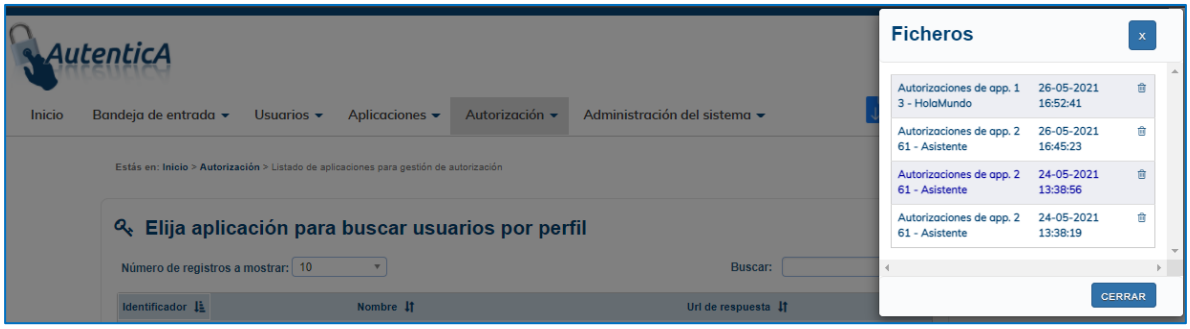
- Se pulsa en el ícono de notificaciones pendientes y se muestra una capa con el listado de ficheros disponibles con el nombre del fichero, la fecha de creación y la opción de borrado del mismo. Si el fichero ha sido descargado al menos una vez se muestra el registro en otro color.

- Se pulsa sobre nombre del fichero y este es descargado.



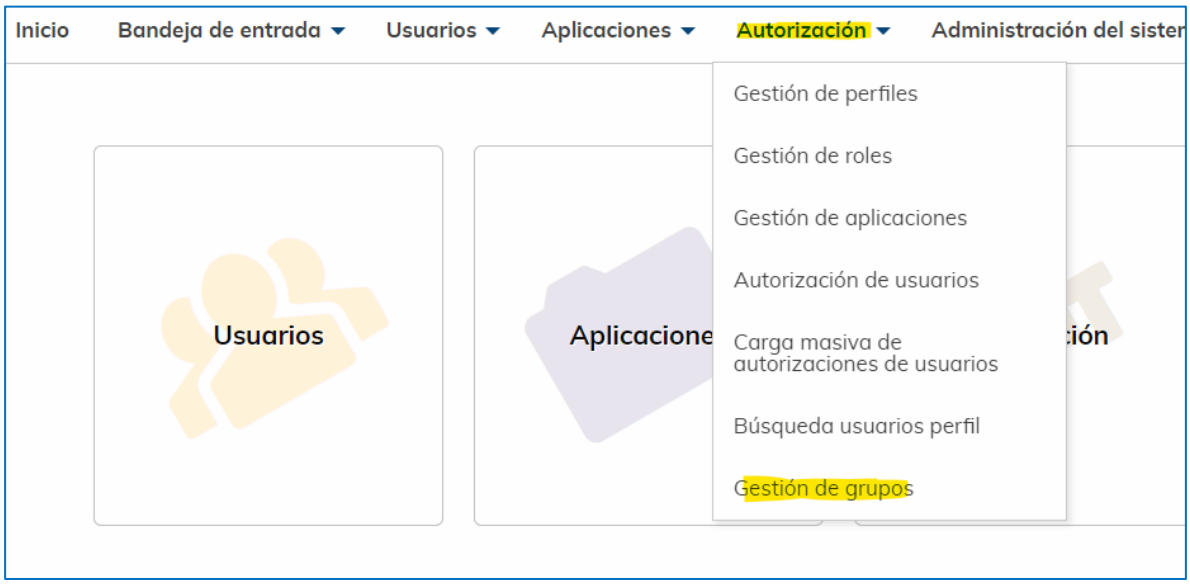
- Para eliminar el fichero se pulsa sobre el ícono de borrado y se actualiza la capa con el listado de ficheros.



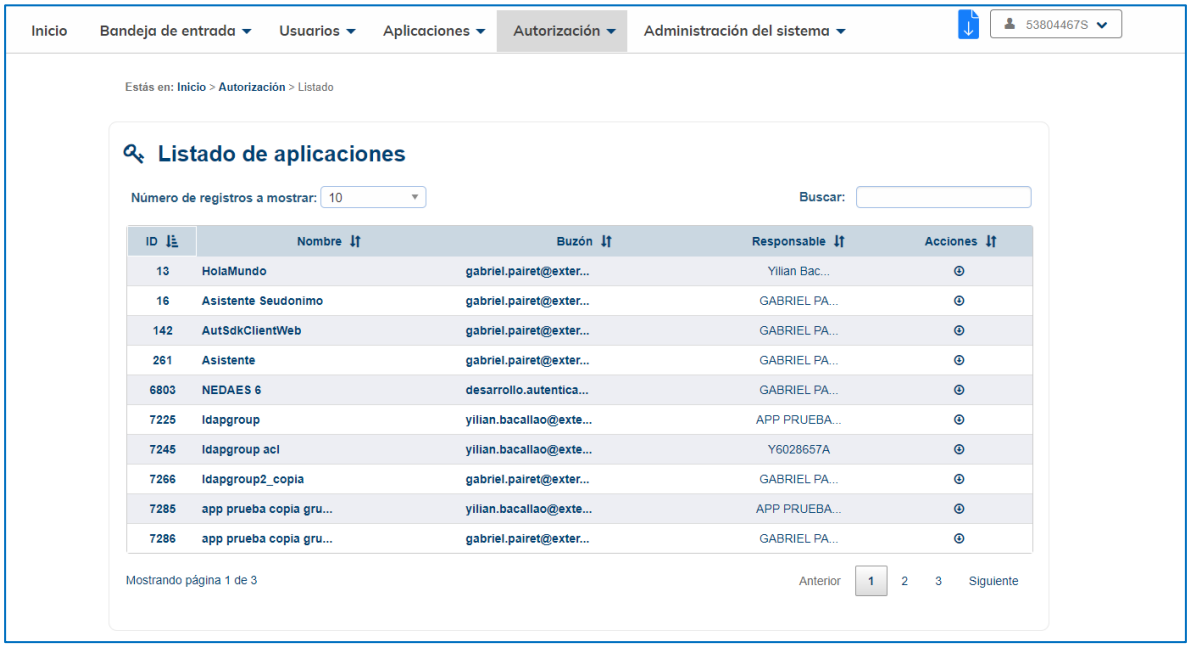


2.5.8. GESTIÓN DE GRUPOS

En el menú de autorizaciones nos encontramos el botón para acceder a la sección de gestión de grupos. Necesitaremos ser usuario administrador, o tener usuario delegado con permisos en autorización.

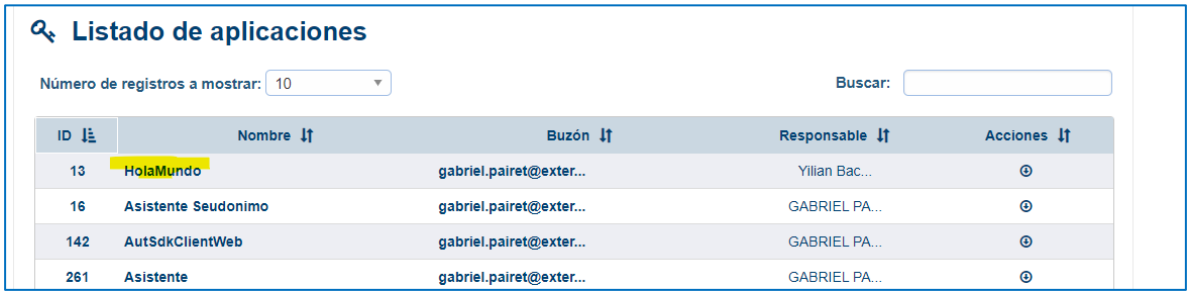


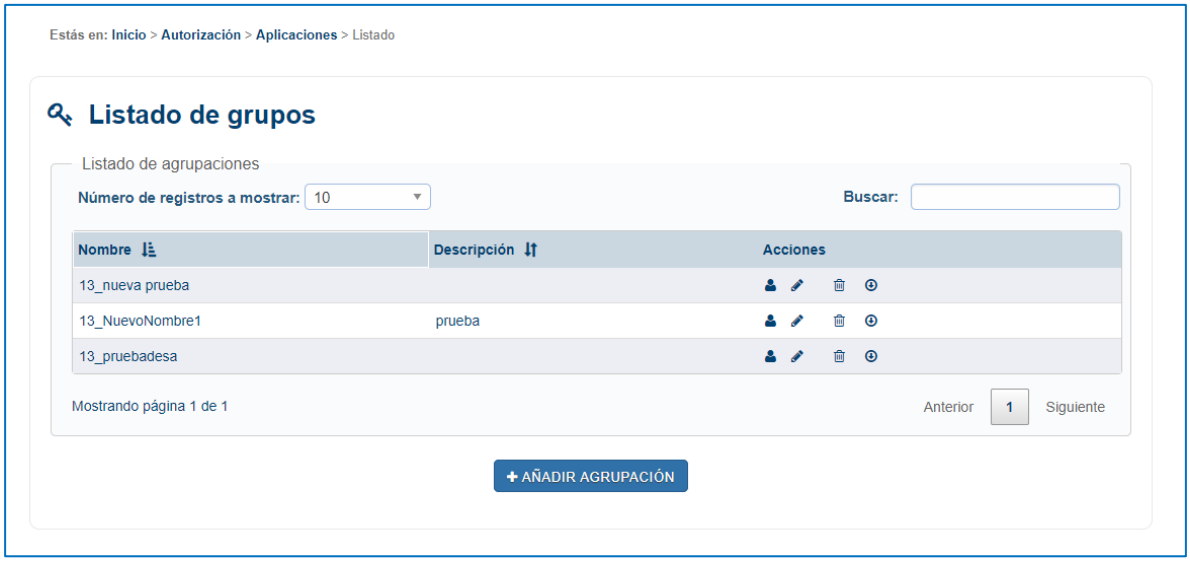
La pantalla muestra todas las aplicaciones que incluyen la opción de grupos de LDAP.



2.5.8.1. Listado de grupos por aplicación

Desde la pantalla de gestión de grupos, si se pincha en el nombre de cualquier aplicación accederemos al listado de grupos de esa aplicación.





En esta pantalla podemos ver que la aplicación 13 tiene tres grupos. Se visualiza el nombre y la descripción del grupo.

Junto a la descripción hay cuatro iconos de acciones, el primero permite ver los usuarios que están asociados a ese grupo, el lápiz permite modificar el grupo, la papelera permite eliminar el grupo, y el icono de la descarga permite descargarse un Excel con los usuarios del grupo.

Al final del listado se puede observar un botón que permite añadir nuevos grupos.

2.5.8.2. Creación de grupos

Dentro del listado de grupos, si hacemos click en el botón de añadir agrupación se nos abrirá la siguiente pantalla modal.

En la cual podemos rellenar el nombre y la descripción de un nuevo grupo. Si le damos a guardar se creará en LDAP el nuevo grupo asociado a la aplicación, **el nombre del grupo será el que indiquemos e internamente se le añadirá el código de la aplicación. Ejemplo:**

Nombre	Descripción
13_nueva prueba	
13_NuevoNombre1	prueba
13_Prueba documentación	Grupo de prueba que estoy usando para documentar
13_pruebadesa	

Mostrando página 1 de 1

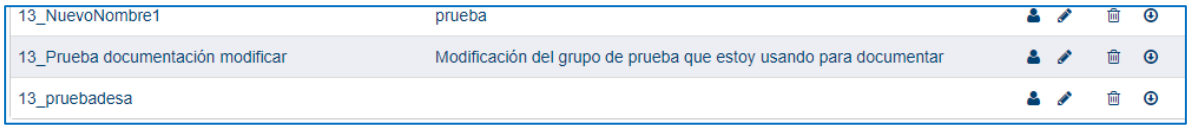
Como podemos ver, no se ha indicado el código de la aplicación e internamente se ha añadido.

Hay que tener en cuenta que, por requisitos técnicos de LDAP, el administrador que crea el grupo se asocia automáticamente a él. Una vez añadido algún otro usuario, se podrá desasignar al administrador que creó el grupo.

2.5.8.3. Modificación de grupos

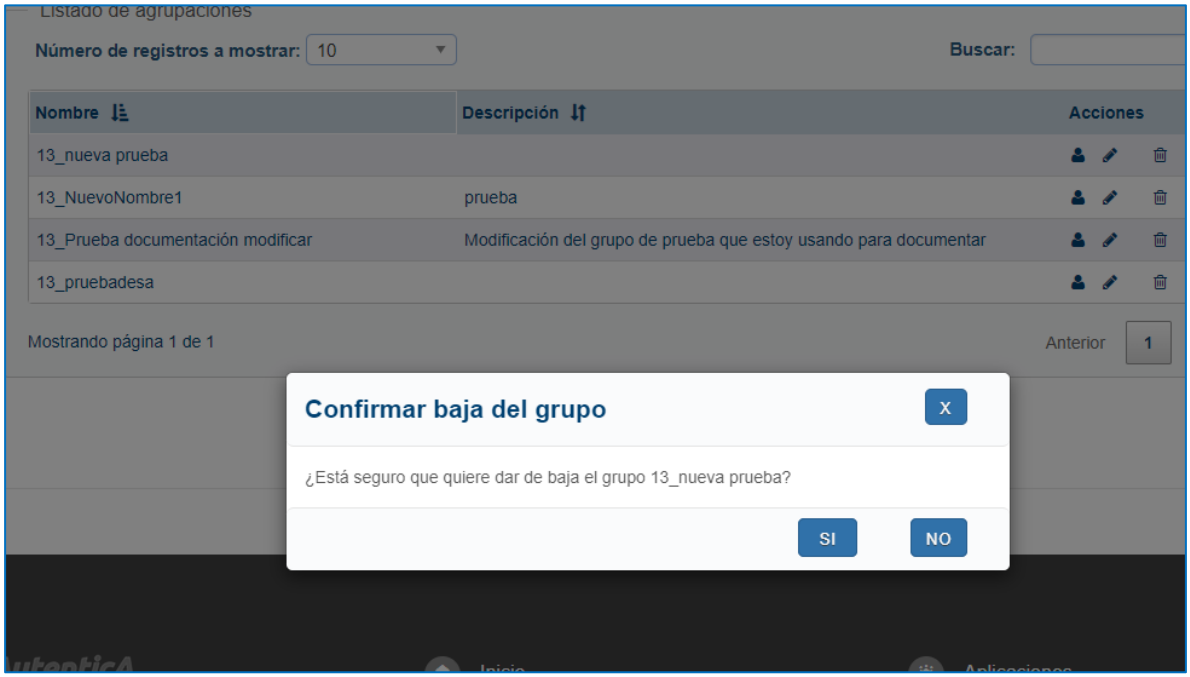
Desde el icono del lápiz se nos abre una pantalla modal en la que se permite cambiar los datos del grupo.

Si aceptamos vemos como se ha modificado.



2.5.8.4. Eliminación de grupos

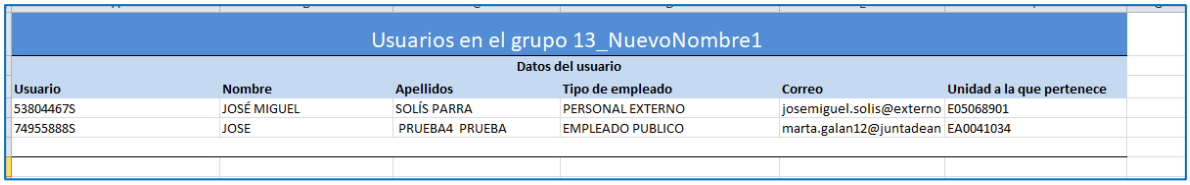
Desde el icono de la papelera se puede borrar el grupo seleccionado. Se nos presenta un mensaje de confirmación y se aceptamos se elimina.



2.5.8.5. Descarga de usuarios del grupo

En el icono de la descarga, lo que hace es descargar un listado de todos los usuarios asociados al grupo. Si el grupo tiene más de 10 usuarios se descargará en segundo plano y se guardará en el icono de descargas del módulo de aprovisionamiento.

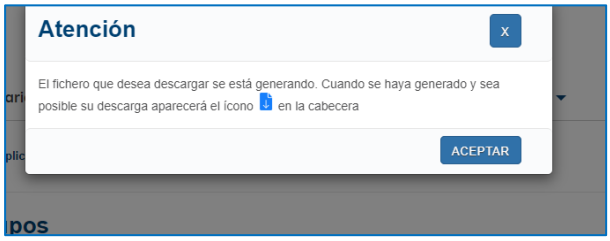
Por ejemplo, el primer grupo tiene dos usuarios, si le damos a descargar se nos descarga el siguiente documento.



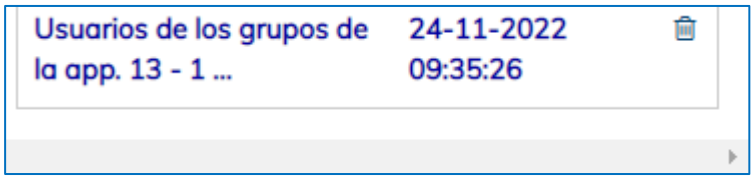
Usuarios en el grupo 13_NuevoNombre1

Datos del usuario					
Usuario	Nombre	Apellidos	Tipo de empleado	Correo	Unidad a la que pertenece
53804467S	JOSÉ MIGUEL	SOLÍS PARRA	PERSONAL EXTERNO	josemiguel.solis@externo	E05068901
74955888S	JOSE	PRUEBA4 PRUEBA	EMPLEADO PUBLICO	marta.galan12@juntadean	EA0041034

Pero el segundo grupo tiene 11 usuarios, nos avisan mediante el siguiente mensaje:



Si esperamos a que se descargue, podemos acceder a él desde donde se nos indica.



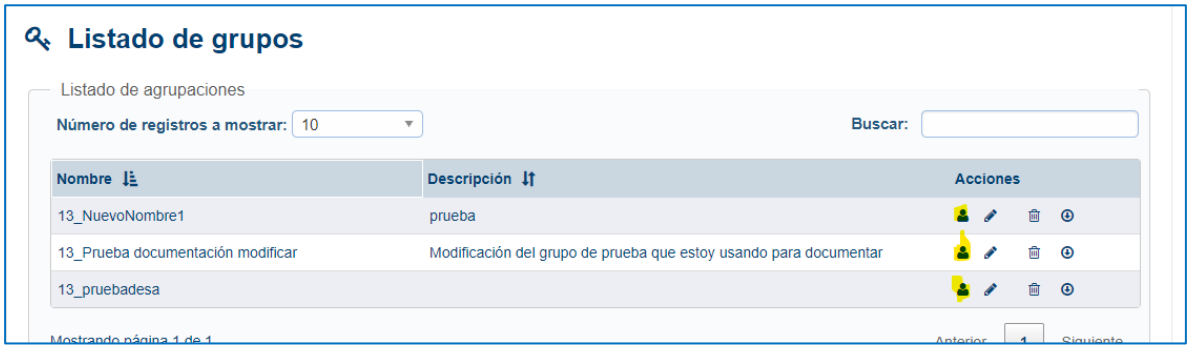
Observamos que el fichero se genera correctamente con los 11 usuarios:

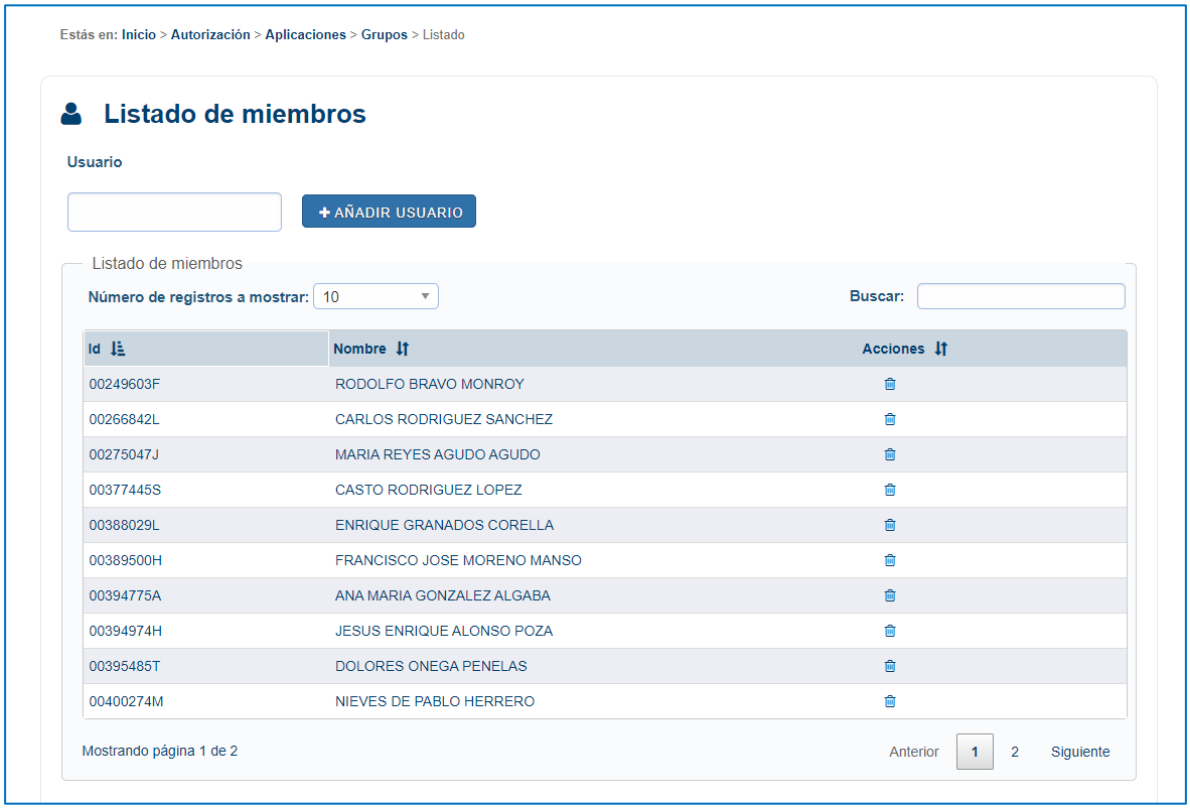
Usuarios en el grupo 13_Prueba documentación modificar

Datos del usuario					
Usuario	Nombre	Apellidos	Tipo de empleado	Correo	Unidad a la que pertenece
00394775A	ANA MARIA	GONZALEZ ALGABA	EMPLEADO PUBLICO		37105
00249603F	RODOLFO	BRAVO MONROY	EMPLEADO PUBLICO		U00172201
00389500H	FRANCISCO JOSE	MORENO MANSO	EMPLEADO PUBLICO		48493
00394974H	JESUS ENRIQUE	ALONSO POZA	EMPLEADO PUBLICO		36413
00275047J	MARIA REYES	AGUDO AGUDO	EMPLEADO PUBLICO		E04821604
00266842L	CARLOS	RODRIGUEZ SANCHEZ	EMPLEADO PUBLICO		U00172201
00388029L	ENRIQUE	GRANADOS CORELLA	EMPLEADO PUBLICO		45735
00400274M	NIEVES DE	PABLO HERRERO	EMPLEADO PUBLICO		49277
00377445S	CASTO	RODRIGUEZ LOPEZ	EMPLEADO PUBLICO		43354
53804467S	JOSÉ MIGUEL	SOLÍS PARRA	PERSONAL EXTERNO	josemiguel.solis@externo	E05068901
00395485T	DOLORES	ONEGA PENELAS	EMPLEADO PUBLICO		35800

2.5.8.6. Listado de usuarios

Desde el icono de usuario, se nos muestran todos los usuarios asociados al grupo.





Desde esta pantalla podemos ver el id del usuario (normalmente su documento de identificación), su nombre y apellidos, y un icono de papelera desde el cual podemos eliminarlo del grupo.

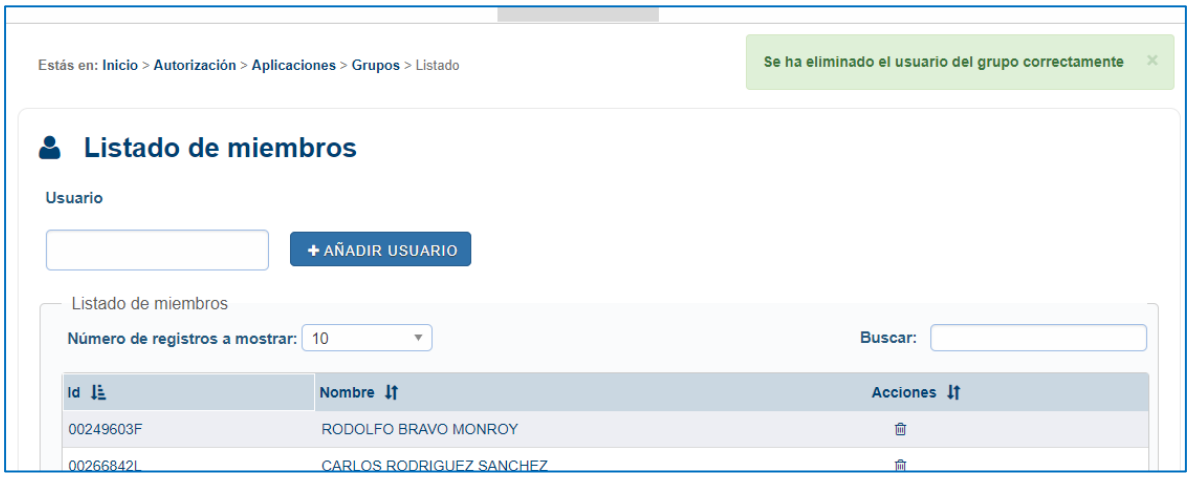
También podemos ver en la parte superior un campo de texto en el que podemos poner el id de un usuario y mediante el botón de añadir se asocia el usuario al grupo.

2.5.8.7. Añadir y eliminar a usuario del grupo

Mediante el campo de texto de la parte superior podemos rellenar el id del usuario que queramos añadir de la siguiente manera.

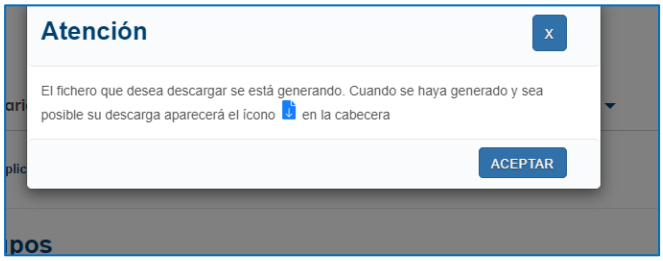
Si le damos a añadir usuario, se comprueba que exista, y si existe se añade.

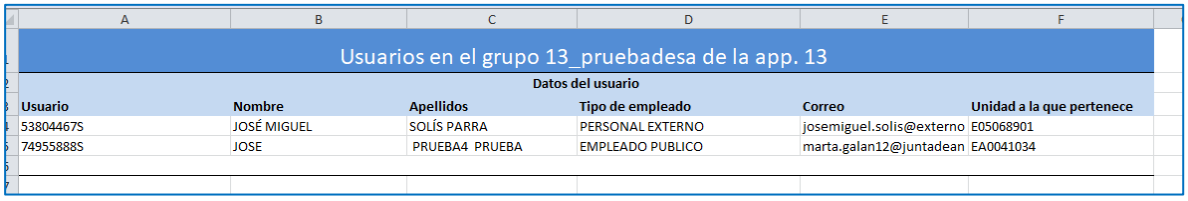
De igual manera, si queremos eliminarlo del grupo le podemos dar al icono de la papelera y se nos mostrará el siguiente mensaje de confirmación.



2.5.8.8. Descarga de grupos y usuarios asociados a la aplicación

Desde la pantalla de gestión de grupos, si pinchamos en el icono de descarga, se nos descargará un listado igual que el del apartado 4.4.5 pero con todos los grupos de la aplicación y sus usuarios.





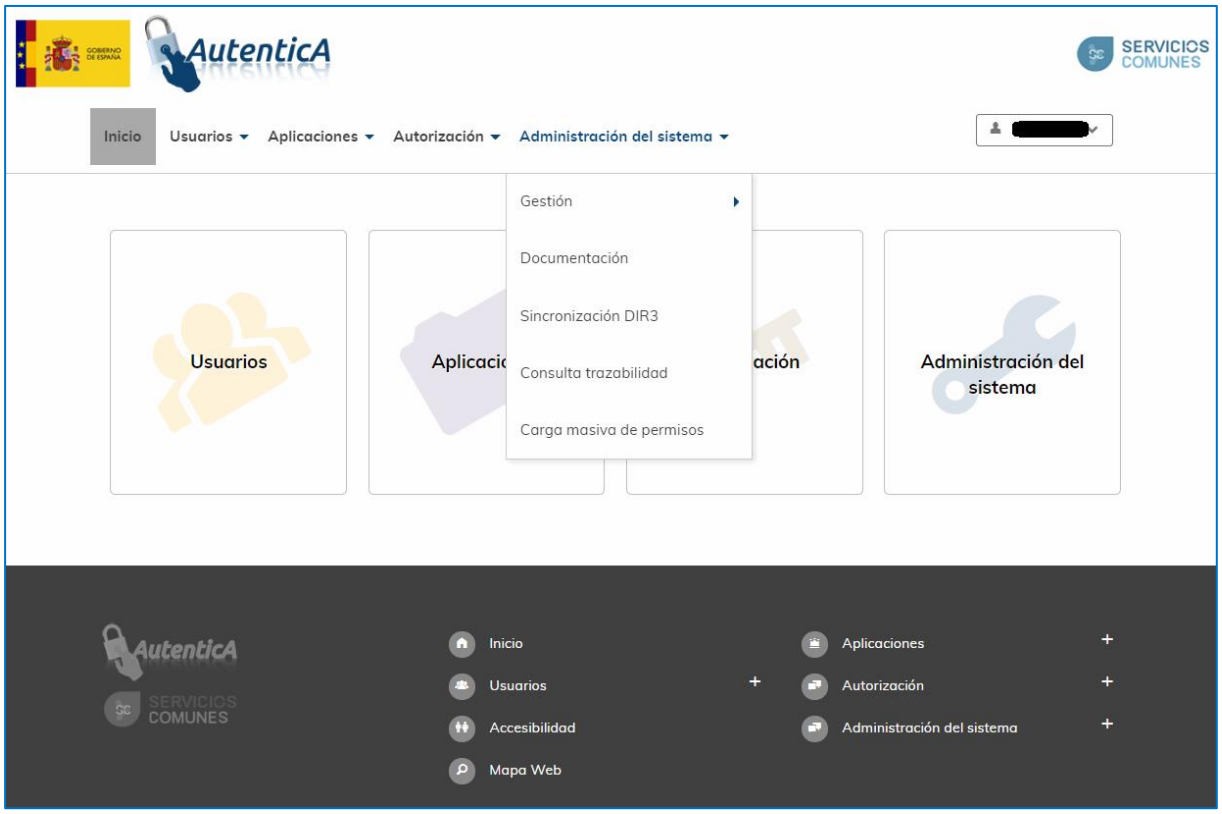
Usuarios en el grupo 13_pruebadesa de la app. 13

			Datos del usuario		
Usuario	Nombre	Apellidos	Tipo de empleado	Correo	Unidad a la que pertenece
53804467S	JOSÉ MIGUEL	SOLÍS PARRA	PERSONAL EXTERNO	josemiguel.solis@externo	E05068901
74955888S	JOSE	PRUEBA4 PRUEBA	EMPLEADO PUBLICO	marta.galan12@juntadean	EA0041034

Podemos ver que cada hoja es un grupo.

2.6. ADMINISTRACIÓN DEL SISTEMA

En el menú superior, desde la pestaña de “Administración” estarán disponibles las opciones para la administración del sistema. Sólo tendrán acceso a esta pestaña los administradores centrales y a la opción de Gestión de permisos, también los administradores delegados.



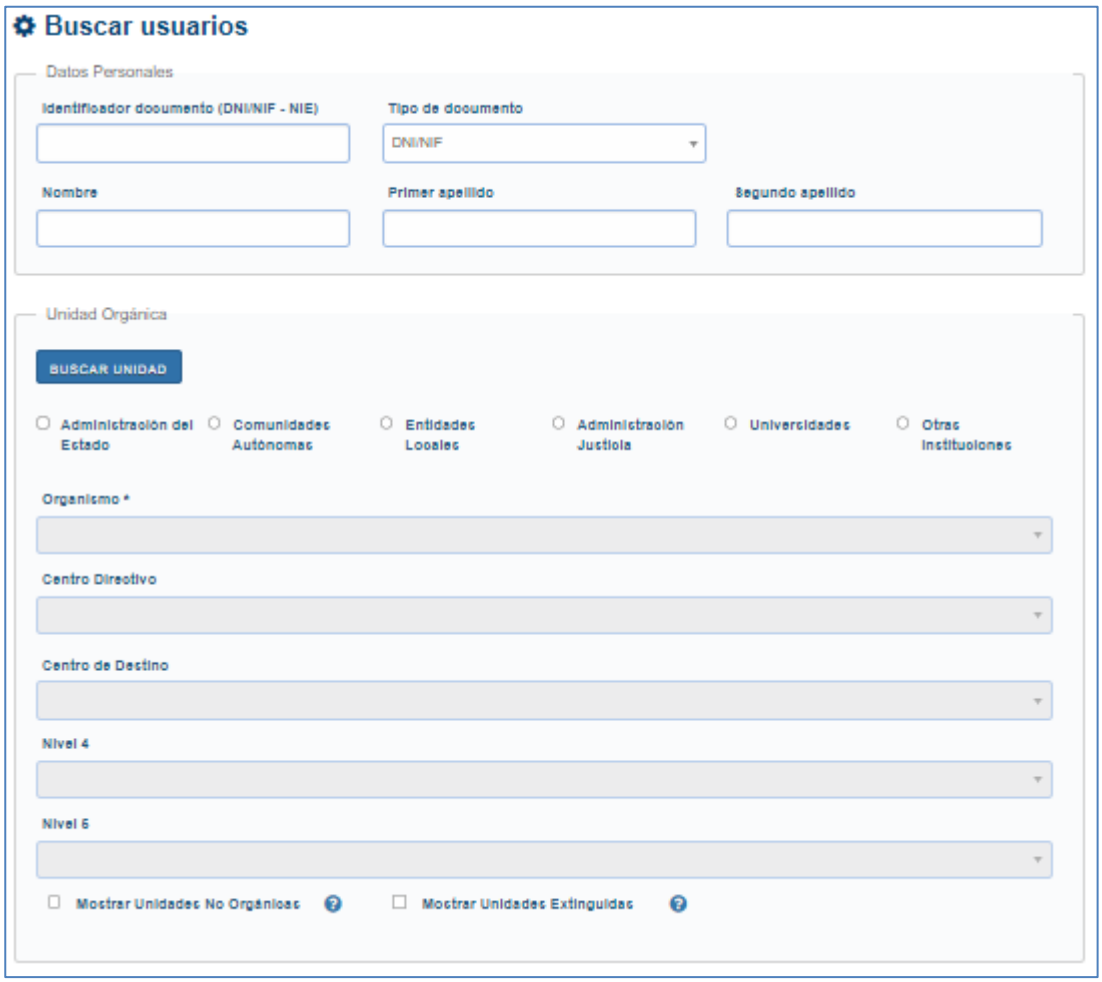
2.6.1. GESTIÓN

2.6.1.1. GESTIÓN DE PERMISOS

2.5.1.1.1 Gestión de permisos por usuario

Desde esta opción se podrán cambiar los perfiles asignados a los diferentes usuarios del repositorio horizontal de autenticación. Para acceder a ella se deben tener permisos de Administrador Central.

En primer lugar, aparecerá un formulario de búsqueda de usuarios con diferentes criterios:



En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

Marcando la opción “Mostrar Unidades No Orgánicas” se mostrarán también en los desplegables de “Unidad Orgánica” las unidades no orgánicas.

Marcando la opción “Permitir unidades extinguidas” se mostrarán también en los desplegables de “Unidad Orgánica” aquellas unidades que ya no tienen estado “Vigente” sino “Extinguido”.

Al buscar, se muestra un listado con los usuarios encontrados:

Al pulsar sobre el enlace “Administrar permisos” de algún usuario se mostrará la pantalla con los datos básicos del empleado y los permisos disponibles en Autentica, teniendo marcados aquellos que ya disponga con la posibilidad de modificarlos o eliminarlos.

Marcando el tipo de permiso “Administrador central”, se le darán permisos al usuario para que tenga acceso a toda la aplicación y por defecto se le asignará el nivel de perfil superior que exista.

En el campo “Gestión de permisos de usuarios” se encuentran los permisos correspondientes al módulo de usuarios, los cuáles son los siguientes:

- Usuario básico: es el nivel mínimo de permiso sobre este módulo, permite acceso a las opciones “Gestión de grupos de usuarios” y “Gestión de atributos de VPN”.
- Usuario avanzado: permite el acceso a la opción “Gestión de usuarios”.

- Bandeja de entrada: permite el acceso a la opción de bandeja de entrada de solicitudes de usuarios, compuesto por la bandeja de solicitudes de alta y de modificación.
- Carga masiva: permite el acceso a la opción de carga masiva de usuarios.

En el campo “Gestión de permisos de autorización” se encuentran los permisos correspondientes al módulo de autorización, los cuáles son los siguientes:

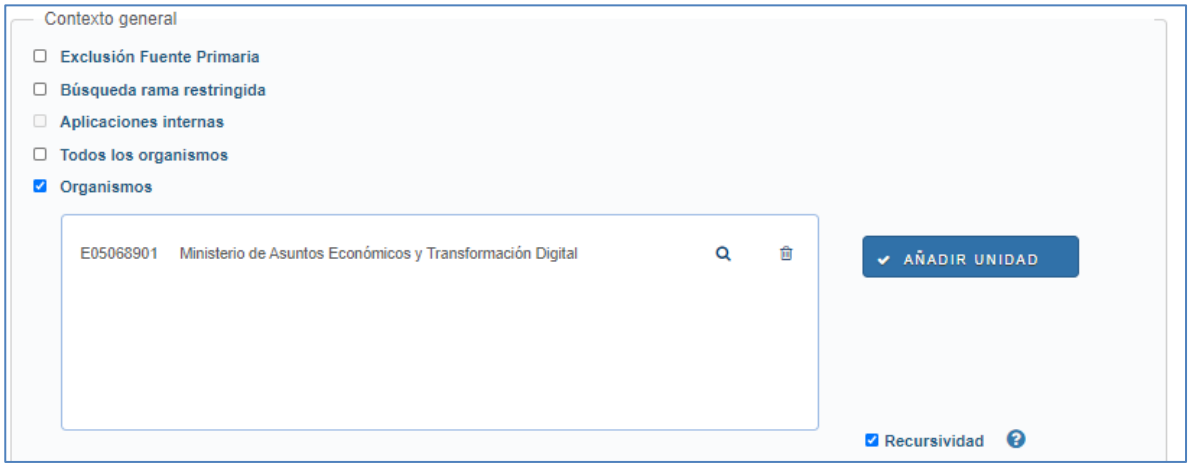
- Autorización básica: es el nivel mínimo de permiso sobre este módulo, permite acceso a las opciones “Sincronización DIR3” y “Búsqueda usuarios perfil”.
- Usuarios: permite el acceso a la opción “Autorización de usuarios”.
- Perfiles y roles: permite el acceso a las opciones “Gestión de perfiles” y “Gestión de roles”.
- Aplicaciones: permite el acceso a la opción “Gestión de aplicaciones”
- Carga masiva: permite el acceso a la opción de cargas masivas.
- Bandeja de entrada: permite el acceso a la opción de bandeja de entrada de solicitudes de autorización, compuesto por la bandeja de solicitudes de alta y de modificación.

En el campo “Gestión de permisos de administradores” se encuentra la opción “Gestión de permisos para las altas de administradores delegados”, con la cual se creará un administrador delegado que pueda administrar los permisos de otros usuarios, asignándoles siempre sus mismos permisos o inferiores. Existirán tres niveles de Administrador delegado con gestión de permisos.

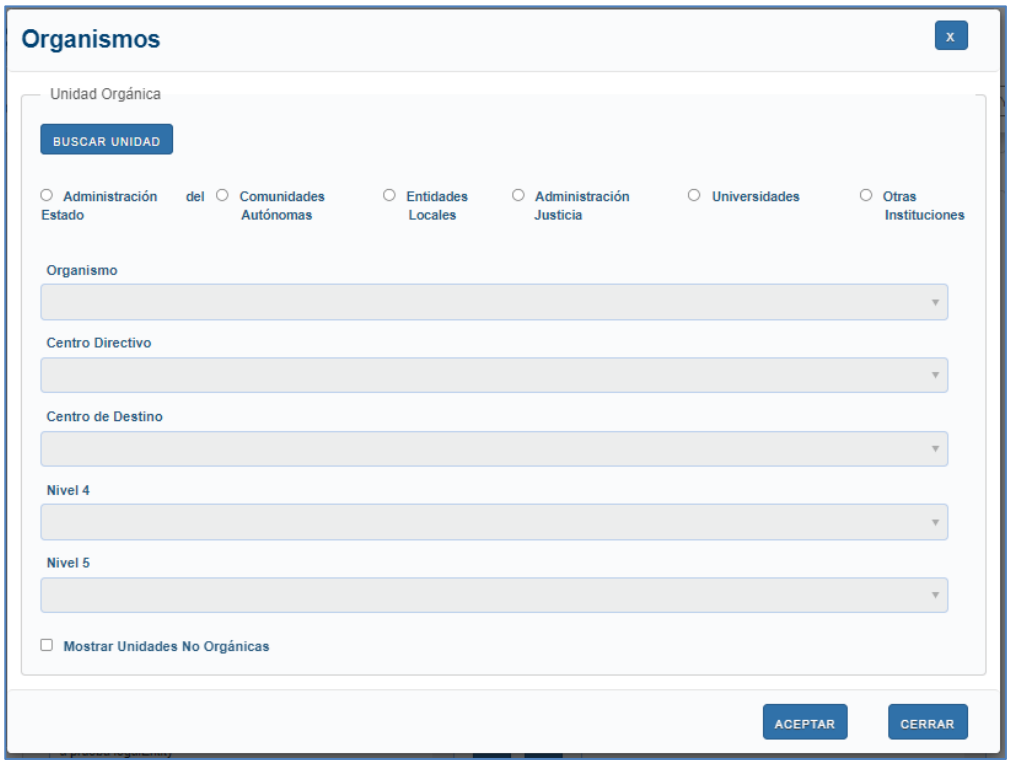
En el apartado Contexto general, se muestra la opción “Búsqueda rama restringida”, con la cual se le permite a un administrador delegado la búsqueda de usuarios en la rama restringida.

Si se marca la opción “Organismos” se muestra un botón para la selección de las unidades del usuario.

Si se marca la opción “Mostrar unidades no orgánicas” se muestran todas las unidades no orgánicas que tenga la ventana organismos, se encuentran en otras instituciones > entidades colaborativas



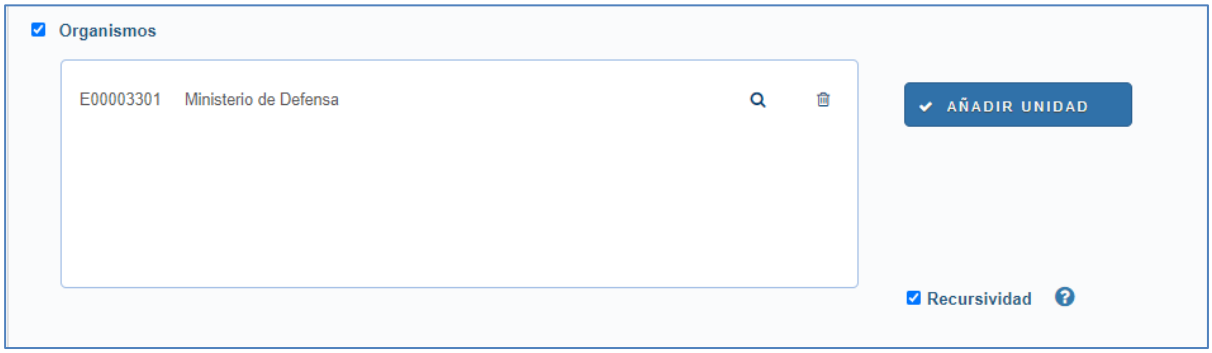
Una vez que se oprime el botón “Añadir unidades” se muestra una pantalla con el listado de unidades a seleccionar. Se podrá seleccionar unidades con nivel de profundidad superior a nivel 5; los desplegables con las unidades superiores se muestran al seleccionar una unidad de nivel inferior que tenga unidades hijas.



En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.

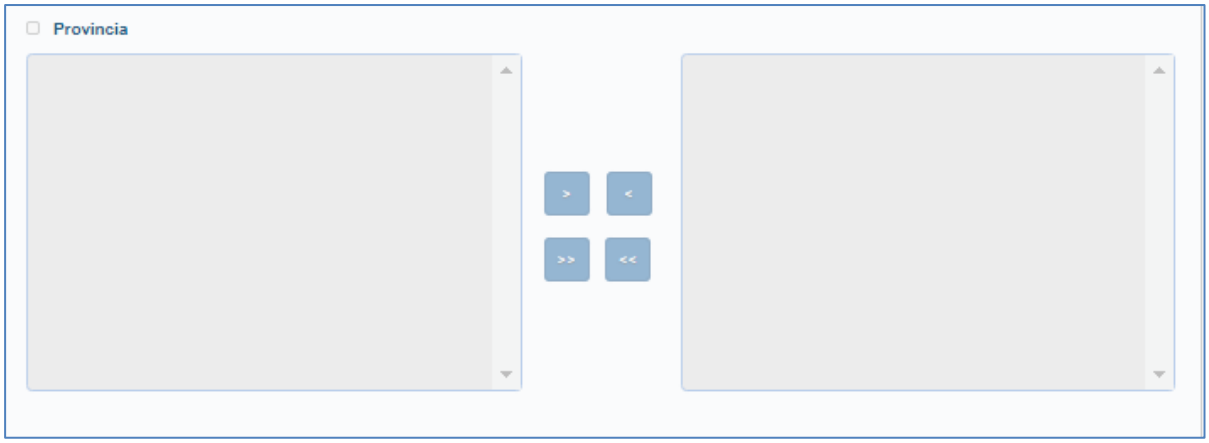
Al pulsar “Aceptar” se muestra el listado de unidades seleccionada con el código y la descripción de la misma.

Si se marca la opción “Recursividad” se aplicarán permisos recursivos en base a las unidades del usuario.



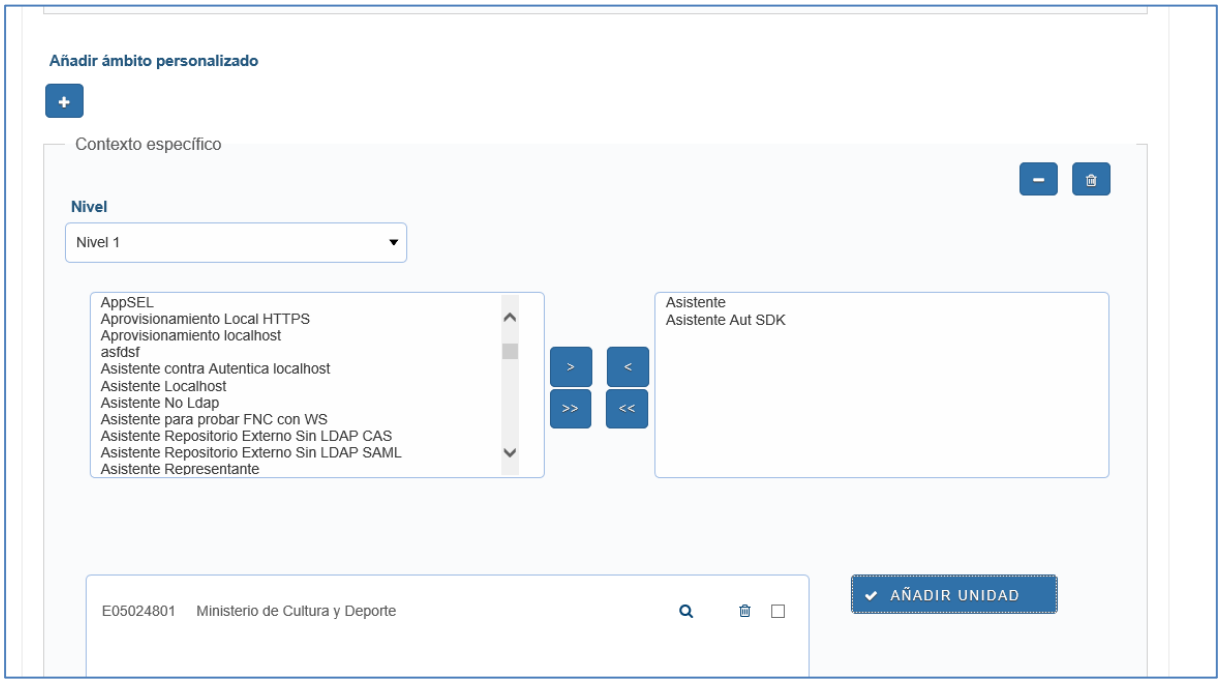
Así mismo, se podrán marcar los contextos de aplicación y provincia, seleccionando tanto las aplicaciones y provincias correspondientes a los permisos que se quieren asignar al usuario. En el apartado de aplicación se podrá seleccionar el nivel permitido para el administrador, siendo el nivel 1 el más bajo y 2 el nivel el más alto.

Se mostrará un buscador de aplicaciones que se filtrarán en la caja del listado.



También puede añadirse una unidad y su recursividad a varias aplicaciones que se encuentre dentro del apartado de contexto de aplicación en el apartado “Añadir ámbito personalizado”. Así mismo, se podrá seleccionar el nivel específico para las aplicaciones seleccionadas, que tendrá prioridad sobre el nivel estándar señalado en el apartado de aplicaciones.

Esta opción se encontrará habilitada sólo en el supuesto de que no se tenga marcada la opción “Todos los organismos”.



En la parte inferior se muestran las opciones “Eliminar permisos” y “Modificar permisos”. En el caso de pulsar “Eliminar permisos” se le quitarán todos ellos. Si se pulsa “Modificar permisos”, se modificarán. Se mostrará una pantalla con el resultado de la operación.

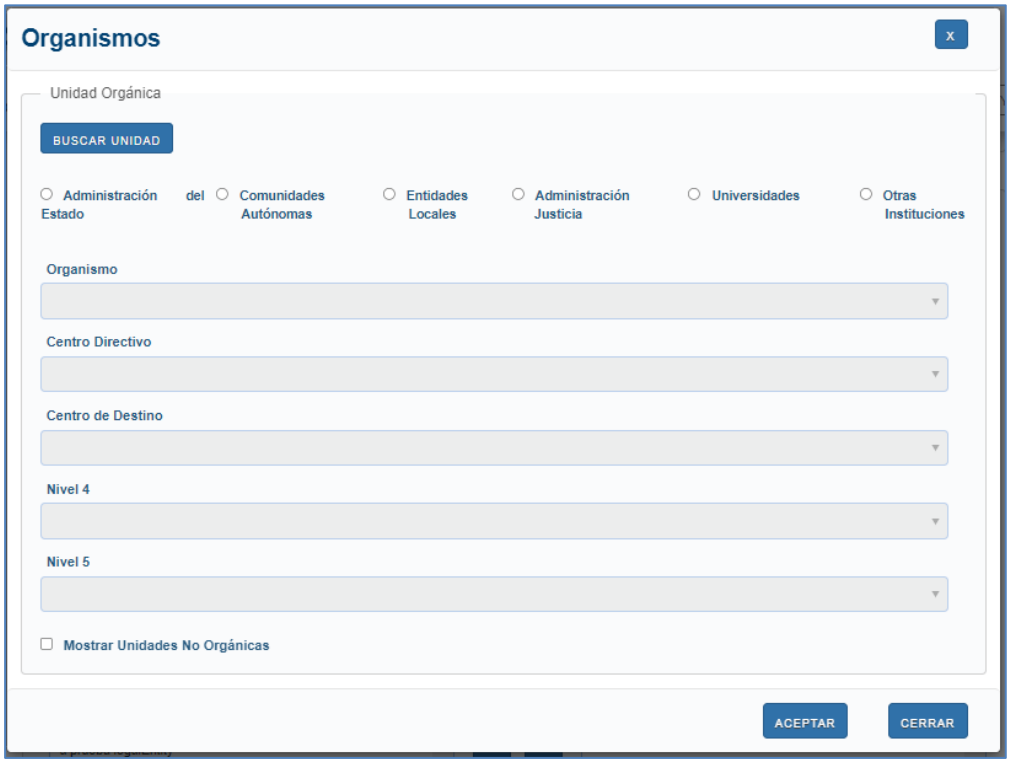
Permisos	Operación	Resultado
CENTRAL	Sin cambios	
AUTORIZACIÓN	Sin cambios	
USUARIOS	Sin cambios	
GESTIÓN PERMISOS	Sin cambios	
APLICACIÓN	Sin cambios	
TODAS LAS UNIDADES	Sin cambios	
UNIDAD	Sin cambios	
PROVINCIA	Sin cambios	
EXCLUSIÓN FUENTES PRIMARIAS	Sin cambios	

2.5.1.1.2 Búsqueda de administradores

Desde esta opción se pueden buscar usuarios con los permisos y contexto seleccionados.

Primero se muestra el formulario de búsqueda y una vez seleccionados los criterios, se pulsa aceptar.

En el apartado “Tipo de permiso organismos”, se podrá seleccionar una unidad para la búsqueda. Se mostrará un cuadro para la selección de la misma, en los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Se muestra un apartado de permiso contexto general, en el cual se puede seleccionar la búsqueda de administradores por el permiso de búsqueda en rama restringida.

Pulsando en los tipos de permisos “Autorización” o “Gestión de usuarios” se mostrarán los permisos asociados a estos contextos.

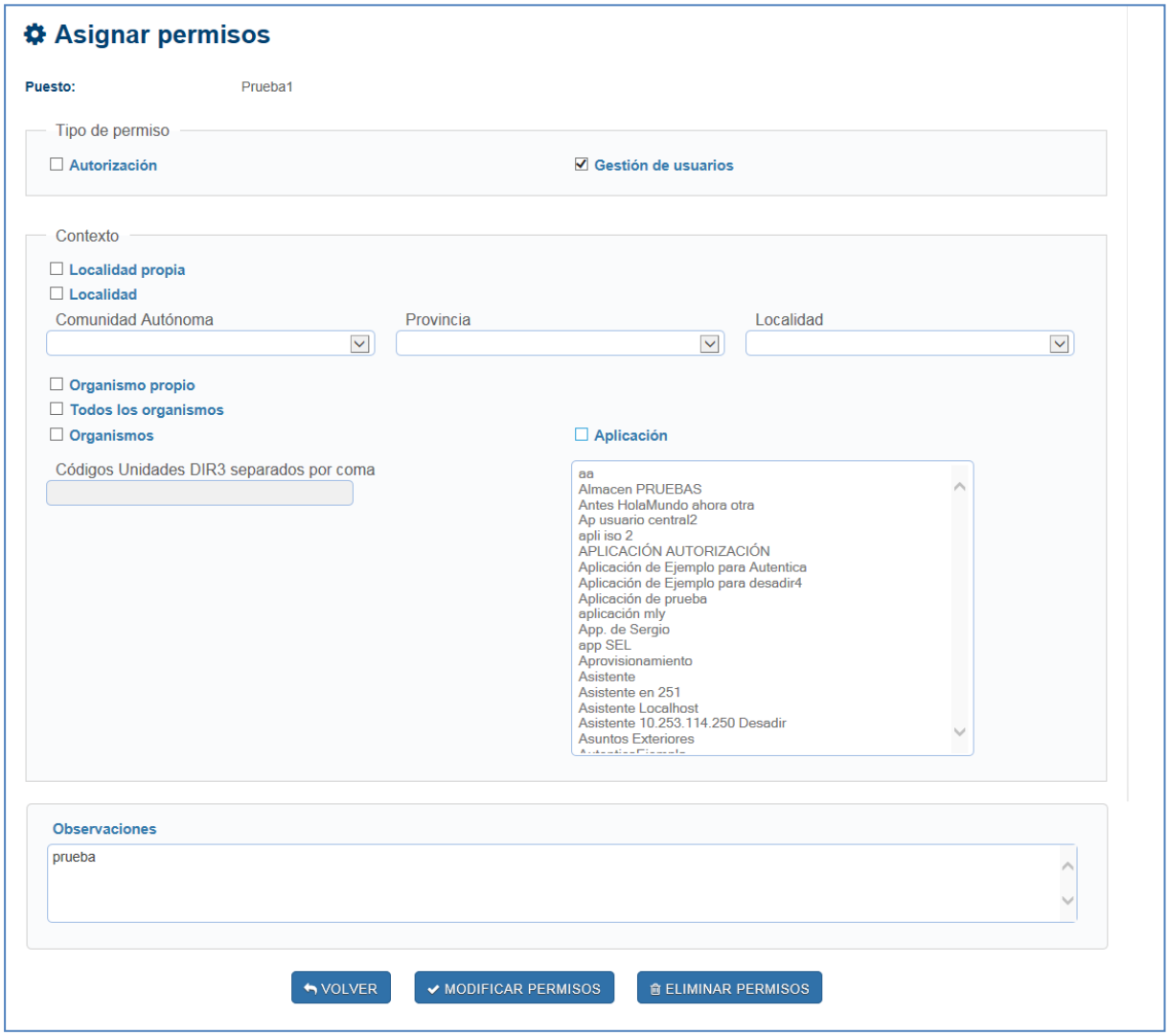
Se mostrará un listado con los usuarios que cumplan las condiciones, información de cada uno y un acceso para ver en detalle los permisos que tienen.

2.5.1.1.3 *Gestión de permisos por puesto*

Esta funcionalidad permitirá a los administradores dar permisos por puesto o cargo. Estos permisos se añadirán a los que ya tenía el usuario cuando este inicie la sesión.

Cuando el administrador acceda a la gestión de permisos por puesto, se le mostrará una pantalla de administración donde podrá añadir, modificar o eliminar puestos de la lista.

Al seleccionar uno de ellos, irá a la pantalla de asignación de permisos.



Desde aquí se podrá

- **Eliminar Permisos**.

  Limpiará los permisos del puesto seleccionado.

- **Modificar Permisos.**

El usuario deberá seleccionar un tipo de permiso y al menos un contexto relacionado a este. Con el tipo de permiso ‘Autorización’, el usuario adquirirá permisos para acceder a la pestaña de Autorización. Con el tipo de permiso ‘Gestión de usuarios’, tendrá permisos para acceder a la pestaña de Usuarios.

El contexto de Localidad y Organismos será excluyente, no pudiéndose seleccionar ambos a la vez. Si se selecciona el check ‘Localidad propia’ u ‘Organismo propio’, se le asignará a cada usuario de ese puesto sus propios organismos o las localidades de estos. Si se selecciona el check ‘Localidad’, obligará a elegir en los tres desplegables de Comunidad Autónoma, Provincia y Localidad. Al seleccionar ‘Todos los organismos’, los usuarios del puesto tendrán permisos sobre todos los organismos existentes. Seleccionando el check ‘Organismos’, podremos insertar en la caja uno o varios códigos DIR3 separados por comas (ej.: E00003601,E04585801,E04921301).

Al seleccionar el check ‘Aplicación’, podremos elegir una o varias aplicaciones de la lista.

Una vez escogidos los permisos, se pulsará el botón ‘Modificar Permisos’ para que se guarden las opciones seleccionadas. Aparecerá una pantalla informativa sobre los permisos asociados al puesto.

Permisos	Operación	Resultado
AUTORIZACIÓN	Sin cambios	
USUARIOS	Sin cambios	
APLICACIÓN	Sin cambios	
UNIDAD	Sin cambios	
LOCALIDAD	Sin cambios	
TODAS LAS UNIDADES	Sin cambios	
LOCALIDAD PROPIA	Permiso añadido	
UNIDAD PROPIA	Sin cambios	

2.5.1.1.4 Gestión de puestos

Esta funcionalidad permitirá a los administradores gestionar los puestos o cargos.

Cuando el administrador acceda a la gestión de puestos, se le mostrará una pantalla de administración donde podrá dar de alta, modificar o eliminar puestos de la aplicación.

2.6.1.2. GESTIÓN DE DOMINIOS DE CORREO

Esta funcionalidad se divide en la gestión de dominios de correos corporativos y en la gestión de dominios de correos no corporativos; los cuales permitirán la gestión de los dominios.

Cuando el administrador acceda a la gestión de dominios de correo, se le mostrará un menú con las opciones de gestión de dominios de correos corporativos y no corporativos. Una vez que se accede tanto a la gestión de dominios de correos corporativos como a la gestión de dominios no corporativos se muestra un formulario para insertar un nuevo dominio y un listado de dominios de correo en el cual se puede consultar, modificar y eliminar el dominio seleccionado. Si elimina o modifica un dominio que algún usuario tenga dado de alta, ese dominio no se modificará ni eliminará en los datos del usuario.

En la zona de Alta dominio

- En la casilla de alta, se ingresarán los dominios, al pulsar el botón de alta, se incluirá en el listado y se mostrará un mensaje de información.

En la zona de dominios

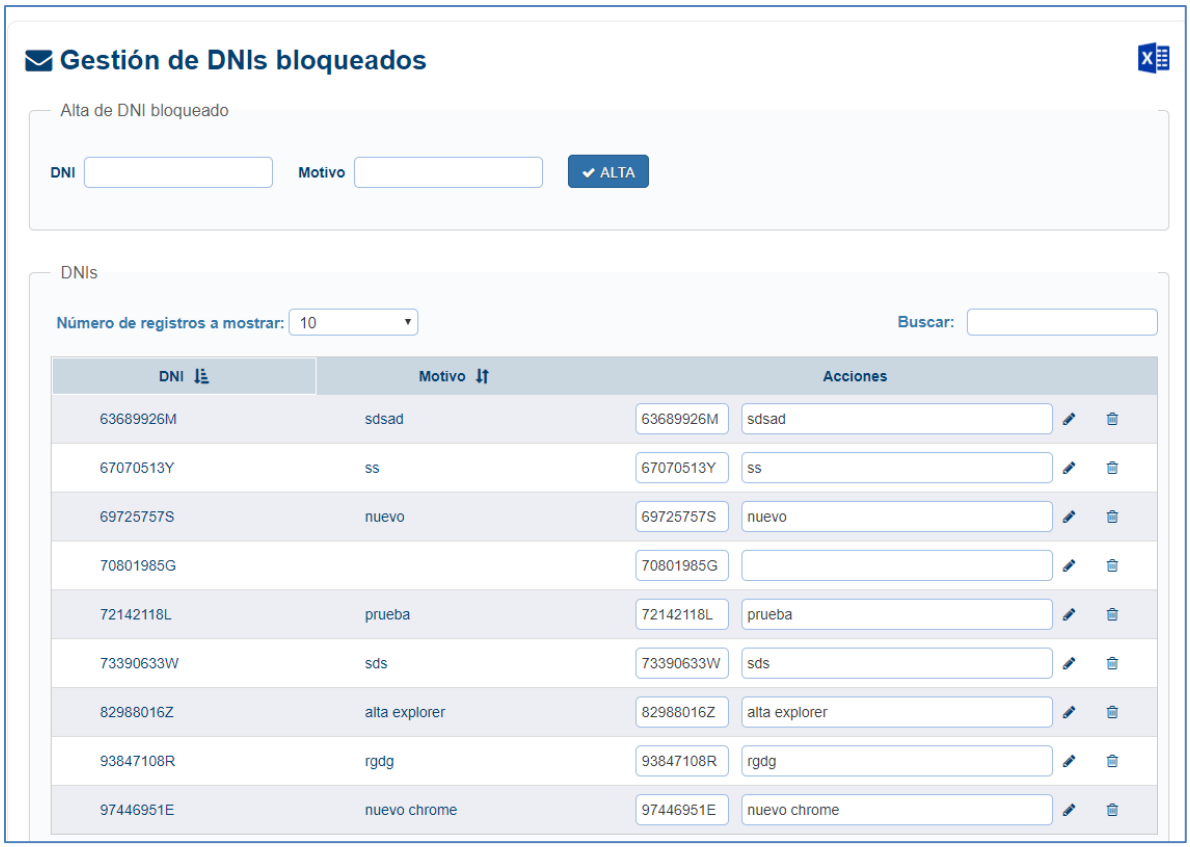
- Columna de la izquierda: Se muestra el dominio de correo ordenado ascendentemente.

- Columna derecha: en la casilla se podrá hacer la modificación deseada y al pulsar sobre el icono del lápiz, se modificará el dominio en el listado y se mostrará un mensaje de información en la zona de alta dominio. Hay que tener en cuenta que modificar el dominio no implica modificarlo de los datos de los usuarios. Al pulsar sobre el icono de la papelera, se eliminará el dominio del listado y se mostrará un mensaje de información en la zona de alta dominio. Hay que tener en cuenta que eliminar el dominio no implica eliminarlo de los datos de los usuarios.

2.6.1.3. GESTIÓN DE DNIs BLOQUEADOS

Esta funcionalidad permitirá gestionar los DNIs bloqueados.

Cuando el administrador acceda a la gestión de DNIs bloqueados, se le mostrará la pantalla para la gestión de DNIs con un formulario que permite bloquear un nuevo DNI y un listado con los DNIs bloqueados, el cual permitirá consultar, modificar y eliminar el DNI seleccionado.



En la zona del Alta de DNI bloqueado

- En la casilla DNI, se ingresará el DNI a bloquear.
- En la casilla Motivo, se ingresará el motivo por el cual se va a bloquear el DNI.

Al oprimir el botón “Alta” se bloquea el DNI insertándose en el listado que se muestra en la zona DNIs y se muestra un mensaje de información.

En la zona de DNIs

- Columnas a la izquierda con los datos del DNI y el motivo del bloqueo; por defecto se encuentra ordenado por DNI de manera ascendente. Se podrá ordenar tanto por DNI como por motivo.
- Columna a la derecha: en la casilla se podrá hacer la modificación deseada del DNI y el motivo y al pulsar sobre el icono del lápiz, se modificarán los datos referentes al DNI bloqueado reflejándose en el listado y se muestra un mensaje de información en la zona de Alta de DNI bloqueado. Al pulsar sobre el icono de la papelera, se desbloquea el DNI siendo eliminado del listado y se muestra un mensaje de información en la zona de Alta de DNI bloqueado.

2.6.1.4. Gestión de lista blanca de certificados

Esta funcionalidad permitirá gestionar las autoridades de certificación permitidas en los accesos de las aplicaciones

El administrador podrá dar de alta nuevas autoridades, modificarlas o dar de baja las existentes.

2.6.1.5. GESTIÓN DE REPOSITORIOS

Esta funcionalidad permitirá gestionar los repositorios externos de usuarios.

El administrador podrá dar de alta nuevos repositorios, modificarlos o dar de baja los repositorios ya existentes.

2.5.1.4.1 Alta de repositorio

Se mostrará un formulario de alta donde se tendrán que rellenar los datos necesarios para crear el nuevo repositorio.

Estos repositorios se consultarán en caso de que el usuario que intenta autenticarse

- Introduzca una contraseña que no sea la registrada en Autentica.
- sea para acceder a una aplicación que tenga marcada la opción para acceder a otros repositorios externos
- pertenezca a una unidad DIR3 que haya sido configurada en la ficha del repositorio externo.

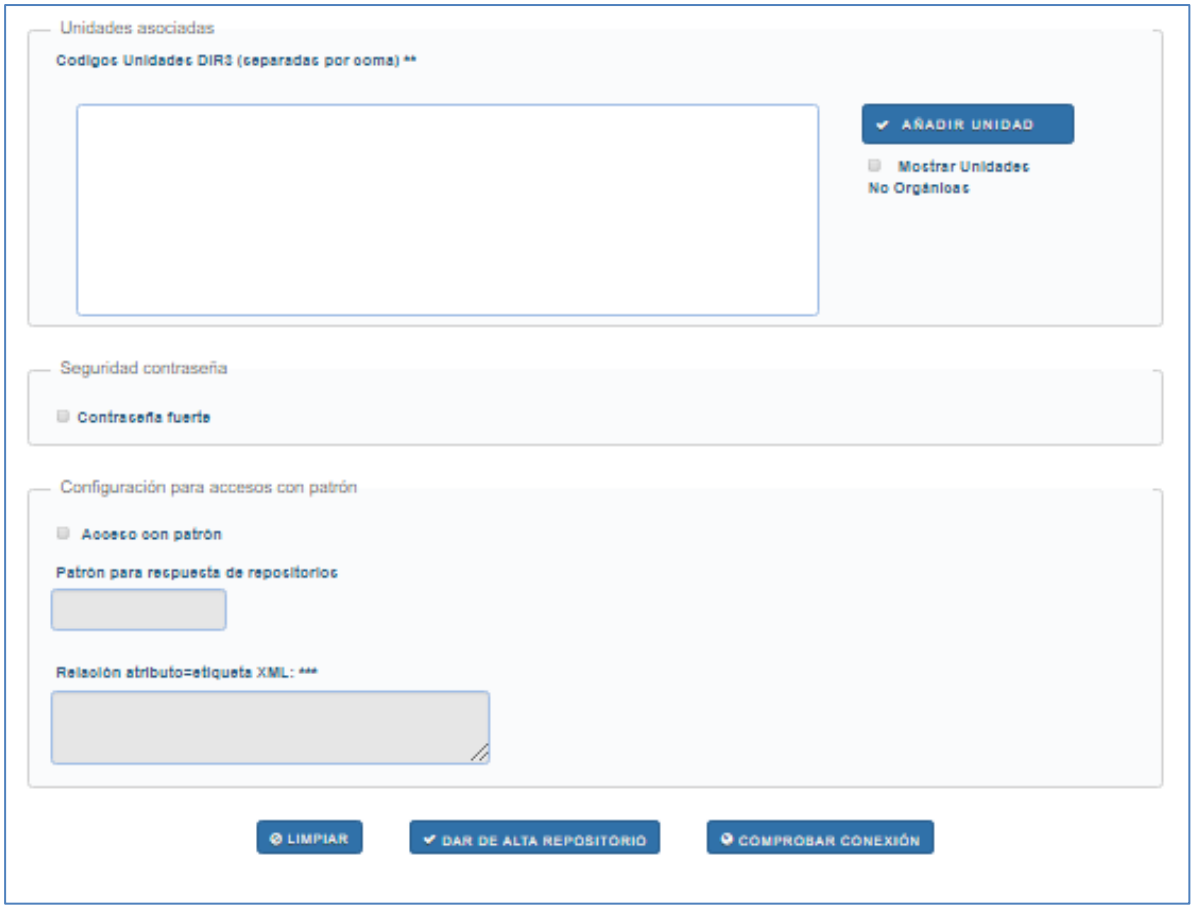
Existe la posibilidad de que se marque la fortaleza de la contraseña del repositorio como fuerte, no pudiendo ser el nivel de seguridad de la contraseña del repositorio más bajo que el de la aplicación a la que se quiere acceder, de tal forma que el acceso a una aplicación indicando una contraseña válida del repositorio externo se evalúa de la siguiente forma:

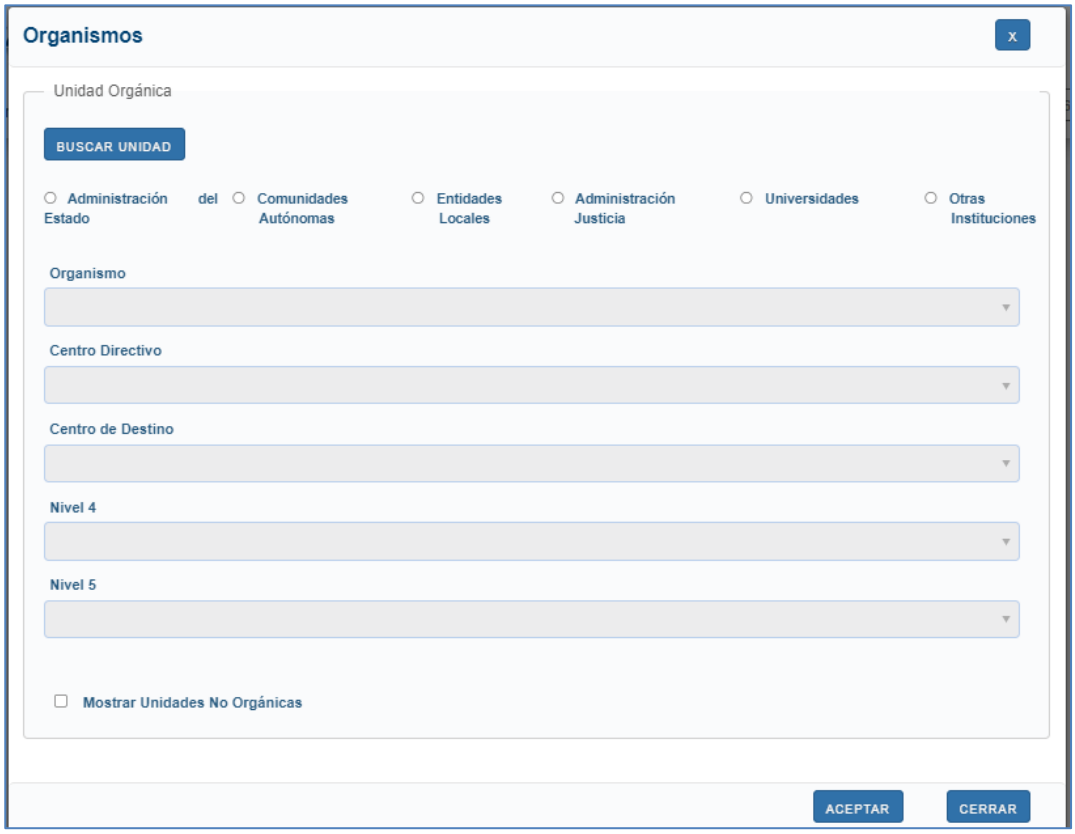
Fortaleza de la contraseña del usuario en Autentica	Fortaleza de la contraseña de la aplicación invocante.	Fortaleza de la contraseña en el repositorio externo.	Acceso con contraseña válida del repositorio
Débil	Débil	Débil	SI
Fuerte	Débil	Débil	SI
Débil	Débil	Fuerte	SI (porque Autentica se fía de la fortaleza de la contraseña en el repositorio externo)
Fuerte	Débil	Fuerte	SI (porque Autentica se fía de la fortaleza de la contraseña en el repositorio externo)
Débil	Fuerte	Débil	NO (El repositorio externo tiene un nivel de seguridad menor que el de la aplicación invocante)

Fuerte	Fuerte	Débil	NO (El repositorio externo tiene un nivel de seguridad menor que el de la aplicación invocante)
Débil	Fuerte	Fuerte	SI (porque Autentica se fía de la fortaleza de la contraseña en el repositorio externo)
Fuerte	Fuerte	Fuerte	SI (porque Autentica se fía de la fortaleza de la contraseña en el repositorio externo)

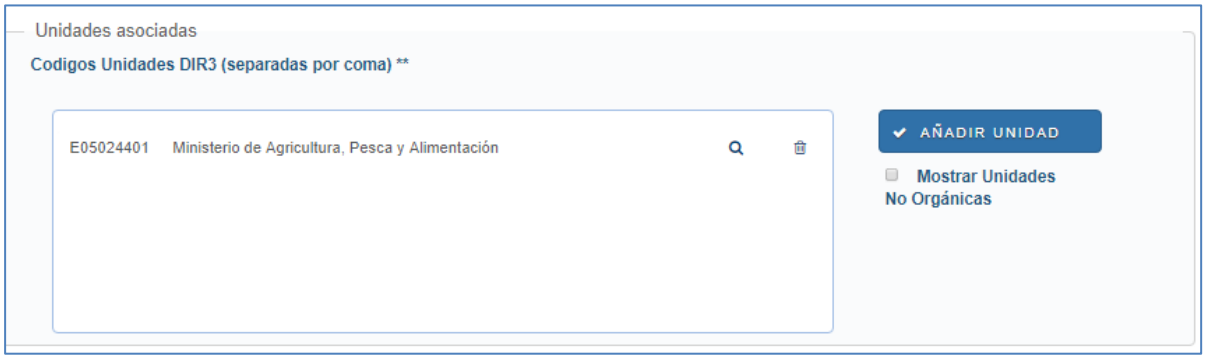
Para introducir el código de la unidad en el formulario se tiene el botón “Mostrar” para realizar la selección de la misma. Al oprimir este botón se muestra una pantalla con el listado de unidades. Una vez seleccionada la unidad se muestra el código de la misma en el área de texto.

Estás en: Inicio > Administración > Gestión > Gestión de repositorios > Alta de repositorio
Alta de repositorio
Los campos marcados con * son obligatorios.
El campo marcado con ** es obligatorio si no se introduce contenido en el campo "Patrón para acceso a repositorio".
El campo marcado con *** es obligatorio si se introduce contenido en el campo "Patrón para acceso a repositorio".
Datos de Repositorio
Nombre *
Dominio (ldap://[dominio]:[puerto])*
Base *
Branch
Atributo de búsqueda *
Tipo *
Active Directory
Usuario *
Contraseña *


Unidades asociadas
Codigos Unidades DIR3 (separadas por coma) **
AÑADIR UNIDAD
Mostrar Unidades No Orgánicas
Seguridad contraseña
Contraseña fuerte
Configuración para accesos con patrón
Acceso con patrón
Patrón para respuesta de repositorios
Relación atributo=etiqueta XML: ***
LIMPIAR
DAR DE ALTA REPOSITORIO
COMPROBAR CONEXIÓN



En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



2.5.1.4.2 Modificación de repositorio

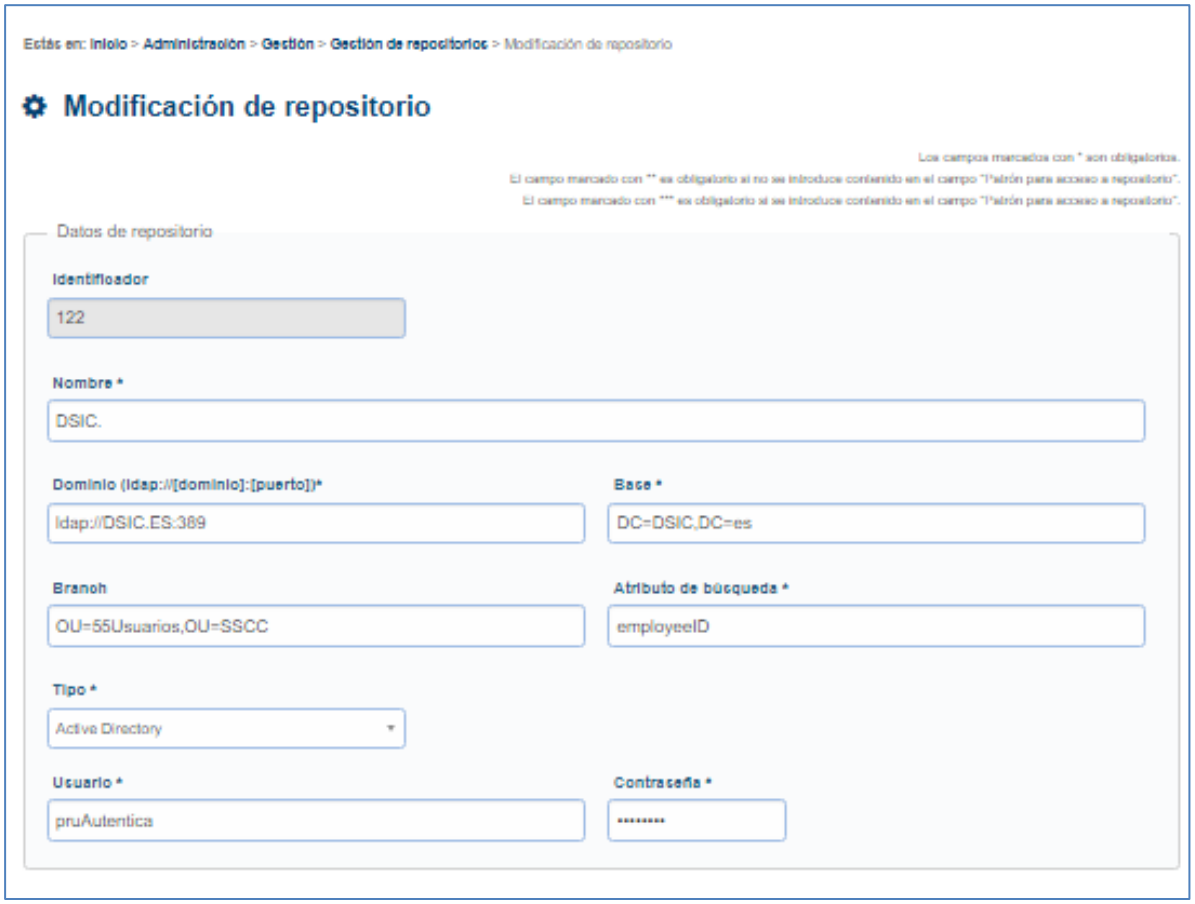
Se mostrará la lista de repositorios existentes para elegir cual se quiere modificar.

Elija repositorio a modificar

Número de registros a mostrar: 10 Buscar:

Identificador	Nombre	Usuario	Dominio	Base	Attr. Búsqueda	Tipo
2	DSIC	pruAutentica	ldap://DSIC.ES:389	DC=DSIC,DC=es	employeeID	AD
21	Meyss (Andromeda)	autentica	ldap://10.16.71.121:389	DC=trabajo,DC=dom	sAMAccountName	AD
61	Meyss trabajo (Controlador de dominio)	autentica	ldap://datrabajo.meyss.autentica.redsara.es:389	DC=trabajo,DC=dom	sAMAccountName	AD
81	INAP	autentica	ldap://10.1.128.150:389	DC=inap,DC=es	employeeID	AD
101	Meyss Inspección - Roble (IP)	U_AUTENTICA_CN	ldap://10.16.71.200:389	DC=inspeccion,DC=dom	sAMAccountName	AD

Al seleccionar el repositorio se muestra un formulario para la modificación, en el cual se tiene la opción de seleccionar las unidades mediante el botón “Mostrar”.



Estás en: Inicio > Administración > Gestión > Gestión de repositorios > Modificación de repositorio

Modificación de repositorio

Los campos marcados con * son obligatorios.
El campo marcado con ** es obligatorio si no se introduce contenido en el campo "Patrón para acceso a repositorio".
El campo marcado con *** es obligatorio si se introduce contenido en el campo "Patrón para acceso a repositorio".

Datos de repositorio

Identificador: 122

Nombre *: DSIC.

Dominio (ldap://[dominio]:[puerto])*: ldap://DSIC.ES:389

Base *: DC=DSIC,DC=es

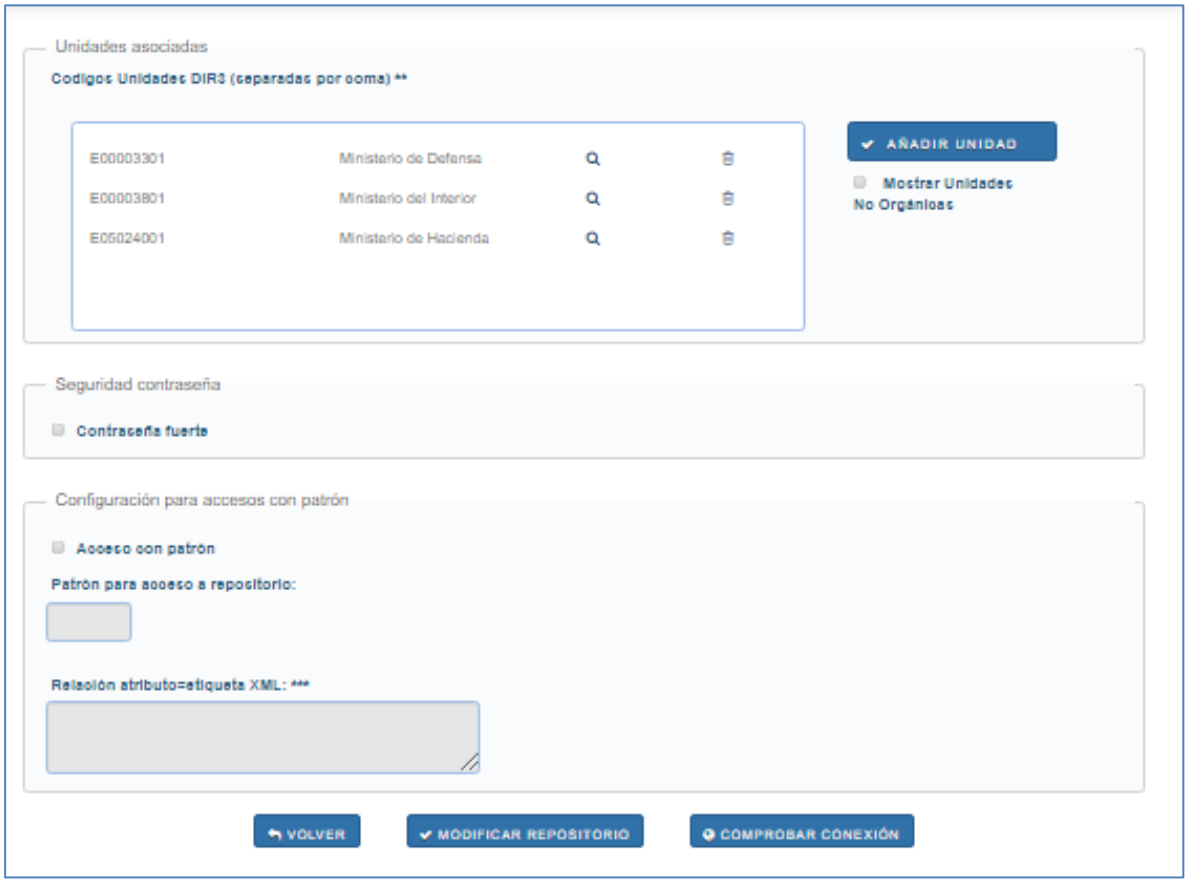
Branch: OU=55Usuarios,OU=SSCC

Atributo de búsqueda *: employeeID

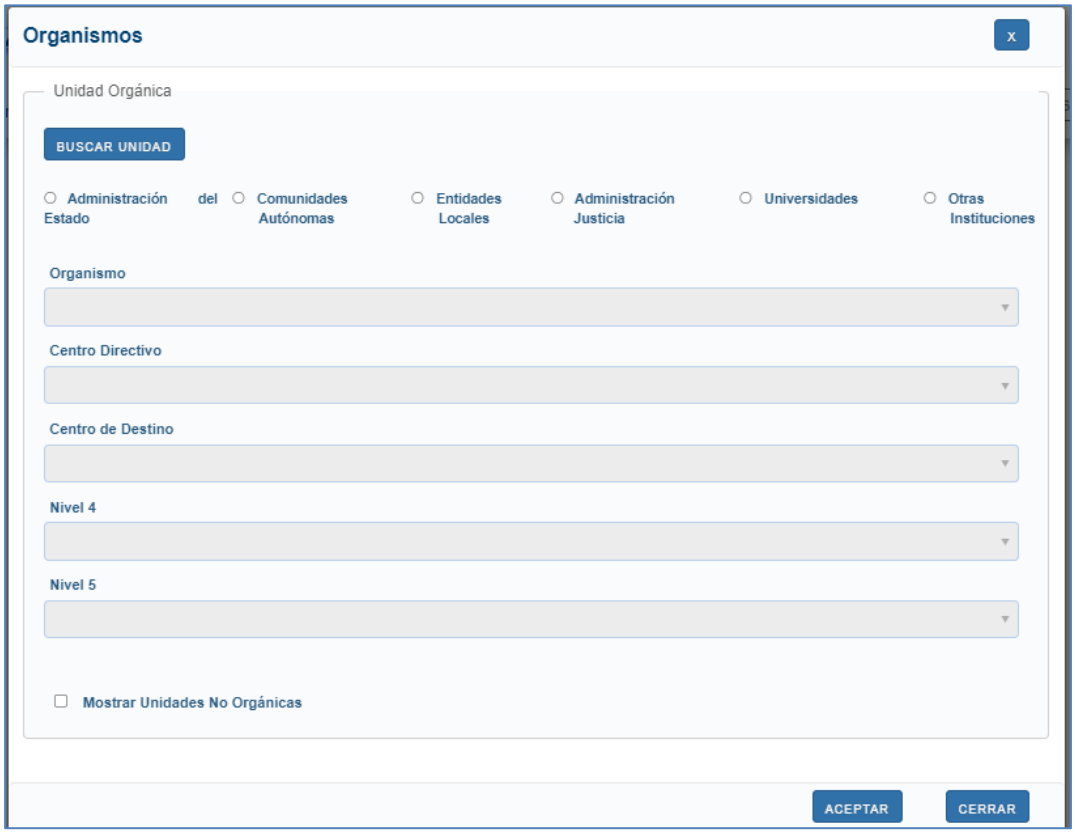
Tipo *: Active Directory

Usuario *: pruAutentica

Contraseña *: ********



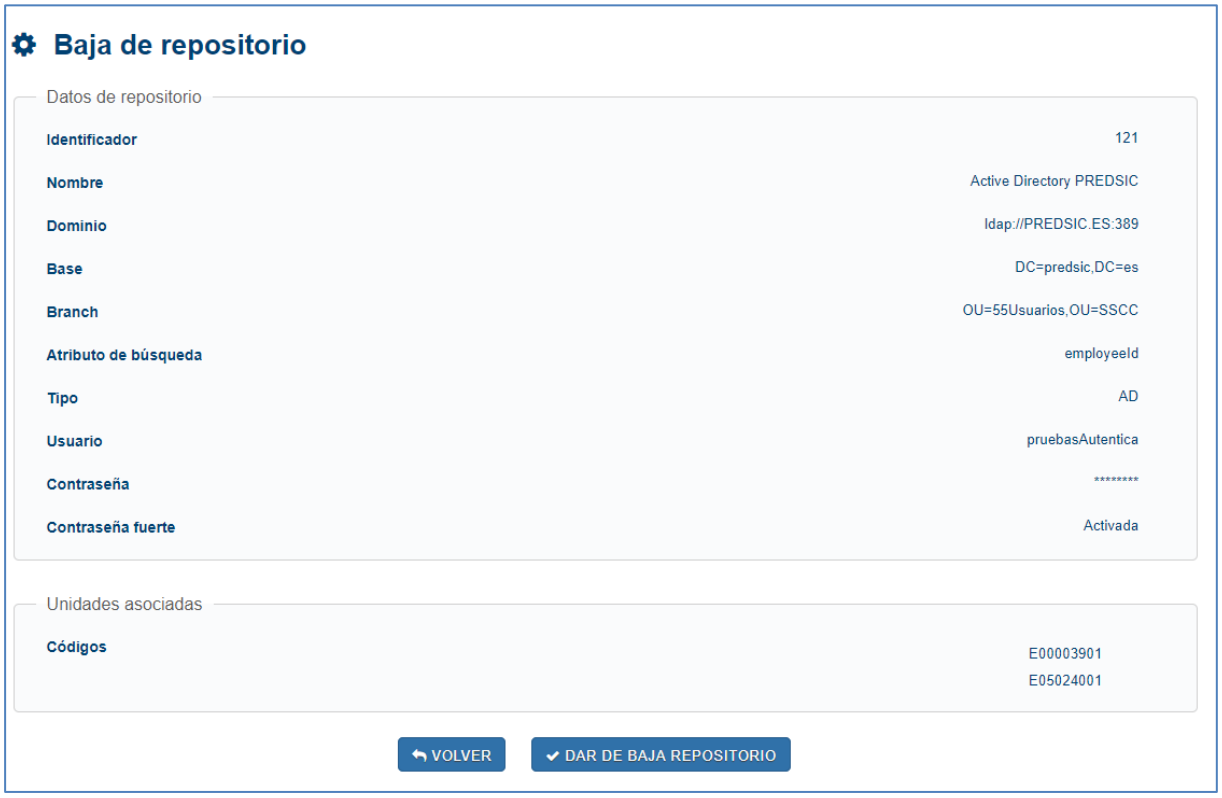
En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



2.5.1.4.3 Baja de repositorio

Se mostrará la lista de repositorios existentes para elegir cual se quiere dar de baja.

Identificador	Nombre	Usuario	Dominio	Base	Attr. Búsqueda	Tipo
2	DSIC	pruAutentica	ldap://DSIC.ES:389	DC=DSIC,DC=es	employeeID	AD
21	Meyss (Andromeda)	autentica	ldap://10.16.71.121:389	DC=trabajo,DC=dom	sAMAccountName	AD
61	Meyss trabajo (Controlador de dominio)	autentica	ldap://datrabajo.meyss.autentica.redsara.es:389	DC=trabajo,DC=dom	sAMAccountName	AD
81	INAP	autentica	ldap://10.1.128.150:389	DC=inap,DC=es	employeeID	AD

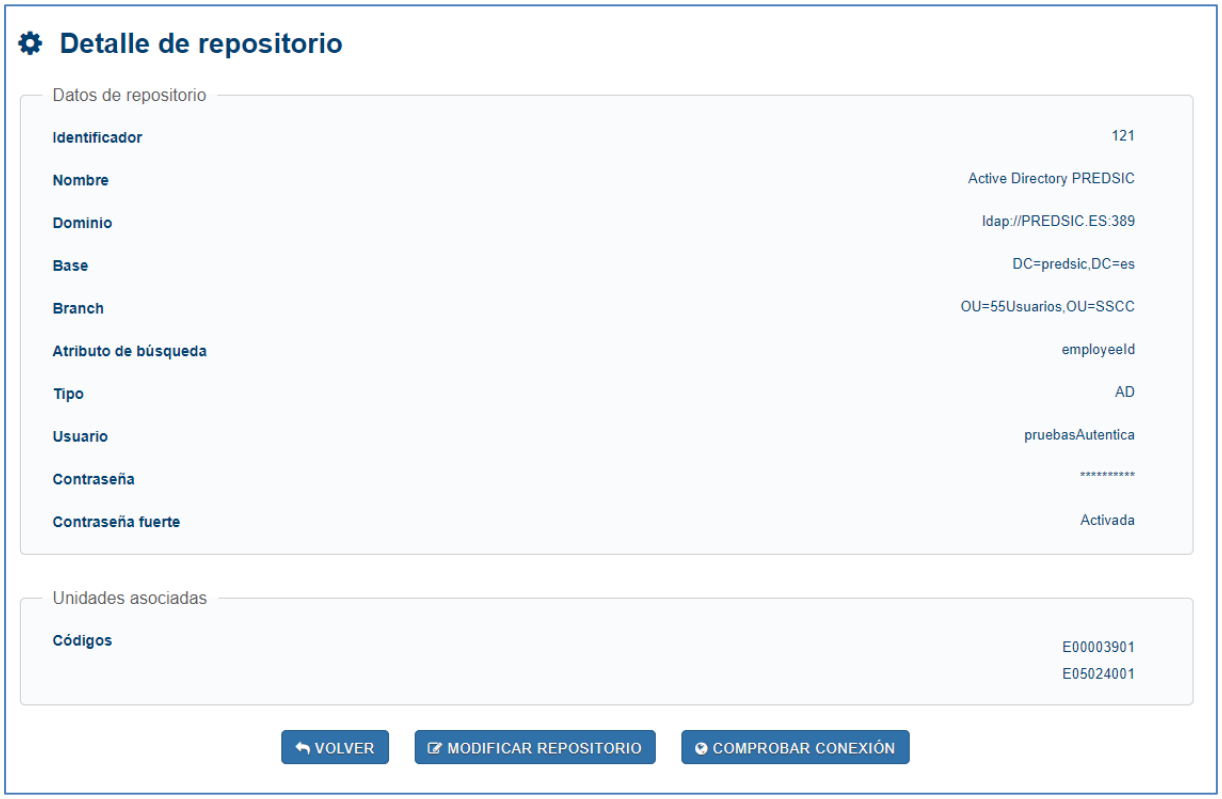


2.5.1.4.4 Listado de repositorios

Se mostrará la lista de repositorios existentes para ver el detalle del repositorio que nos interese.

Identificador	Nombre	Usuario	Dominio	Base	Attr. Búsqueda	Tipo
2	DSIC	pruAutentica	ldap://DSIC.ES:389	DC=DSIC,DC=es	employeeID	AD
21	Meyss (Andromeda)	autentica	ldap://10.16.71.121:389	DC=trabajo,DC=dom	sAMAccountName	AD
61	Meyss trabajo (Controlador de dominio)	autentica	ldap://datrabajo.meyss.autentica.redsara.es:389	DC=trabajo,DC=dom	sAMAccountName	AD
81	INAP	autentica	ldap://10.1.128.150:389	DC=inap,DC=es	employeeID	AD

Al pulsar sobre un repositorio determinado, se mostrará el detalle del mismo.



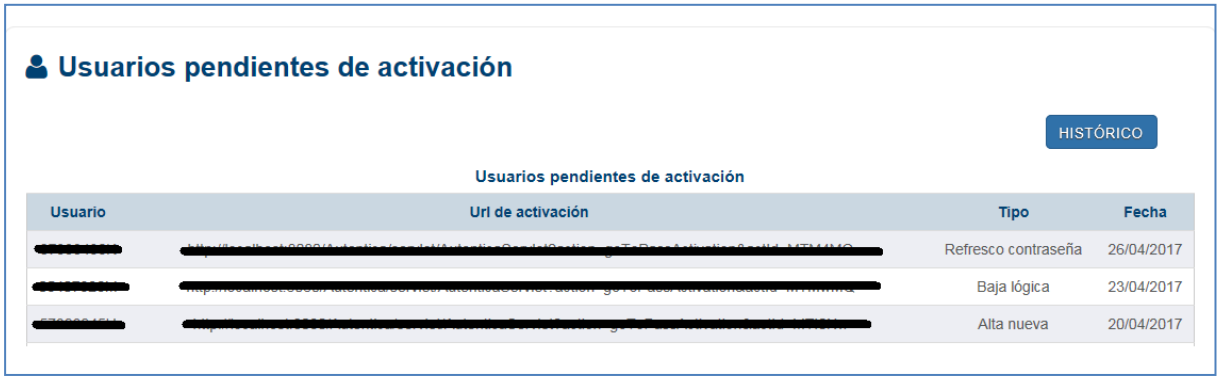
2.6.1.6. GESTIÓN DE ALERTAS Y VISIBILIDAD

2.6.1.7. GESTIÓN DE USUARIOS PENDIENTES DE ACTIVACIÓN

Esta opción permite visualizar las URL´s que los usuarios pendientes de activación reciben por correo para poder activar su contraseña.

Los usuarios pendientes de activación pueden ser de tres tipos:

- Alta nueva: Son usuarios cuya solicitud de alta ha sido aceptada.
- Refresco contraseña: Son usuarios que ha pedido una solicitud de nueva contraseña.
- Baja lógica: Son usuarios que tenían estado de baja lógica y han sido activados.



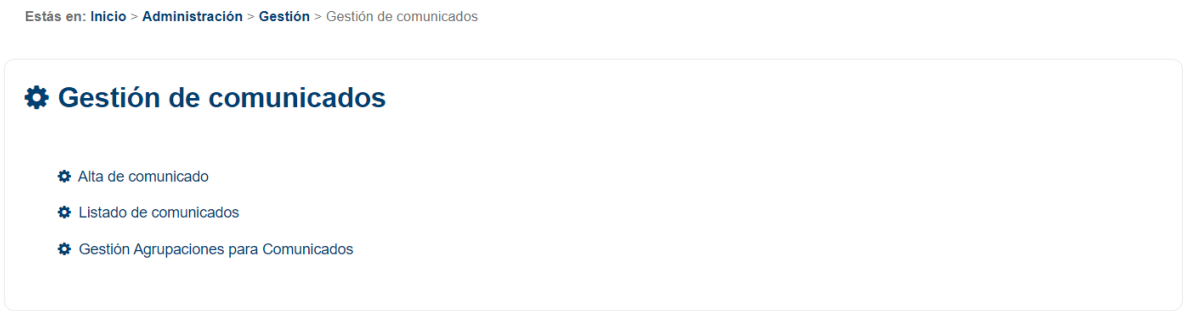
Pulsando en el botón de 'Histórico' se mostrará una pantalla con la lista de usuarios que ya han sido activados.

2.6.1.8. GESTIÓN DE COMUNICADOS

Esta opción permite a un administrador central poder enviar un comunicado, ya sea de forma programada o en el momento de generar el comunicado.

Para ello, se muestran dos opciones, una para dar de alta un comunicado y otra para ver los comunicados que se han generado, ya sea para consultarlos, modificarlos o eliminarlos.

El envío se puede realizara todos los buzones de correo de las aplicaciones integradas en Autentica o a un grupo determinado de aplicaciones, que se podrán gestionar mediante la opción Gestión Agrupaciones para Comunicados.



2.6.1.8.1. Alta de un comunicado

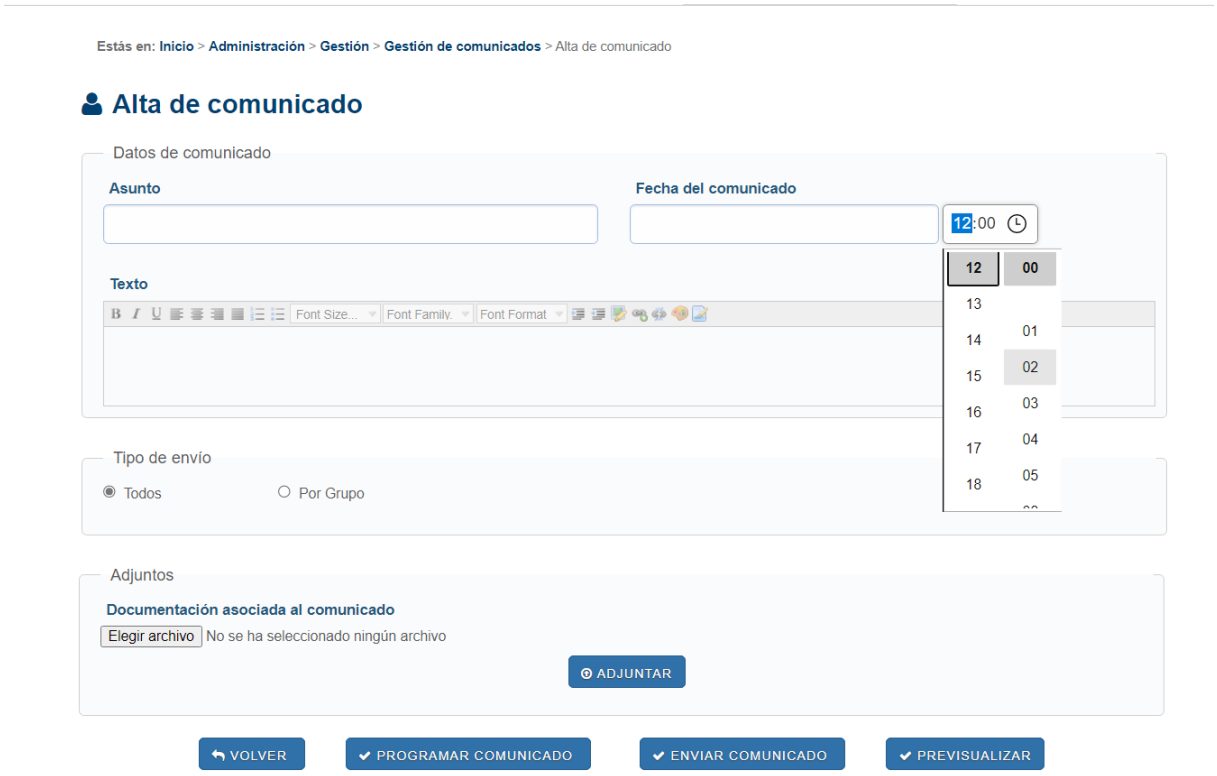
Al acceder al formulario de alta de un comunicado, el administrador deberá completar los siguientes campos obligatorios:

- Asunto: se indica el asunto del correo.
- Texto: se indica el texto del correo que se va a enviar.

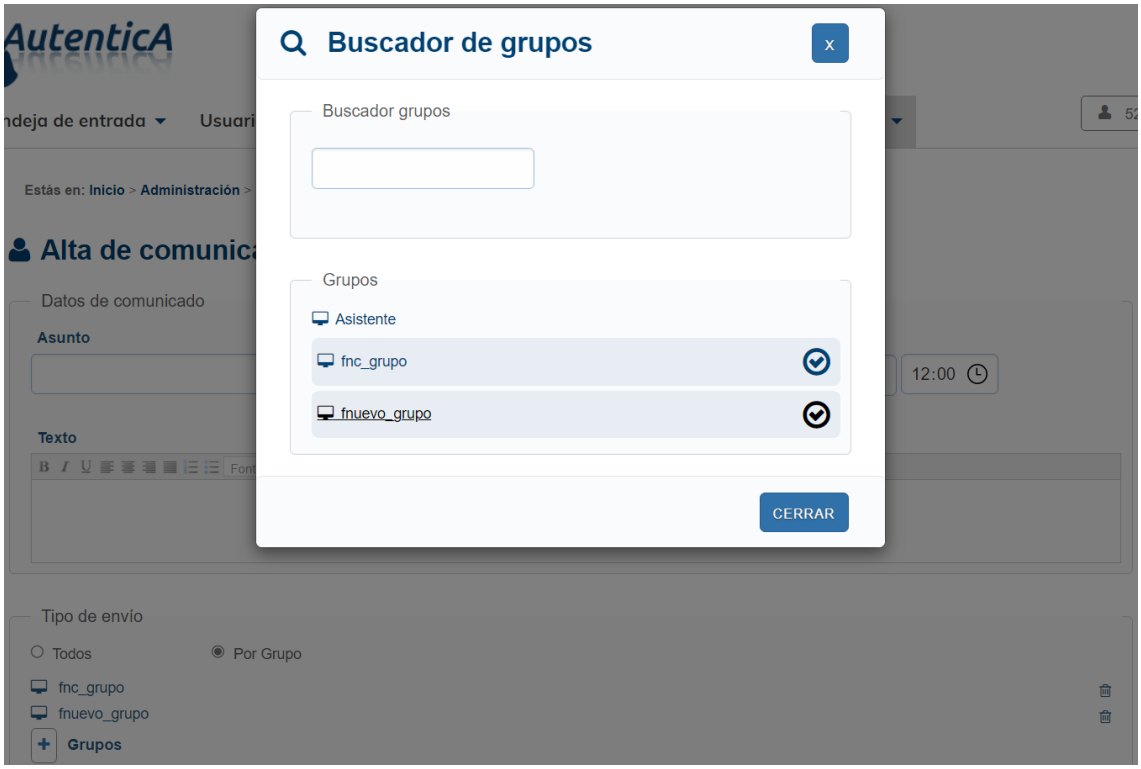
De forma opcional, podrá seleccionar algún fichero adjunto para enviar por correo. El número de adjuntos que se podrá enviar se define por medio de un fichero de configuración, permitiéndose en la actualidad enviar 2 ficheros adjuntos.

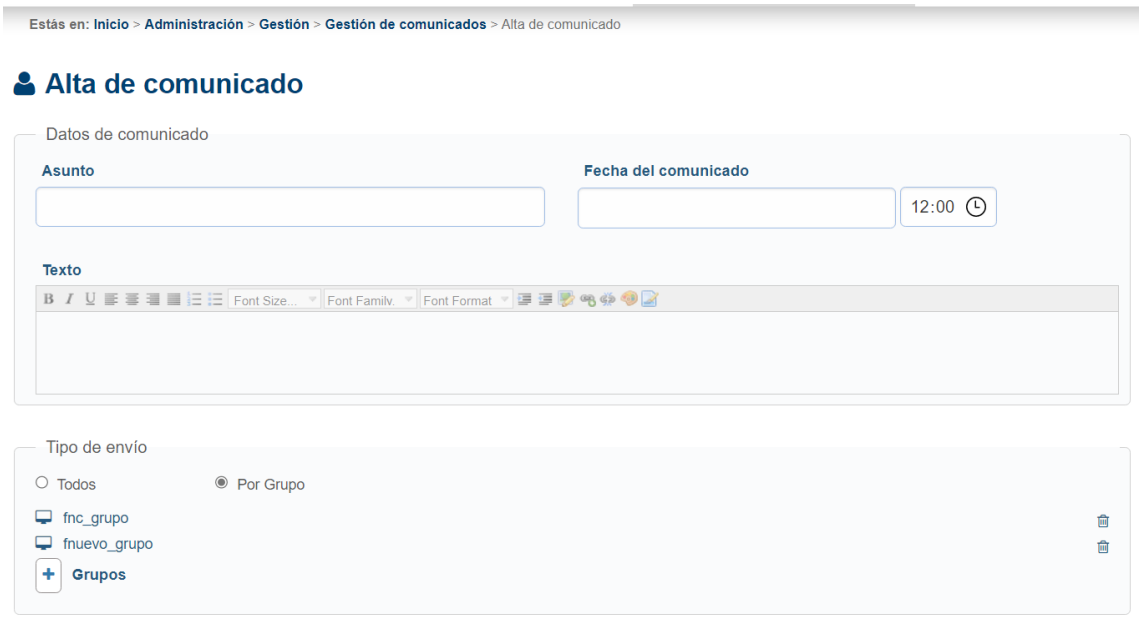
La fecha en la que se va a programar el envío del comunicado se configura en el campo "Fecha". Completar este campo sólo es obligatorio en el supuesto de programar un comunicado, ya que en el caso de que se envíe en esos momentos no se tendrá en consideración la fecha que se haya seleccionado.

Además se puede programar la hora de envío, que por defecto está a las 12:00 h.



Además, se puede seleccionar a que grupos de aplicaciones va dirigido el comunicado, enviándose solamente a los buzones de las aplicaciones que forman los grupos seleccionados.

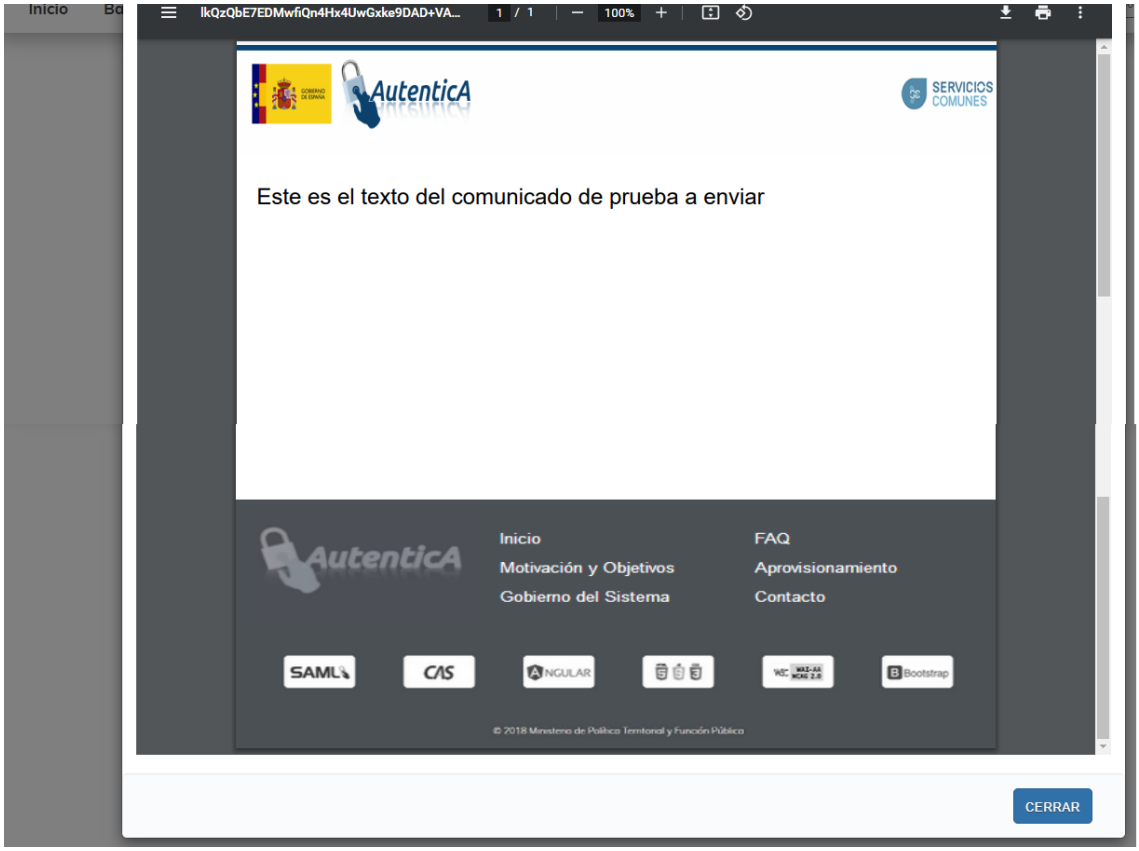




Una vez completados los campos del comunicado a enviar, se podrá pulsar, según la acción que se desee realizar, los botones “Programar comunicado” o “Enviar comunicado”, mostrándose una pantalla al administrador, en el caso de que se haya generado correctamente,

En cualquiera de los dos casos, el comunicado que se haya configurado se podrá ver en el apartado “Listado de comunicados”.

Si así se desea, pulsando el botón “Previsualizar”, se muestra el formato del comunicado a enviar.

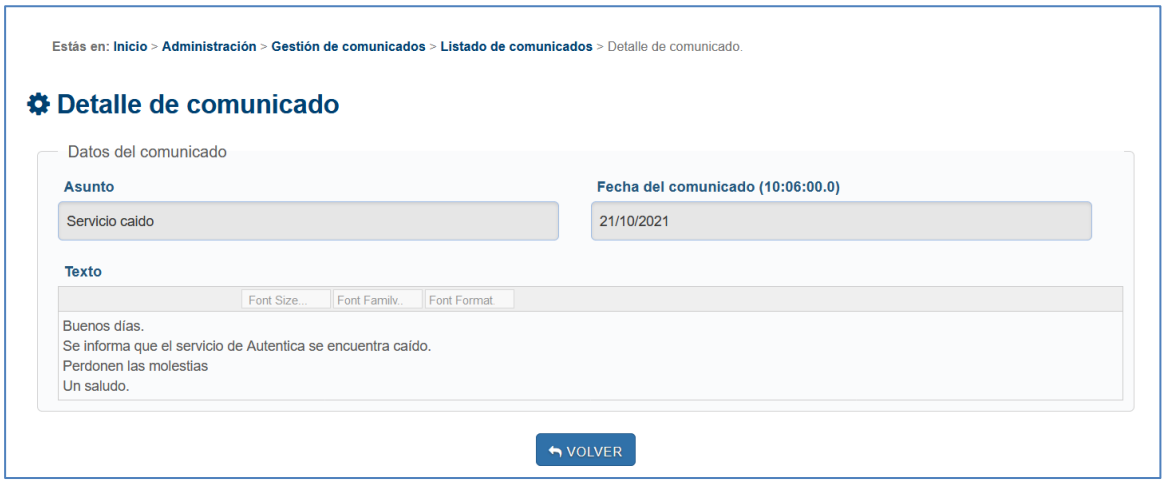


2.6.1.8.2. Listado de comunicados

Al acceder a esta opción, se muestra al administrador central un listado paginado ordenado por la fecha más reciente, con los comunicados emitidos y programados.

- Para aquellos comunicados programados que todavía no han sido enviados, se muestran tres opciones: “Ver detalle”, “Modificar” y “Eliminar”.
- Para aquellos comunicados que ya han sido enviados, sólo se muestra la opción “Ver detalle”.

En la opción “Ver detalle” (icono libro), podremos ver el comunicado en modo consulta.



En la opción “Modificar” (icono lápiz), podremos ver el comunicado y modificarlo. Sólo se podrá acceder a esta opción si el comunicado no ha sido enviado.

En la opción “Eliminar” (icono papelera), podremos ver el comunicado en modo consulta y eliminarlo. Sólo se podrá acceder a esta opción si el comunicado no ha sido enviado.

2.6.1.8.3. Gestión de Agrupaciones para comunicados

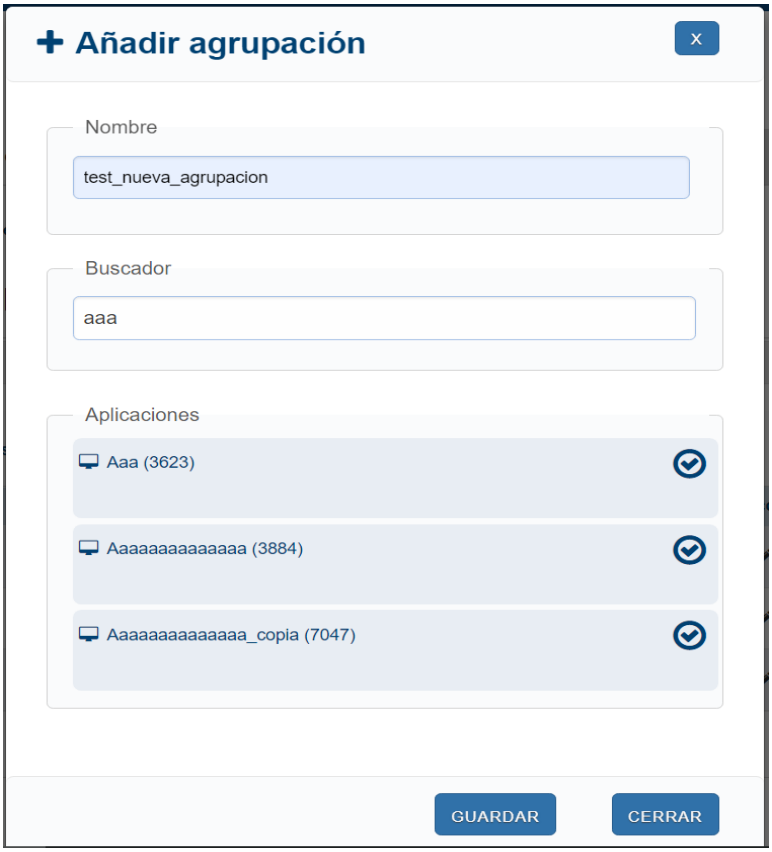
El usuario accede a la gestión de agrupaciones de aplicaciones para comunicados, pulsando sobre la opción de menú que aparece en la página principal de gestión de comunicados.

Seleccionando la opción Gestión de Agrupaciones para Comunicados, se accede al formulario para gestión de agrupaciones.

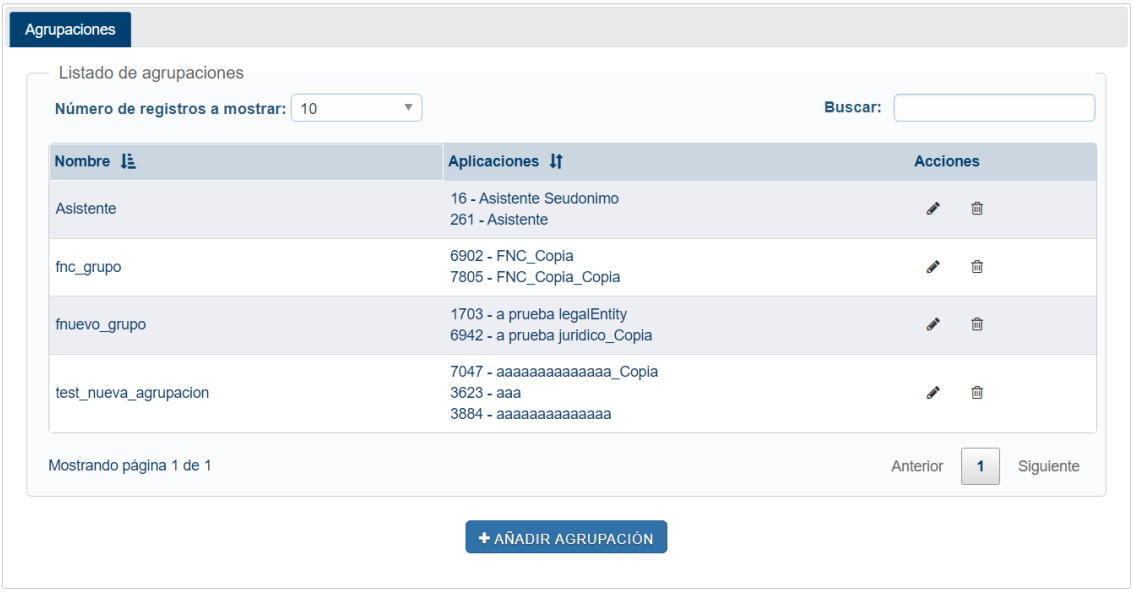
- Alta de una nueva agrupación de aplicaciones

Pulsando sobre la opción Añadir Agrupación, se muestra una ventana modal donde el usuario debe indicar un nombre de la agrupación y seleccionar aquellas aplicaciones que la componen.

Además, se dispone de un buscador para filtrar por aquellas aplicaciones que coincidan con el patrón indicado en el campo Buscador:

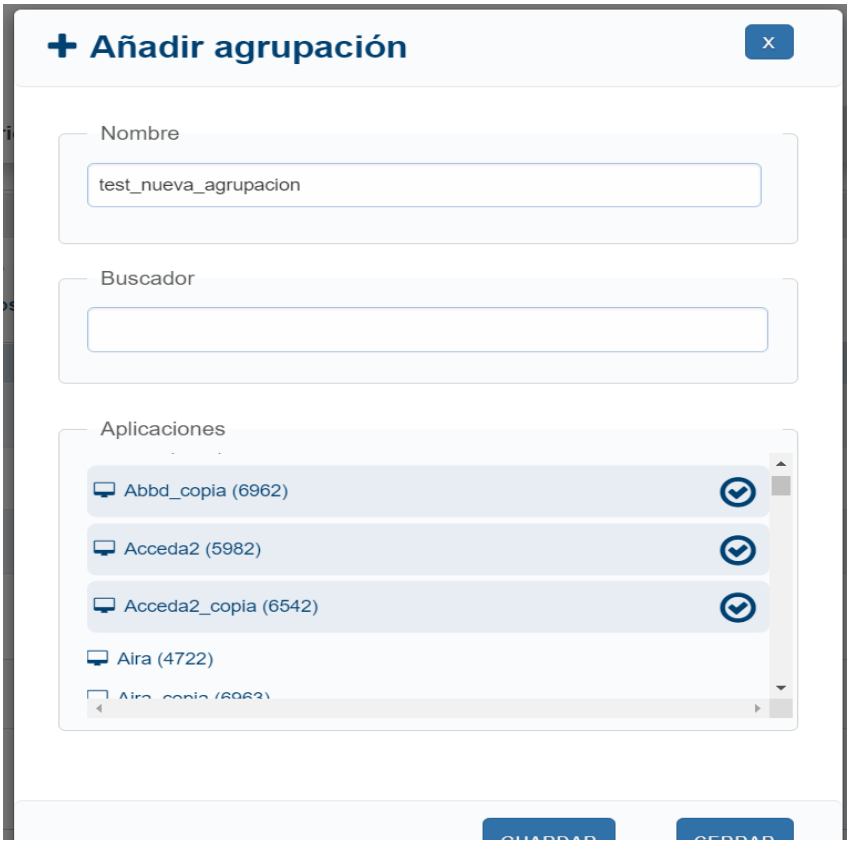


Si el alta de la nueva agrupación ha sido correcta, se mostrará en el listado de agrupaciones y aplicaciones, así como habrá nuevos registros en las tablas

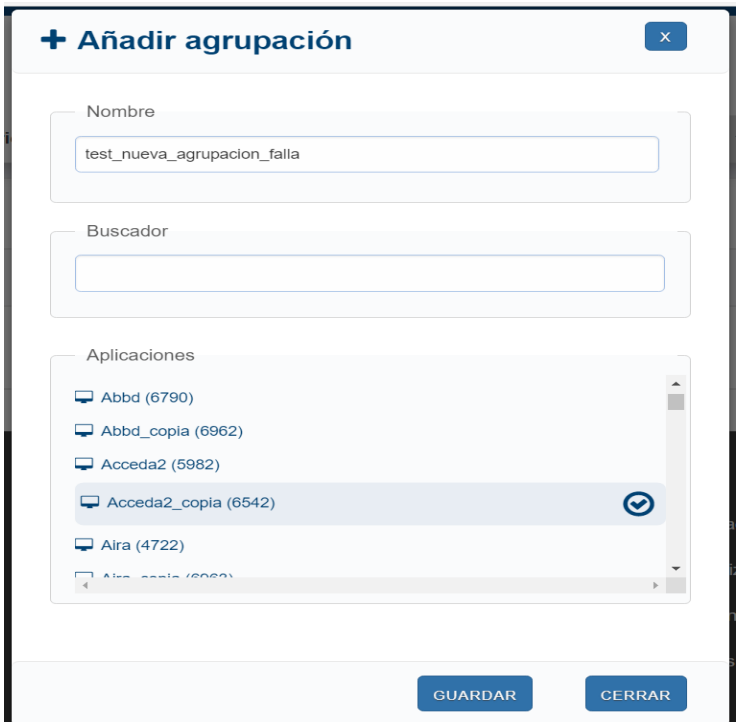


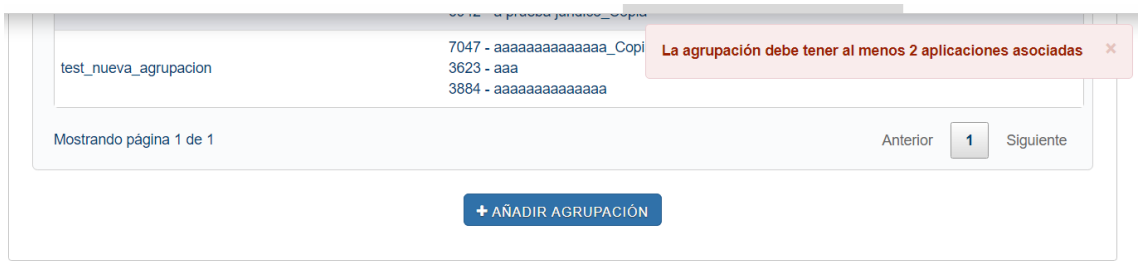
En caso que no se pueda dar de alta la agrupación, se mostrará un mensaje informativo como resultado de la operación a regresar a la pantalla de listado de agrupaciones.

- Nombre de agrupación ya introducido

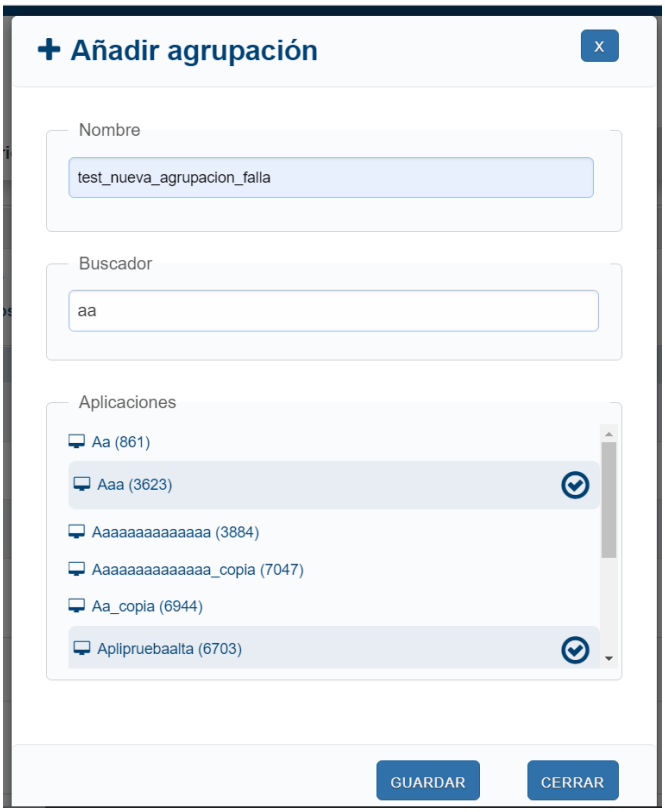


- Número de aplicaciones seleccionadas inferior al permitido



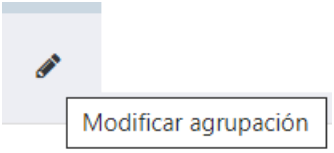


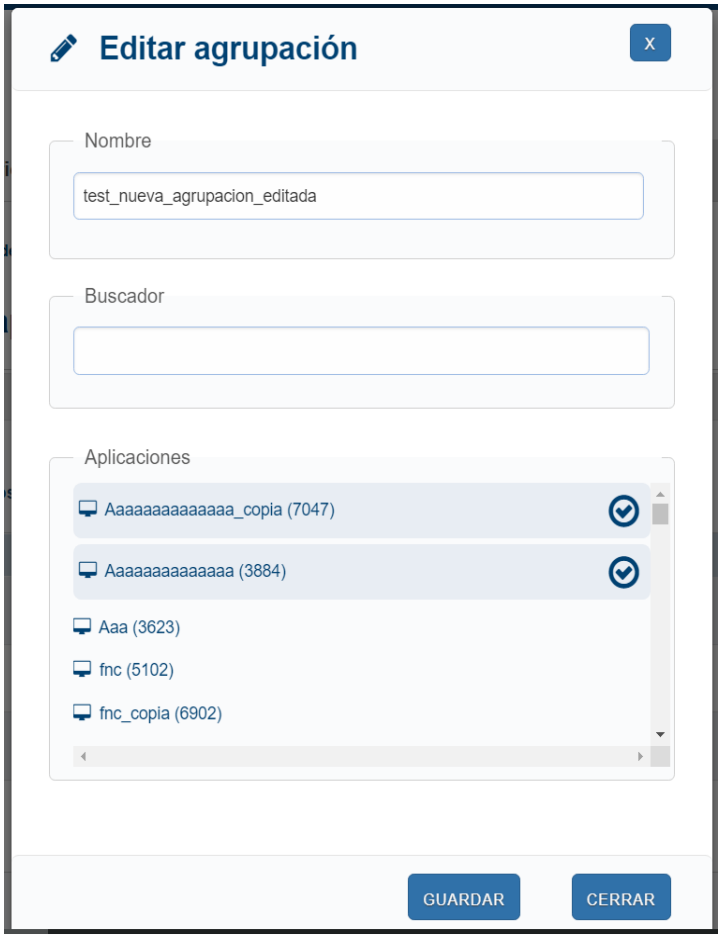
- Se ha seleccionado una aplicación ya asociada a otra agrupación



- Editar una agrupación.

El usuario puede editar una agrupación del listado de agrupaciones, pulsando sobre el icono lapicero



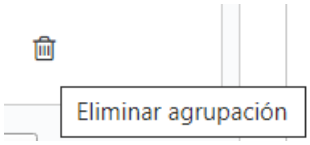


El usuario puede cambiar el nombre de la agrupación y/o las aplicaciones que la componen.

Las restricciones para poder editar la agrupación son las mismas que para el alta.

- Eliminar una agrupación.

El usuario podrá eliminar una agrupación, desde el icono



, donde borrará de la tabla agrupaciones el registro correspondiente y la relación de aplicaciones que la componen.

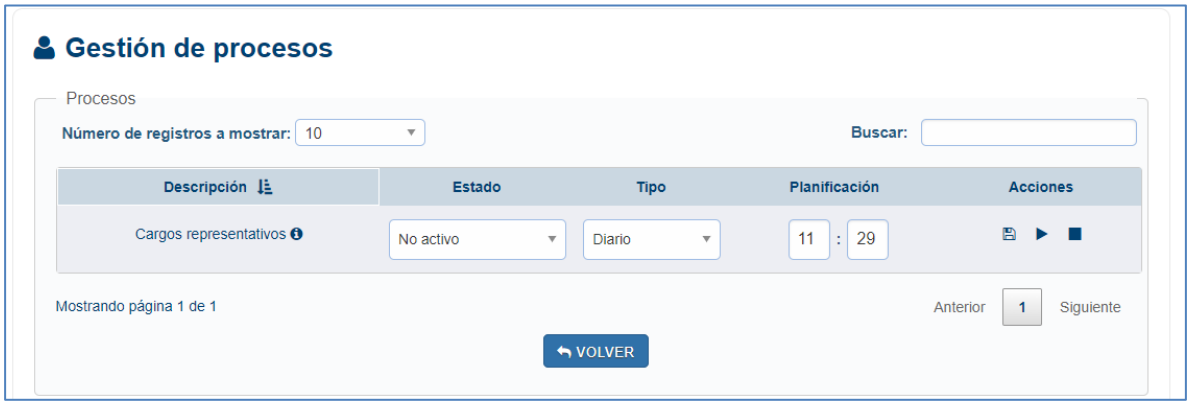
Esto permite usar esas aplicaciones para otra agrupación.

2.6.1.9. GESTIÓN DE PROCESOS

Esta opción permite a un administrador central con permiso de aplicaciones internas poder

gestionar los procesos auxiliares de Autentica, desde la cual se podrá planificar la ejecución de los mismos o realizar una ejecución manual.

Para ello, se muestra en la pantalla un listado de los procesos disponibles con los datos de planificación como son la activación, el tipo de programación, el día (según el tipo de planificación) y la hora; así como, las opciones de guardar, ejecutar o detener el proceso.



En la opción “Guardar”(ícono guardar), se podrá modificar los datos de planificación del proceso, una vez guardado los datos del mismo, se realiza una planificación de la próxima ejecución del proceso siempre que se seleccione como activo, el cual se ejecutará en la fecha y hora correspondiente.

En la opción “Ejecutar”(ícono iniciar), se podrá realizar una ejecución puntual del proceso y al finalizar se notificará al administrador.

En la opción “Detener”(ícono detener), se podrá detener el proceso seleccionado, el cual debe estar en ejecución.

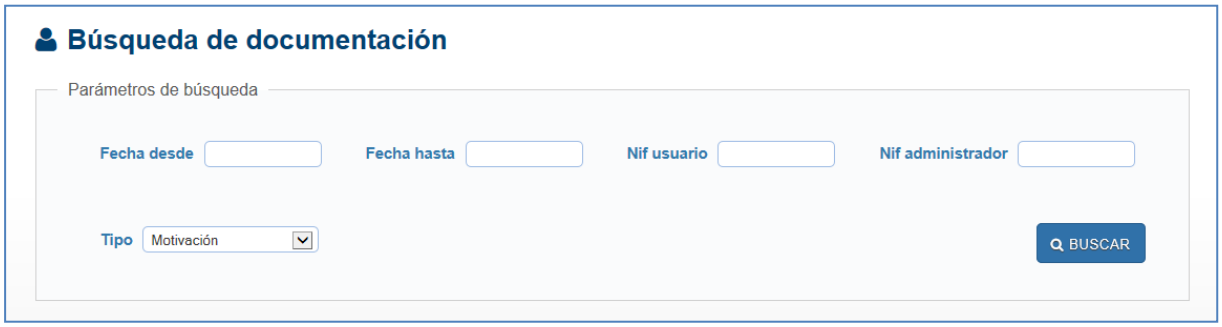
2.6.2. DOCUMENTACIÓN

Desde esta opción se podrá buscar toda la documentación adjuntada por los usuarios o administradores, así como todos los documentos generados a la hora de firmar cada operación.

Se puede filtrar por:

- Fechas, fecha inicio y fecha fin, se mostrarán todos los documentos comprendidos entre esas fechas.
- Nif usuario, búsqueda por Nif de un determinado usuario.
- Nif administrador, búsqueda por Nif de un determinado administrador.
- Motivación, gestión de usuarios y auto registro.
- También se puede buscar alternando entre ellos.

Una vez se pulse a buscar, se generara un listado con los resultados obtenidos. Cada uno de ellos con la información del documento (Nombre, fecha, usuario y administrador que han intervenido, operación y botón de visualización).



2.6.3. SINCRONIZACIÓN DIR3

Esta funcionalidad mostrará al administrador los usuarios y unidades que se queden pendientes de actualizar, después de que se ejecute el proceso de sincronización entre Autentica y DIR3. Este proceso hace una actualización de las unidades en las que ha cambiado algún dato respecto a los que había.

2.6.3.1. Usuarios pendientes DIR3

Se mostrará una lista con los usuarios que pertenecen a alguna unidad en la que se ha producido algún cambio. Sólo aparecerán en esta lista si los cambios afectan a una antigua unidad que se ha dividido y no se puede saber la nueva unidad a la que asociarle, o si la antigua unidad se ha extinguido.

Pulsando sobre el registro, se mostrará una pantalla con el formulario para asignar una nueva unidad al usuario.

2.6.3.2. Unidades pendientes DIR3

Se mostrará una lista con las unidades que han sufrido algún cambio. Sólo aparecerán en esta lista si la antigua unidad se ha dividido y no se puede saber la nueva unidad a la que se corresponde, o si la antigua unidad se ha extinguido.

Bandeja de entrada de unidades pendientes de sincronización con DIR3

Unidades

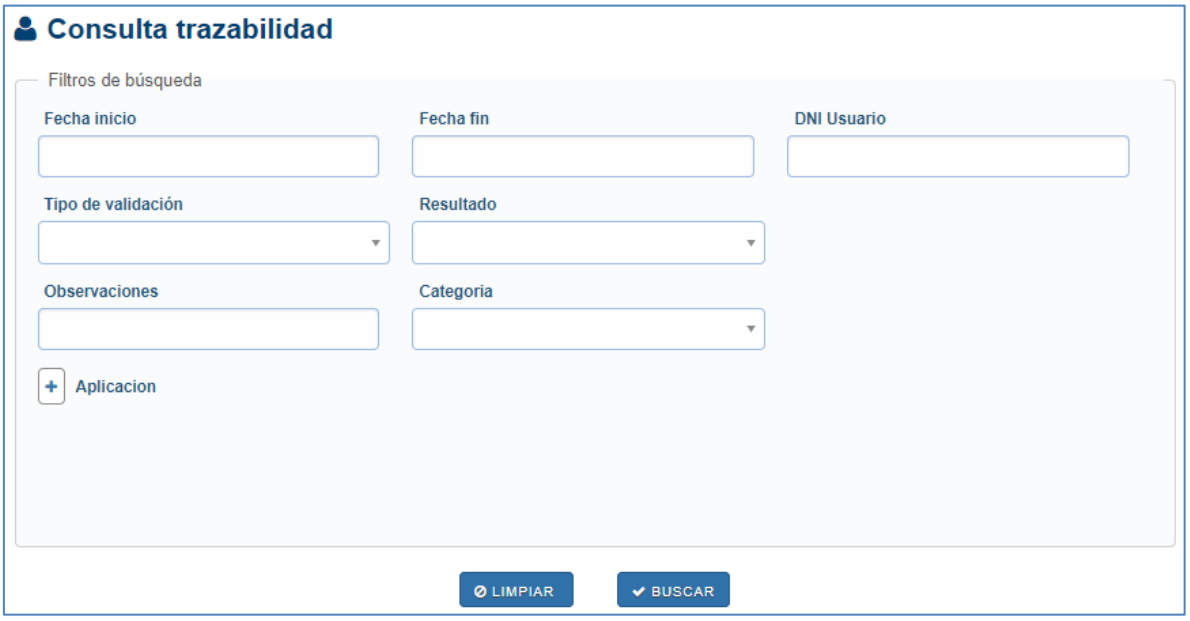
Unidad anterior	Unidades últimas	Fecha de la sincronización
A03006297 (DIRECCIÓN GENERAL DE PLANIFICACIÓN, ORDENACIÓN E INNOVACIÓN SANITARIAS)	A03016142 (Dirección General de Política Sanitaria)	24/08/2016
A12002997 (CONSELLERÍA DE MEDIO AMBIENTE, TERRITORIO E INFRAESTRUCTURAS)	A12017418 (Consellería de Infraestructuras y Vivienda)	24/08/2016
A09010588 (BARCELONA MOBILE WORLD CAPITAL FOUNDATION)	A09019097 (Barcelona Mobile World Capital Foundation)	24/08/2016
A03002954 (CONSEJERÍA DE ECONOMÍA Y EMPLEO)	A03015217 ()	24/08/2016
A14005413 (D.G ADMINISTRACION LOCAL Y RELACIONES INSTITUCIONALES)	A14013890 (Direccion General Administracion Local)	24/08/2016
A03002952 (CONSEJERÍA DE PRESIDENCIA)	A03015214 ()	24/08/2016
U01700174 (VICERRECTORADO DE INFRAESTRUCTURAS)	U01700190 (Vicerrectorado de Desarrollo Digital y Evaluació	24/08/2016
LA0007431 ()	LA0008537 (D.G. de Recursos Humanos)	24/08/2016
A03003817 (CONSEJERÍA DE BIENESTAR SOCIAL Y VIVIENDA)	A03015224 ()	24/08/2016
A03003853 (DIRECCIÓN GENERAL DE CALIDAD AMBIENTAL)	A03016219 (Dirección General de Calidad Ambiental)	24/08/2016
A03003816 (CONSEJERÍA DE EDUCACIÓN, CULTURA Y DEPORTE)	A03015221 ()	24/08/2016

2.6.4. CONSULTA TRAZABILIDAD

2.6.4.1. Trazabilidad

Esta funcionalidad mostrará al administrador un listado con los accesos realizados por los usuarios, informando de la hora, la aplicación, la categoría, el tipo de validación, el resultado de la misma y las observaciones en caso de que las haya.

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.



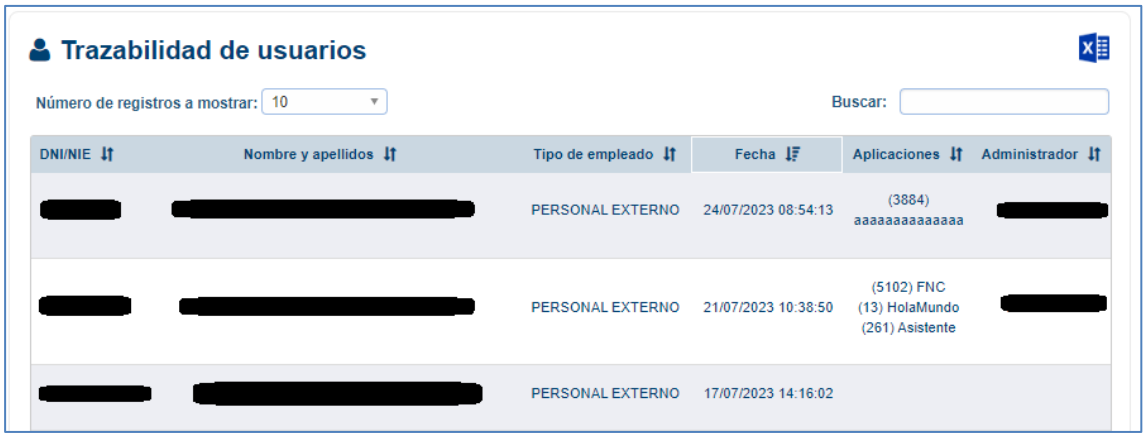
Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

2.6.4.2. Trazabilidad de usuarios

Esta funcionalidad mostrará al administrador un listado con los usuarios con datos gestionados, informando del DNI/NIE, nombre y apellidos, tipo de empleado, fecha de última actualización, aplicaciones asociadas y administrador de última actualización.

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.

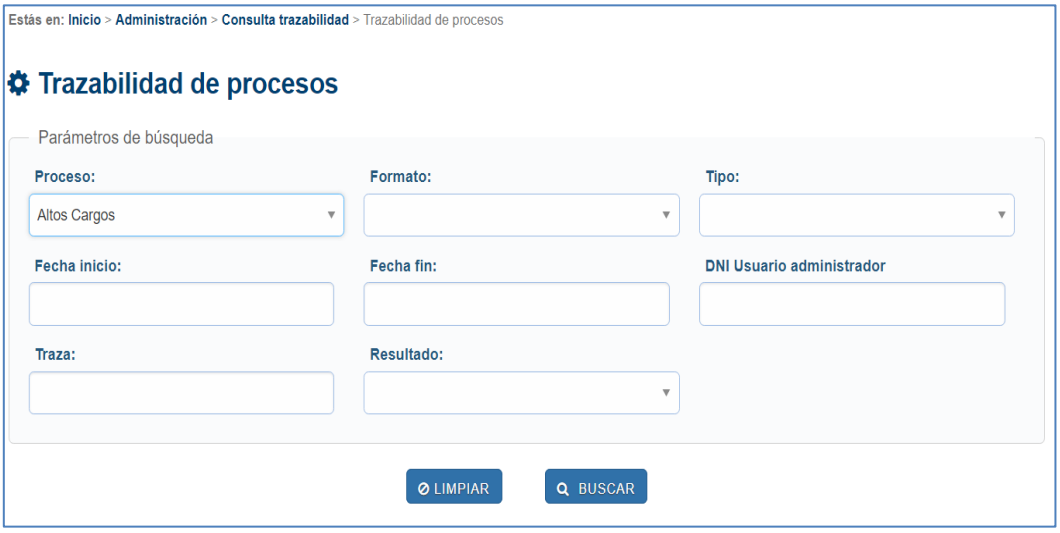
Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

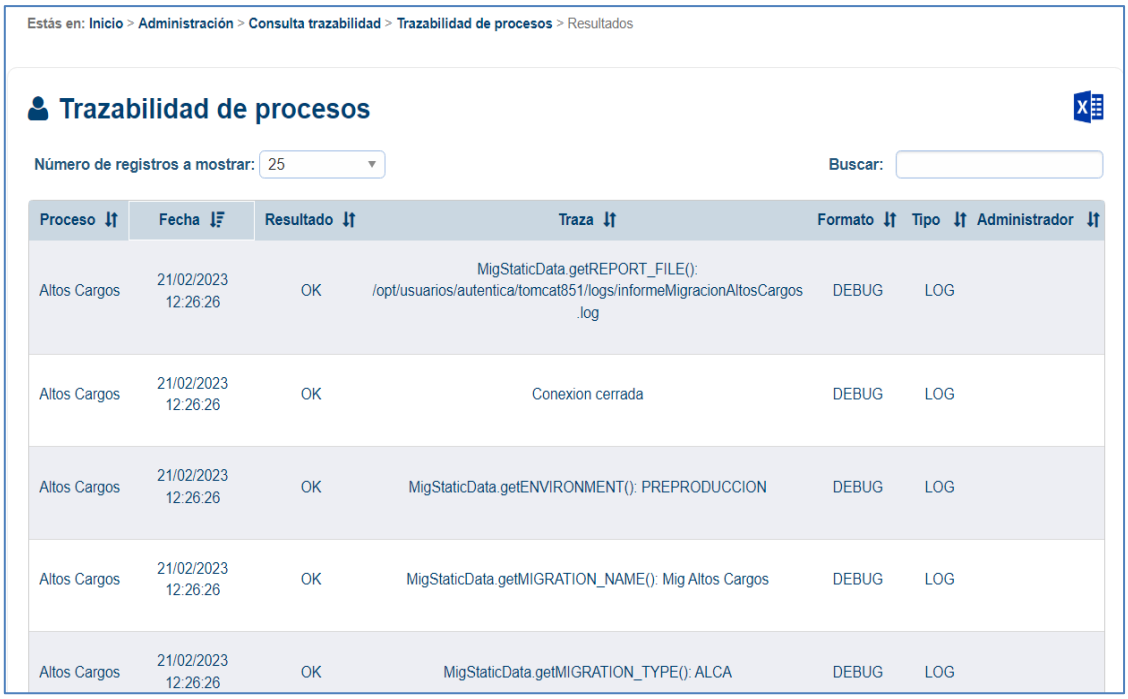


2.6.4.3. Trazabilidad de procesos

Esta funcionalidad mostrará al administrador un listado con los procesos realizados por los usuarios, informando del proceso, fecha, resultado, traza, formato, tipo y administrador

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.





Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

2.6.4.4. Trazabilidad de autorización

Esta funcionalidad mostrará al administrador un listado con las autorizaciones que tienen los usuarios, informando la aplicación, DNI usuario, DNI administrador, perfil, rol, fecha y tipo.

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.

Aplicacion	Dni usuario	Dni usuario administrador	Perfil	Rol	Fecha	Tipo
261	09748856F	02275580Y	CIUDADANO	C16_CONSULTA - SENDAS	29-10-2019 01:15:58	Modificado
261	09748856F	02275580Y	CIUDADANO	C17_CONSULTA - SOLICITUDES	29-10-2019 01:15:58	Modificado
261	00408258P	02275580Y	ADMINISTRADOR	PROFESOR	29-10-2019 12:53:22	Modificado
261	00408258P	02275580Y	ADMINISTRADOR	USER_ROLE	29-10-2019 12:53:22	Modificado
261	00408258P	02275580Y	ADMINISTRADOR	JSV	29-10-2019 12:53:21	Modificado
261	09748856F		CIUDADANO	C16_CONSULTA - SENDAS	29-10-2019 12:04:30	Alta
2481	53389876E	02275580Y	TUTORIA	ALUMNO	05-11-2019 11:09:29	Modificado
2481	09748856F	02275580Y	FUNCIONARIO (REA)	ROL POR DEFECTO	05-11-2019 08:04:18	Alta
2481	53389876E	02275580Y	TUTORIA	ALUMNO	29-10-2019 03:42:43	Baja
2481	53389876E	02275580Y	TUTORIA	ALUMNO	29-10-2019 03:40:54	Baja

Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

2.6.4.5. Trazabilidad de permisos

Esta funcionalidad mostrará al administrador un listado con las modificaciones se han realizado en gestión de permisos.

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.

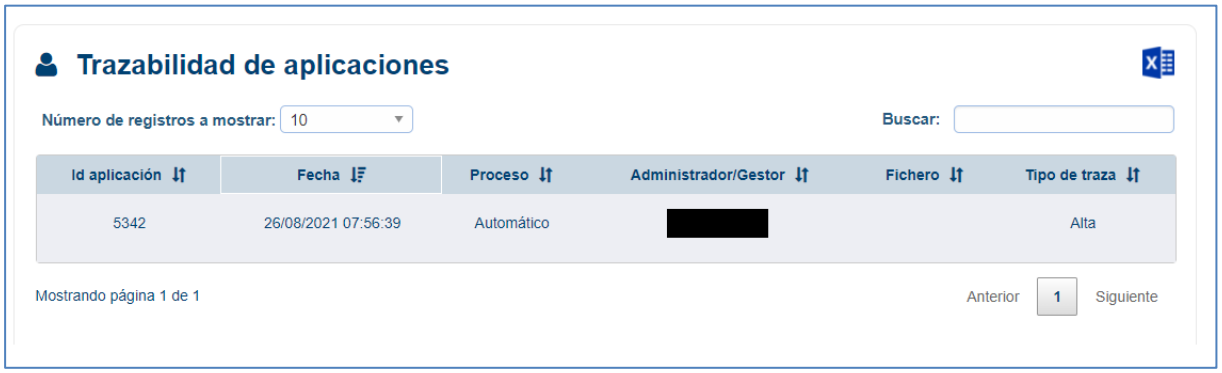
Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

2.6.4.6. Trazabilidad de aplicaciones

Esta funcionalidad mostrará al administrador un listado con las trazas de procesos sobre las aplicaciones, informando la aplicación, la fecha, el tipo de proceso, el administrador que ejecutó el proceso, el fichero backup en caso de que exista y el tipo de traza grabada.

Tendrá un formulario previo para acotar la búsqueda de trazabilidades.

Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.



2.6.4.7. Trazabilidad de FNC

Esta funcionalidad mostrará al administrador un listado con las operaciones de firma no criptográfica realizadas. Para ello, dispone de un formulario de búsqueda con el fin de filtrar los resultados obtenidos, con las opciones de fecha de inicio y fin, firmante, csv y aplicaciones; así como, los tipos de documentos firmados que podrá ser para los procesos internos de Autentica u otro tipo de documento.

Los resultados se muestran por defecto ordenados por fecha, pudiéndose ordenar por otros campos pulsando sobre la cabecera de las columnas, mostrándose los datos ordenados de mayor a menor.

Los datos que se muestran son el nombre del fichero, el justificante, la fecha de firma, el DNI/NIE del usuario firmante del documento, la aplicación desde la que se realizó la operación de firma no criptográfica y el CSV. Además, hay una columna “Evidencias” para descargar un fichero en formato .zip con las evidencias recogidas de la firma. Este fichero contiene un fichero .pdf con el resumen de la firma, un fichero .txt con el resumen criptográfico del fichero firmado y un fichero .txt con la evidencia de la autenticación realizada para realizar la firma no criptográfica.

Se podrá descargar el fichero firmado pulsando en el nombre del mismo que se encuentra en la columna “Nombre del fichero”, así como el justificante, pulsando sobre el nombre del fichero que se encuentra en la columna “Justificante”.

En la parte superior de la tabla se muestra un botón para que un usuario pueda descargarse todos los registros buscados en un fichero Excel.

2.6.4.8. Trazabilidad de cargas masivas

Esta funcionalidad mostrará al administrador un listado de las cargas masivas realizados por los usuarios, informando de la carga realizada, fecha, resultado, traza, formato, tipo y administrador

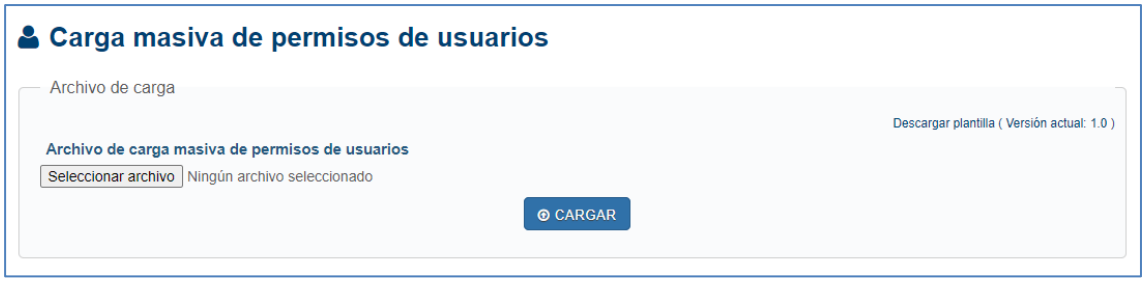
Tendrá un formulario previo para acotar la búsqueda de dichas trazabilidades.

Se puede ordenar el resultado de la consulta pulsando sobre cualquiera de los campos. Por defecto aparece ordenado por fecha más reciente. Al pulsar sobre cada una de las

columnas, la ordenación se mostrará de mayor a menor en función a los valores de la columna seleccionada. A demás tendrá un botón en la parte superior de la tabla para que un usuario pueda descargarse todos los registros buscados.

2.6.5. CARGA MASIVA DE PERMISOS DE USUARIOS

Se permitirá a los administradores asignar permisos a usuarios, tanto de autorización como de administrador delegado en Autentica, de manera masiva utilizando un fichero en formato CSV para ello.



Dicho fichero contendrá:

- ***version_#*** *(Obligatorio): Versión de la plantilla para la carga. El símbolo # se sustituye en la plantilla descargable por la última versión. El valor del campo no se debe modificar ni eliminar y no se debe rellenar la columna correspondiente.*

  Ejemplo: version_1.0

- ***COD APLICACIÓN*** *(Opcional): Código de aplicación para dar permisos de aplicación*
- ***DNI/NIE*** *(Obligatorio): NIF/NIE con formato 00000000T (sin guión y completando con ceros a la izquierda hasta 9 caracteres)*
- ***NOMBRE PROVINCIA*** *(Opcional): Nombre provincia*
- ***AD.DELEGADO*** *(Opcional): Si el usuario ya tiene permisos en autentica, no se realizará ninguna acción aunque se indique que se quieren asignar permisos, únicamente se creará la autorización.*
  - *SI – Se quieren crear permisos de administrador delegado para el usuario que corresponderán con los valores de los siguientes campos.*
  - *NO – No se quieren crear permisos de administrador delegado para el usuario y no se tendrán en cuenta los valores de los siguientes campos.*

Campos gestión de permiso autorización: Todos estos campos son opcionales y solo se insertaran sin el campo AD.DELEGADO está marcado a SI. El usuario lo rellenará con un SI cuando se le quiera crear el permiso al usuario que contiene la plantilla y NO o vacío si no se le quiere asignar, estos son:

- ***GPA AUTORIZACION BASICA***
- ***GPA USUARIOS***

- ***GPA PERFILES ROLES***
- ***GPA APLICACIONES***
- ***GPA CARGA MASIVA***
- ***GPA BANDEJA ENTRADA***

Campos gestión de permiso usuario: Todos estos campos son opcionales y solo se insertaran sin el campo AD.DELEGADO está marcado a SI. El usuario lo rellenará con un SI cuando se le quiera crear el permiso al usuario que contiene la plantilla y NO o vacío si no se le quiere asignar, estos son:

- ***GPU USUARIO BASICO***
- ***GPU USUARIO AVAZADO***
- ***GPU BANDEJA ENTRADA***
- ***GPU CARGA MASIVA***

- ***ORGANISMO*** *(Opcional):*
    - *SI – Se quieren asignar permisos para uno o varios organismos al usuario. Si son varios, vendrán separados por coma.*
    - *NO – No se quiere asignar permisos para ningún organismo al usuario.*

Ejemplos:

version_1.0	COD APLICACIÓN	DNI/NIE	NOMBRE PROVINCIA	AD.DELEGADO	GPA AUTORIZACION BASICA	GPA USUARIOS	GPA PERFILES ROLES	GPA APLICACIONES
	16	*02256896K*	*Madrid*	SI	SI	SI	SI	SI
	16	*02256896K*		SI	SI	SI	SI	SI
	16	*02256896K*						
	16	*02256896K*	*Madrid*	SI		SI		SI

GPA CARGA	GPA BANDEJA	GPU USUARIO	GPU USUARIO	GPU BANDEJA	GPU CARGA	ORGANISMO

MASIVA	ENTRADA	BASICO	AVANZADO	DE ENTRADA	MASIVA	
SI	SI	SI	SI	SI	SI	*A18002893,LA0006911*
SI	SI	SI	SI		SI	*A18002893*
SI			SI			*A18002893,LA0006911*

Una vez editado el fichero que se quiere cargar, se selecciona y se pulsa el botón “Cargar” para proceder a la carga de los datos.

Se contrasta que la versión empleada en la plantilla es la más actual para la carga masiva de permisos de usuarios.

2.6.6. CONSULTA Y ACTUALIZACIÓN DE USUARIOS EN EL LDAP

2.6.6.1. Actualización masiva de usuarios

Se permitirá a los administradores centrales realizar la actualización masiva de usuarios en Autentica, utilizando un fichero en formato CSV para ello.

El fichero tendrá obligatoriamente como primer campo la versión de la plantilla para la carga. El valor del campo no se debe modificar ni eliminar, no se debe rellenar la columna correspondiente y tendrá el formato version_# . El símbolo # se sustituye en la plantilla descargable por la última versión. Ejemplo: version_1.0

El fichero tendrá obligatoriamente como segundo campo el DNI del usuario, y luego tantos campos como atributos se vayan a actualizar.

Una vez creado el fichero que se quiere cargar, se introduce la descripción, se selecciona el fichero de datos y se pulsa el botón “Cargar” para proceder a la ejecución del proceso. Al pulsar el botón “Cargar” se contrasta que la versión empleada en la plantilla es la más actual para la actualización masiva usuarios y se insertan los datos en la tabla de procesos ejecutados con el estado “En ejecución” y las opciones de descarga deshabilitadas.

Una vez ejecutado el proceso, se modifican los datos del proceso ejecutado habilitándose las opciones de descarga, se actualizan la fecha de ejecución con la fecha de finalización de la ejecución y el estado de la siguiente manera:

- “Finalizado” si ha terminado correctamente y se han actualizado todos los usuarios.
- “Finalizado con errores” si ha habido algún usuario que no se ha podido actualizar.
- “Erróneo” si se ha producido algún error grave que ha impedido el procesamiento del fichero (total o parcialmente).

En la tabla de procesos ejecutados se muestran los enlaces de descarga:

- “Actualizacion.csv”: Fichero de datos cargado.
- “Informe.log”: Informe de ejecución del proceso.

2.6.6.2. Eliminación de usuario en el LDAP

Se permitirá a los administradores centrales realizar la eliminación de un usuario en LDAP.

Cuando el administrador acceda a la eliminación de un usuario en LDAP, se le mostrará un formulario para realizar la búsqueda de usuarios.

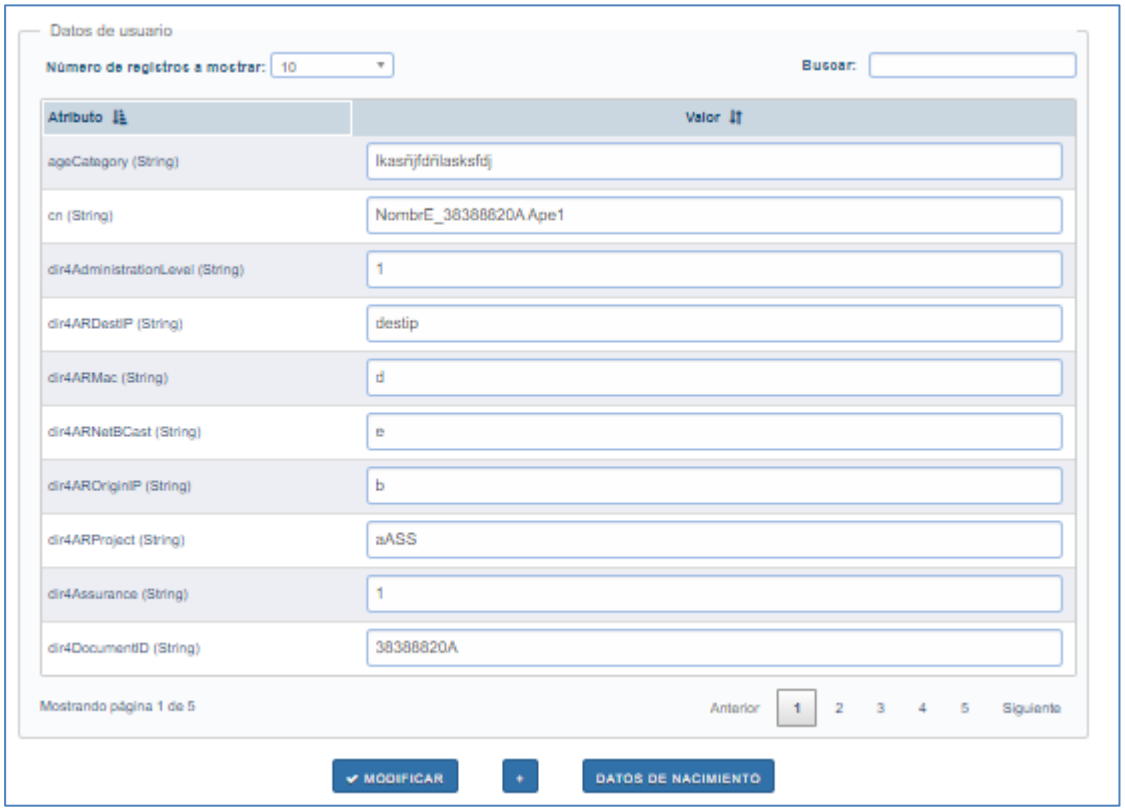
Una vez realizada la búsqueda se mostrará un listado con los usuarios que cumplan las condiciones, al lado izquierdo un botón para consultar un usuario antes de la eliminación y otro para la eliminación del usuario.

2.6.6.3. Actualización directa de usuario en el LDAP

Se permitirá a los administradores centrales consultar y modificar la información del LDAP

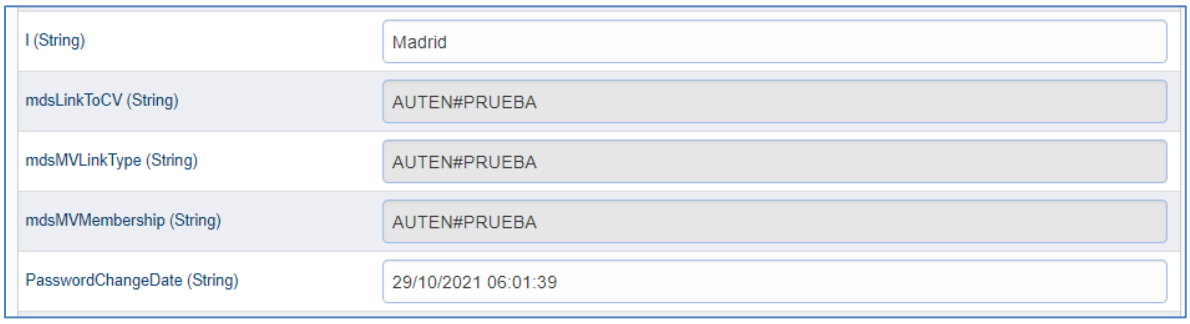
Cuando el administrador acceda a la actualización directa de un usuario en LDAP, se le mostrará un formulario para realizar la búsqueda de usuarios.

Una vez realizada la búsqueda se mostrará un listado con los atributos que tiene el usuario buscado si tiene una sola rama. El administrador podrá modificar los datos encima del campo que quiera modificar,crear nuevos campos en el botón “+” o consultar/modificar los datos de nacimiento.



El administrador podrá modificar los datos de nacimientos desde el botón de dicha opción o desde la propio entrada de datos del atributos; en ambos casos se carga una ventana flotante con una serie de desplegables para la selección del país, comunidad, provincia y localidad de nacimiento.

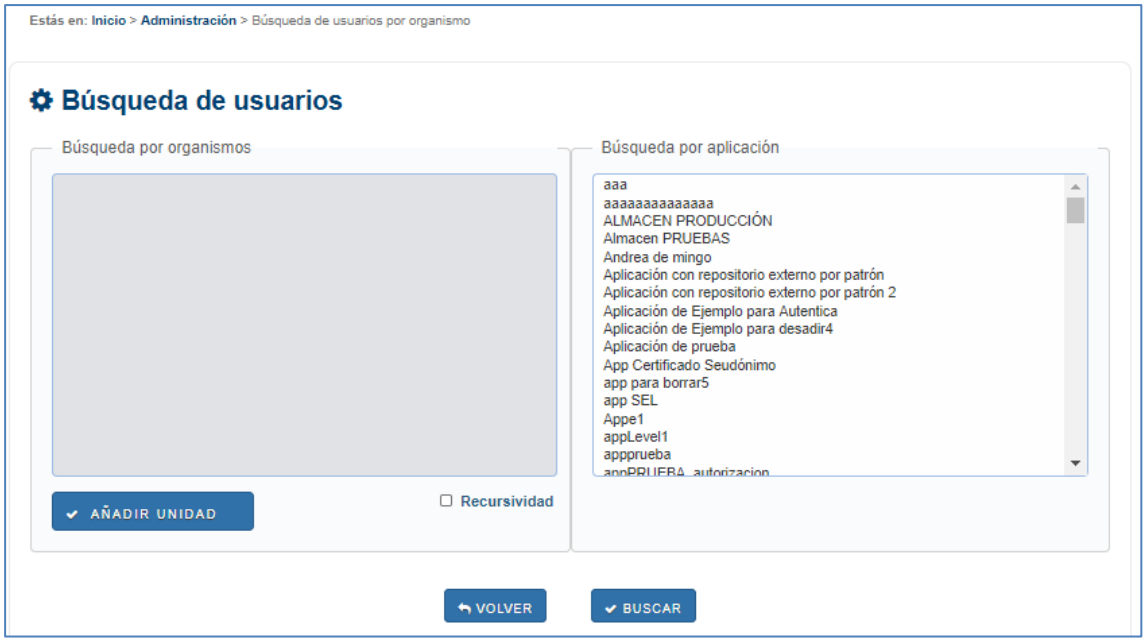
El administrador no podrá modificar los datos mdsMVLink que estarán deshabilitados y dentro de la ventana para añadir nuevos campos no estarán estos campos. Solo se podrá visualizar dichos campos para los usuarios que lo contengan.



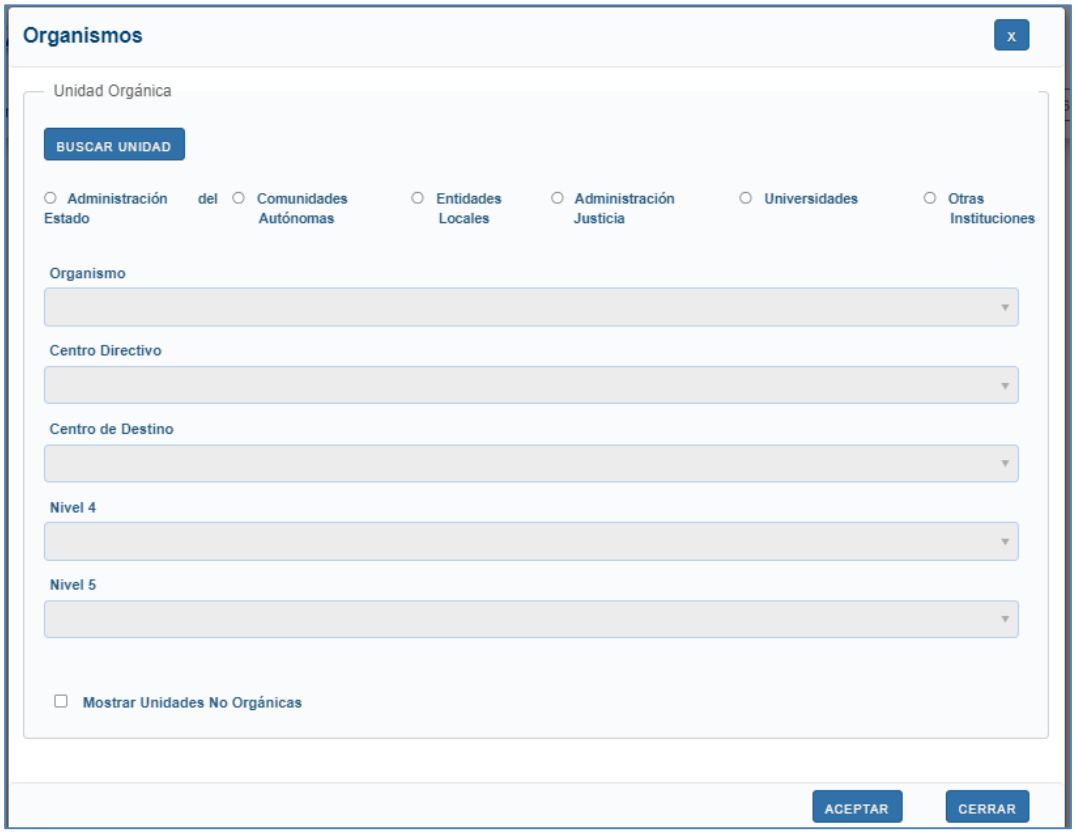
Si el usuario buscado tiene más de una rama se mostrará cada rama en una línea separada, junto a un botón de borrar que permita eliminar al usuario de dicha rama

2.6.7. BÚSQUEDA DE USUARIOS POR ORGANISMO

Se permitirá a los administradores centrales realizar la búsqueda de usuarios por organismo. Cuando el administrador acceda a la pantalla de búsqueda de usuarios por organismo, se le mostrarán los criterios de consulta por organismo y por aplicación. El administrador podrá seleccionar varios organismos, siendo obligatorio seleccionar al menos uno; además podrá seleccionar varias aplicaciones, sin ser obligatorio seleccionar alguna y la recursividad o no sobre los organismos.



En los datos relativos a la unidad orgánica, podrá buscar la unidad mediante el buscador de unidades DIR3. Se muestra los campos de búsqueda: uno para introducir un texto correspondiente al nombre o descripción de la unidad, y otro para introducir el código DIR3.



Una vez aplicados los filtros y realizar la búsqueda, se le mostrará la pantalla de resultado con los datos del usuario y las autorizaciones asociadas. Si se selecciona aplicación en los criterios de búsqueda solo se muestran los usuarios asociados a la aplicación seleccionada.

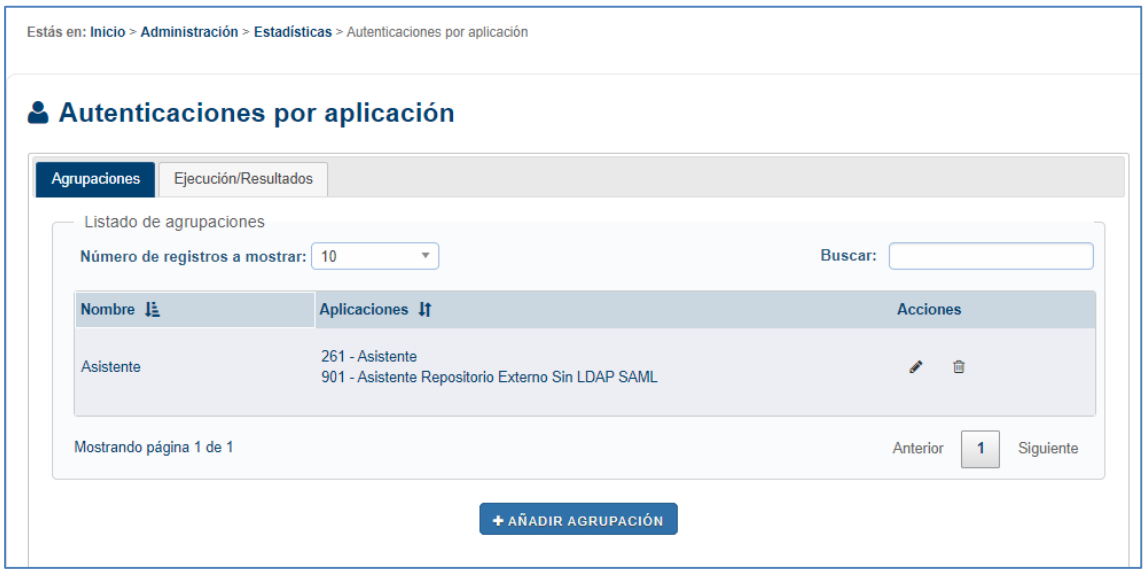
Se permitirá descargar el listado de usuarios resultante de la búsqueda.

2.6.8. ESTADÍSTICAS

2.6.8.1. Autenticaciones por aplicación

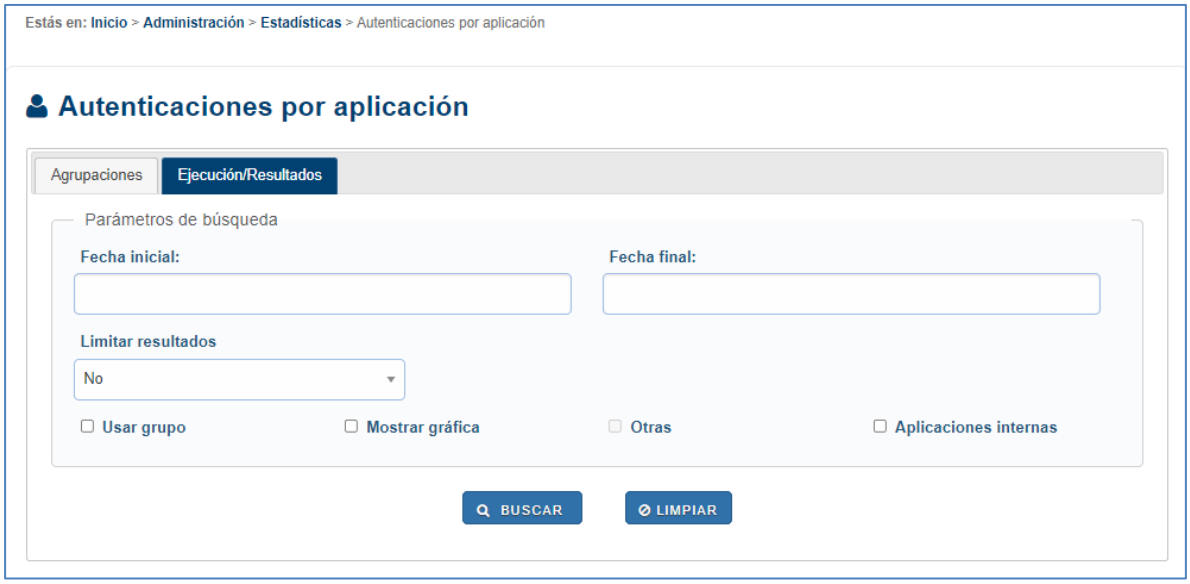
Se permitirá obtener el número de autenticaciones realizadas para cada aplicación durante un período de tiempo determinado. Una vez se acceda a la pantalla de autenticaciones por aplicación se mostrará agrupada en dos pestañas.

En la pestaña "Agrupaciones" se permitirá gestionar la agrupación y las aplicaciones asociadas a las mismas.

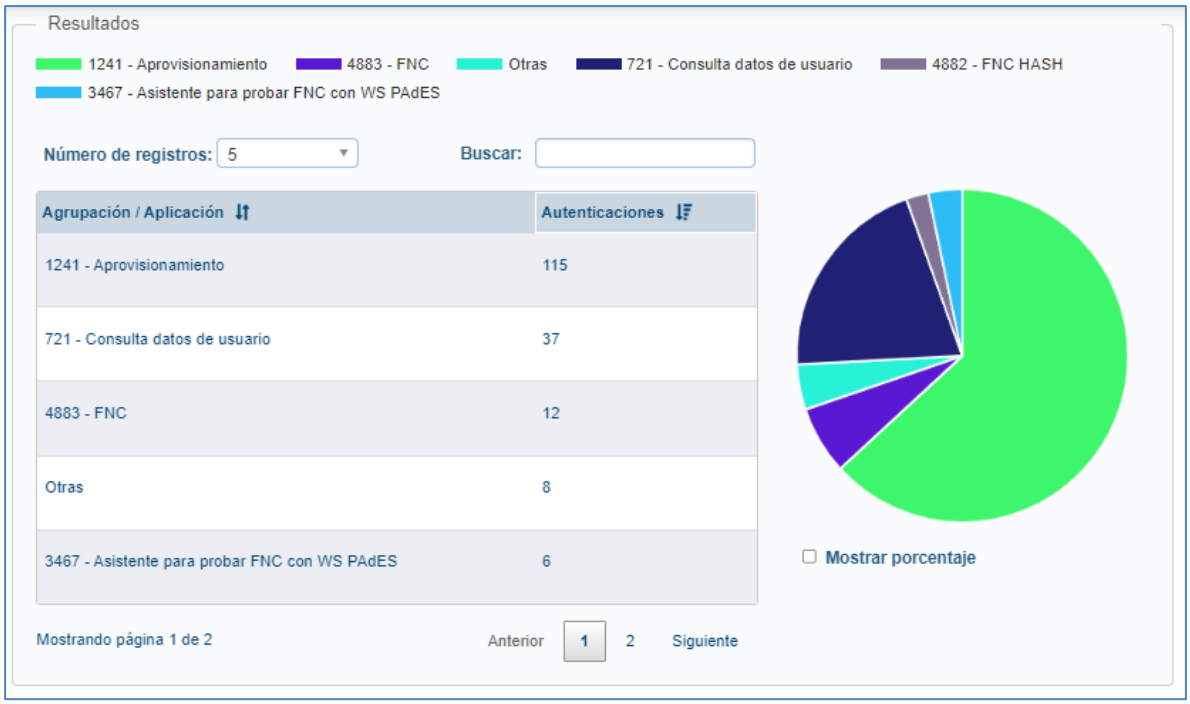


En la cual se permitirá insertar, modificar o eliminar las agrupaciones. El nombre de la agrupación no puede duplicarse y una misma aplicación no podrá estar asociada a más de una agrupación.

En la pestaña "Ejecución/Resultados" se permitirá realizar la búsqueda de autenticaciones en un período determinado.



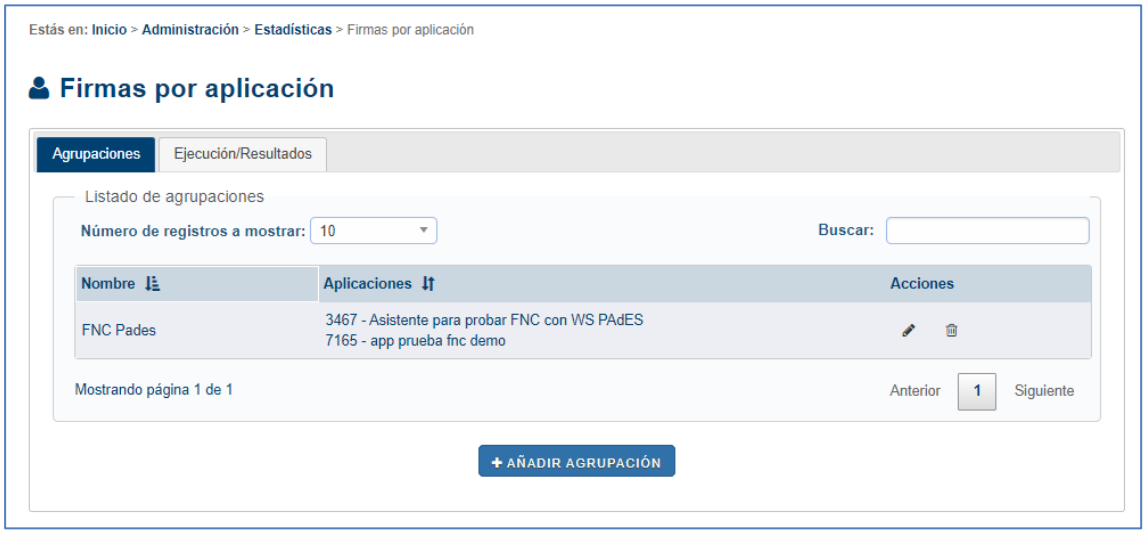
Se podrá limitar los resultados de búsqueda y usar grupos en la misma, para los administradores con permiso sobre aplicaciones internas se permitirá realizar la búsqueda contemplando dichas aplicaciones. La fecha inicial es obligatoria. Una vez se realice la búsqueda según los criterios, se mostrarán los resultados en una tabla. Si se selecciona la opción de mostrar gráfica, se mostrará además una gráfica con los resultados obtenidos. Se permitirá mostrar los porcentajes de la gráfica marcando el check.



2.6.8.2. Firmas por aplicación

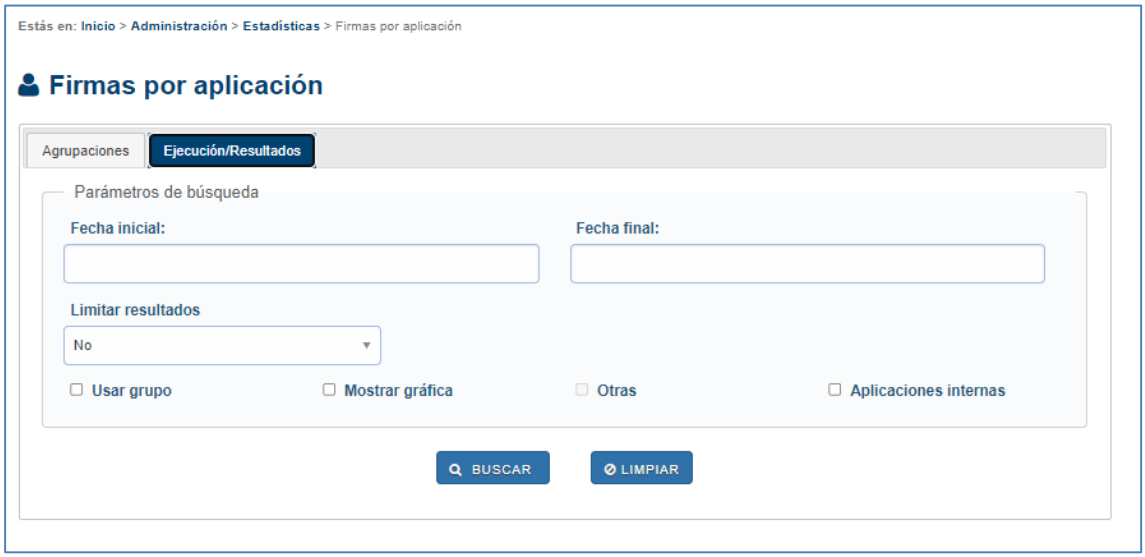
Se permitirá obtener el número de firmas no criptográficas realizadas para cada aplicación durante un período de tiempo determinado. Una vez se acceda a la pantalla de firmas por aplicación se mostrará agrupada en dos pestañas.

En la pestaña “Agrupaciones” se permitirá gestionar la agrupación y las aplicaciones asociadas a las mismas.

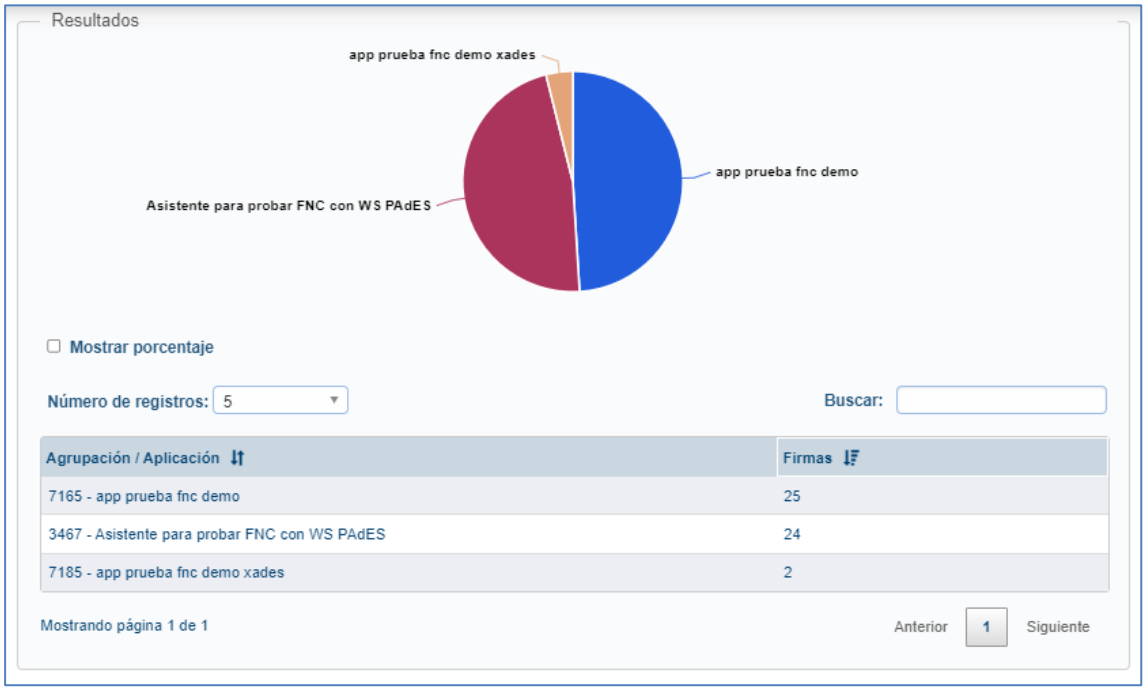


En la cual se permitirá insertar, modificar o eliminar las agrupaciones. El nombre de la agrupación no puede duplicarse y una misma aplicación no podrá estar asociada a más de una agrupación.

En la pestaña “Ejecución/Resultados” se permitirá realizar la búsqueda de firmas en un período determinado.



Se podrá limitar los resultados de búsqueda y usar grupos en la misma, para los administradores con permiso sobre aplicaciones internas se permitirá realizar la búsqueda contemplando dichas aplicaciones. La fecha inicial es obligatoria. Una vez se realice la búsqueda según los criterios, se mostrarán los resultados en una tabla. Si se selecciona la opción de mostrar gráfica, se mostrará además una gráfica con los resultados obtenidos. Se permitirá mostrar los porcentajes de la gráfica marcando el check.



2.7. HERRAMIENTAS

Existen a su disposición una serie de herramientas que le harán la integración aún más sencilla y más integra.

2.7.1. CREACIÓN DE BOTON CERRAR SESIÓN PERSONALIZADO

A la hora de cerrar sesión en Autentica, se necesitará de un botón que elimine cualquier rastro de nuestro certificado y de datos de sesión.

Se ha habilitado una página que genera el botón cerrar sesión siguiendo la estética que se quiera para adaptar al sitio.

Para ello se entrará en la siguiente dirección:

https://autentica.redsara.es/DIR4/servlet/Dir4Servlet?action=customButtonCloseSession

Se abrirá una página como la que vemos arriba. En ella podremos elegir:

- Tamaño del botón
- Color de fondo del botón
- Color del borde del botón
- URL donde se dirigirá después de cerrar la sesión

Cada cambio que se haga se podrá visualizar en el apartado “Vista previa” de la derecha, en tiempo real.

Una vez se elija el diseño del botón, tendremos que copiar el código generado para pegarlo en nuestro sitio.

El código se divide en dos partes, código para insertar en el principio de nuestra página y código para insertar donde se quiera que se vea el botón. Pulsando sobre el botón de los folios, el código se copiara automáticamente.

2.8. MIS DATOS

Se permitirá a todos los administradores poder ver todos sus datos de usuarios: datos personales, unidades orgánicas con todos los niveles definidos, datos profesionales y autorizaciones asignadas.

Estás en: Inicio > Datos de usuario

Datos de usuario

Datos personales

DNI/NIE	09748856F
Nombre	JOSE MANUEL
Apellidos	GUTIERREZ GUTIERREZ
Fecha de nacimiento	27/05/1993
País de nacimiento	España
Comunidad Autónoma de Nacimiento	Comunidad de Madrid

Unidad Orgánica

Organismo	Ministerio de Asuntos Económicos y Transformación Digital
Centro Directivo	Centro Directivo no disponible
Centro de Destino	Centro de Destino no disponible
Centro de Nivel 4	Centro de Nivel 4 no disponible
Centro de Nivel 5	Centro de Nivel 5 no disponible

Datos profesionales

Tipo de Empleado	PERSONAL EXTERNO
Teléfono	633000000
Correo electrónico	yilian.bacallao@externos.correo.gob.es
Datos CIBI	Datos CIBI no disponible
Planta	Planta no disponible
Sala/Despacho	Sala/Despacho no disponible
Puesto físico	Puesto físico no disponible

Autorización asignada

Número de registros a mostrar: 10 Buscar:

Autorizaciones

Aplicación	Ámbito	Perfil	Rol
13	SIN ÁMBITO	ACCESO JAVA	C13_CONSULTA - PROYECTOS
13	Deyá	BENEFICIARIO	ALUMNO
13	Guipúzcoa	BENEFICIARIO	ALUMNO
13	GABPERSONALIZADOUNIDAD1	PPPPPPPPPPPPPPPPPPPPPPPPPP	ExSgTE_NUEVO_ROL_DE_PRUEBA_PARA_ASIGNACION_AUTORIZACIONES_APLICACIONES_HOLA_MUNDO
16	GABPERSONALIZADOUNIDAD	CAID	AA
261	SIN ÁMBITO	ADMINISTRADOR ORGANISMO (REA)	AD
1661	SIN ÁMBITO	TUTORIA	ALUMNO
2481	SIN ÁMBITO	ASESOR JURÍDICO (REA)	ROL POR DEFECTO
3822	SIN ÁMBITO	ADMINISTRADOR GENERAL	ROL POR DEFECTO
4443	PRUEBA	AAAAAAA	AA

Mostrando página 1 de 1 Anterior 1 Siguiente