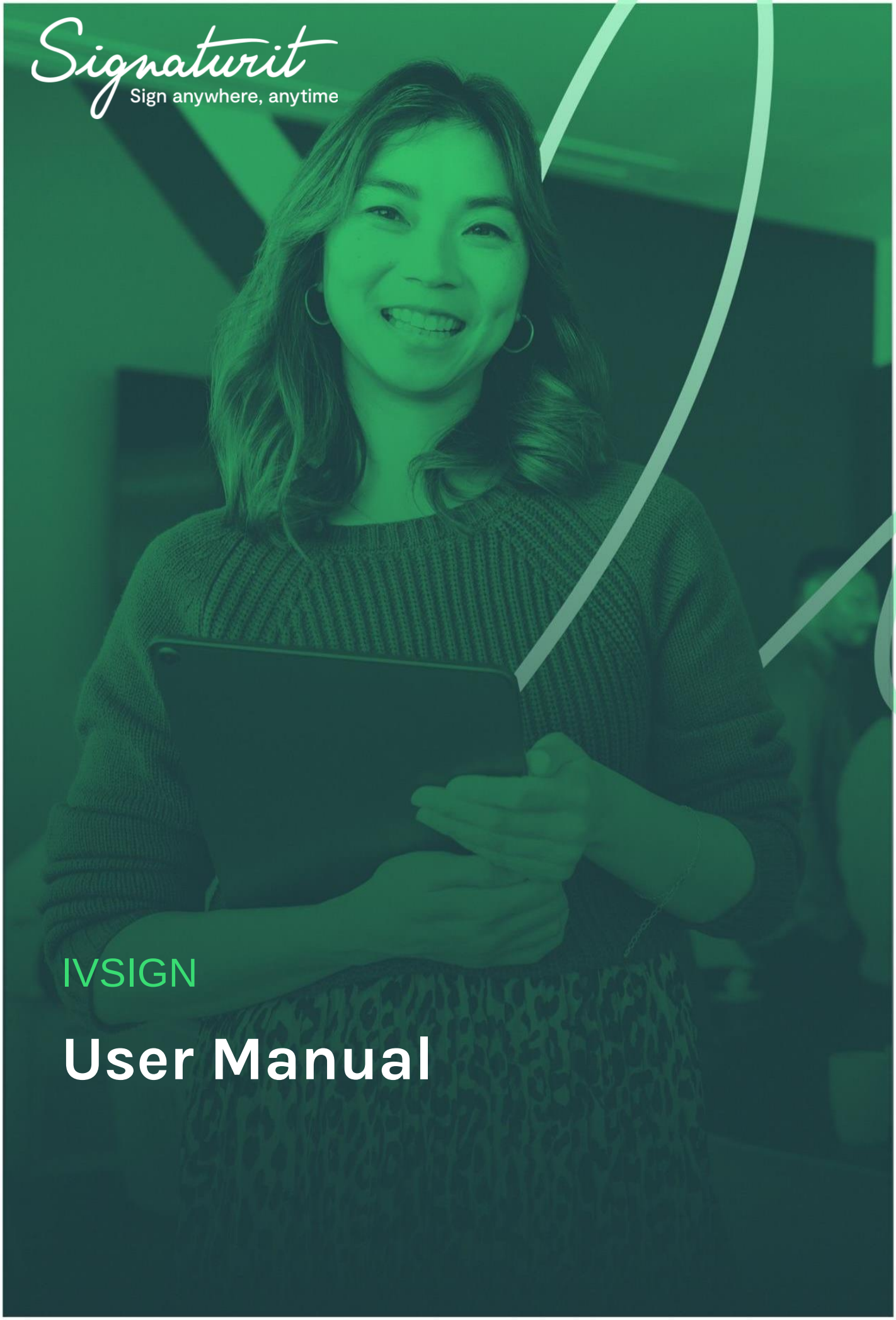
Signaturit
Sign anywhere, anytime



IVSIGN

User Manual

CONTENTS

OPERATING MANUAL

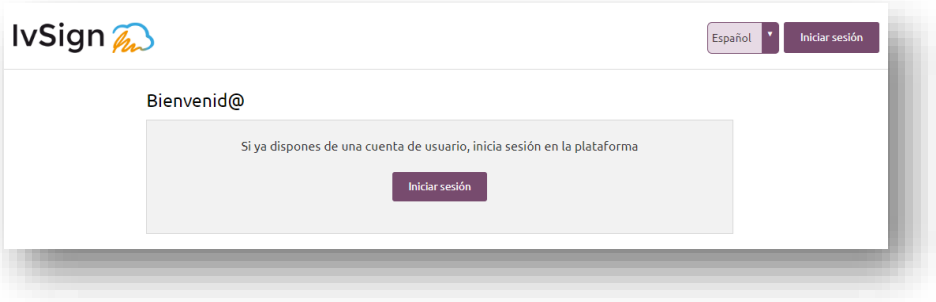
1. ACCESS TO THE PLATFORM

We present the user's manual so that you can solve any doubts that may arise in the organization.

Below are the instructions for accessing the key centralization platform:

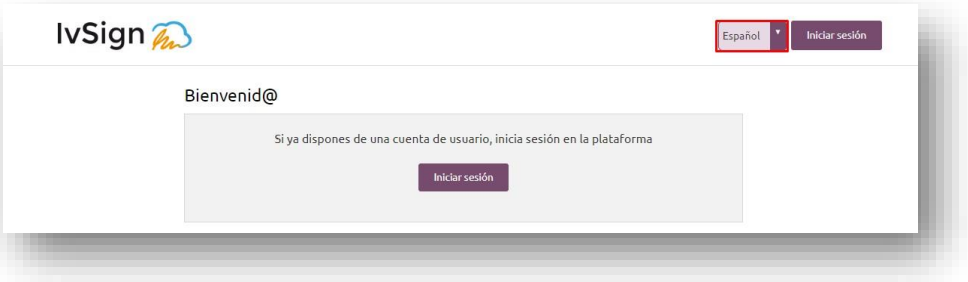
STEP 1. Email sent to the user with credentials and access URL. By accessing this URL, the following page is displayed (Illustration 1):

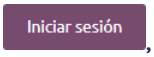
Illustration 1. Welcome IvSign



STEP 2. Select the language in which you wish to navigate the page from the drop-down menu at the top right of the screen (Illustration 2).

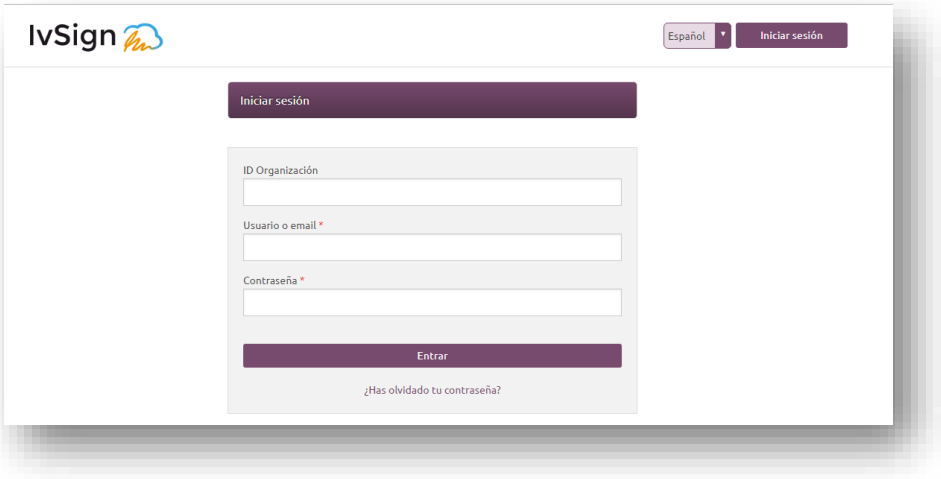
Illustration 2. Language selection



STEP 3. By clicking on any of the two buttons of 

, the form to include the access credentials is displayed (Illustration 3).

Illustration 3. Access credentials



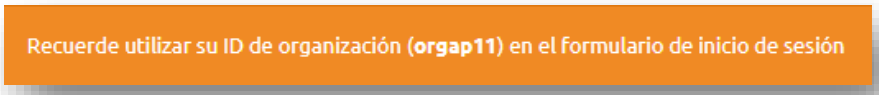
STEP 4. After entering your username or email and password, click Entrar to log in to the platform (Username or Email and Password are required fields).

In the case of any erroneous data, an informative message is displayed.

STEP 5. When accessing the platform, the data of the active session is displayed (user / name / surname / ID / email / organization / date of registration and previous connection).

In the login, the organization's id must be indicated. If it is not entered, a warning appears indicating that the organization's login must be used the next time the platform is accessed (Illustration 4).

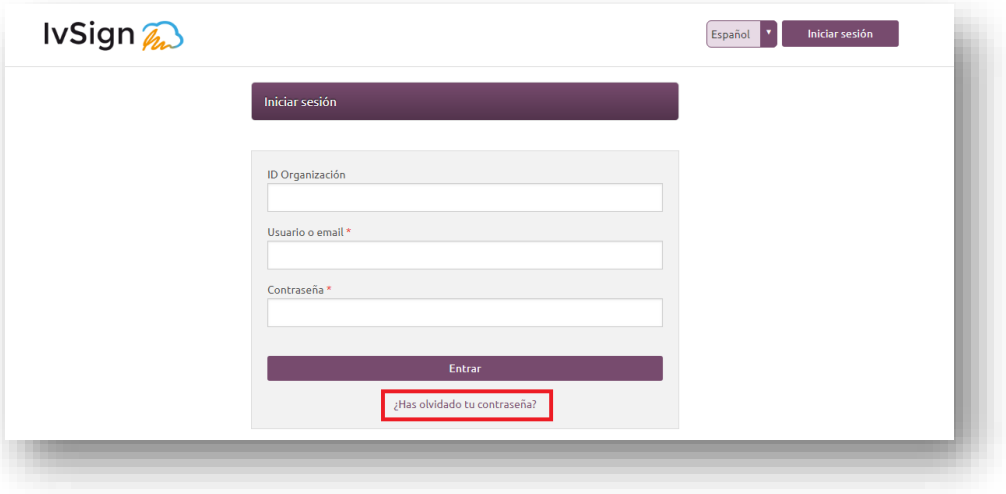
Illustration 4. Warning login



2. HOW TO RECOVER THE PASSWORD?

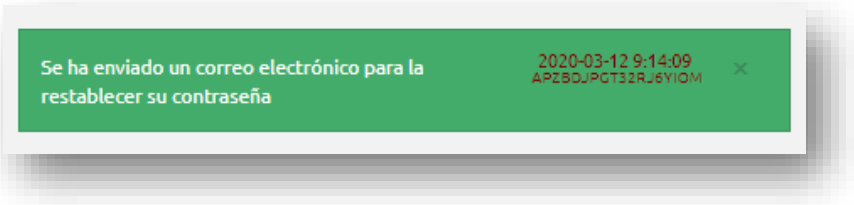
If the user subsequently tries to access IvSign and does not remember his/her password, he/she can request a new password by clicking on **"Forgot your password?"** at the bottom of the login form (Figure 5).

Illustration 5. Password recovery



A form is displayed in which the user or access email must be entered and Continuar must be clicked (Illustration 6).

Illustration 6. New password



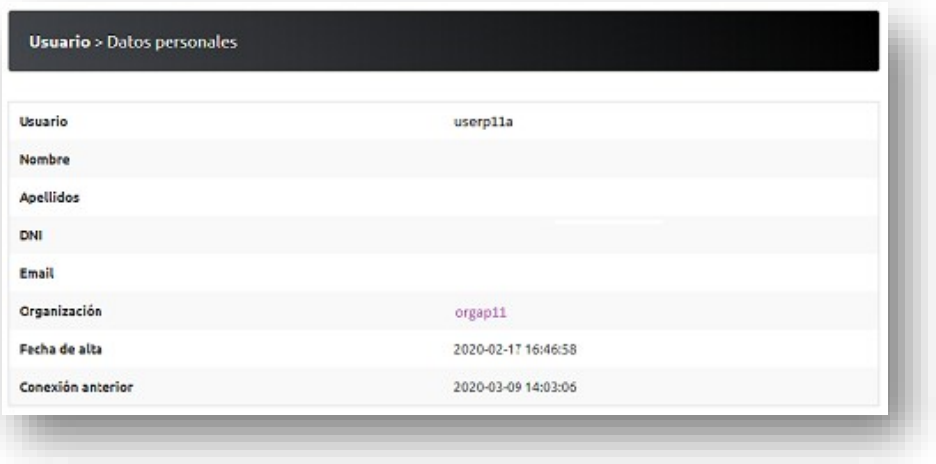
Next, a message is displayed informing that '**A password reset email has been sent**' (Illustration 6).

The user must use the new credentials sent by e-mail to access the platform.

3. USE OF THE KEY CENTRALIZATION PLATFORM

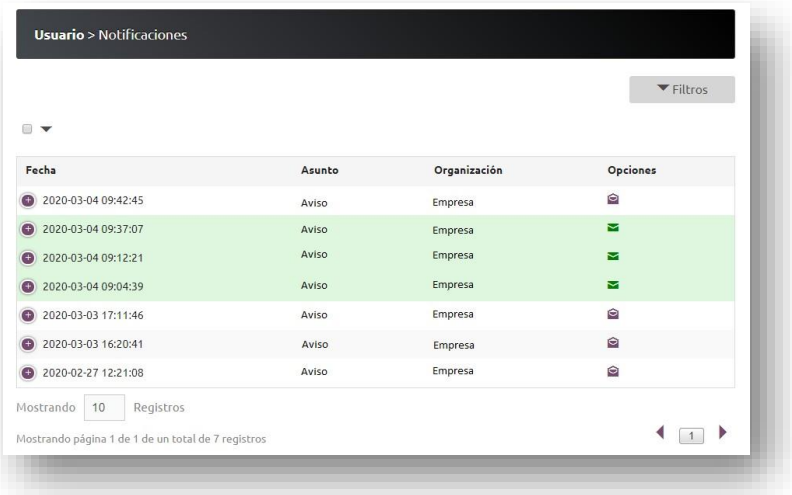
Access to the key platform offers the availability of several menus (on the left side) depending on the permissions that have been set (Figure 7).

Illustration 7. Menus



In the upper right area, by clicking on the icon  you can access the notifications (Illustration 8).

Illustration 8. Notifications



Two types of notifications and/or warnings can be displayed:

- **Notifications with acceptance**: these notifications are displayed directly when accessing the platform, to be accepted before access. In addition, after acceptance, they can also be consulted in the notifications section.
- **Informative notifications**: they are only shown in the notifications section.

Information on each of the notifications, the date of creation, the subject and the status in which it is:

: read.

: not read.

4. USER MENU

By clicking on the **User** menu, the following sections are available (Illustration 9):

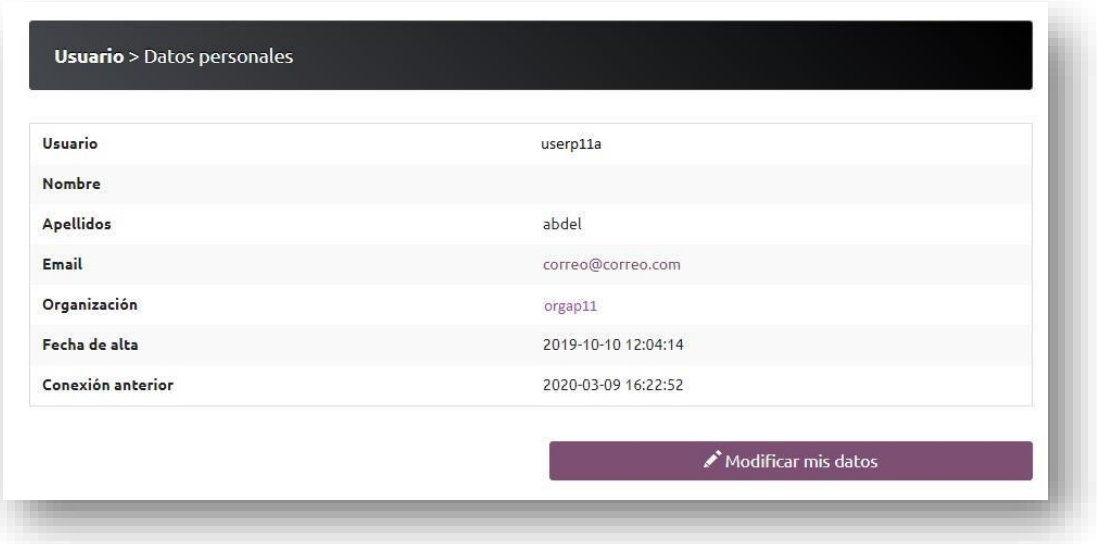
Illustration 9. User Menu

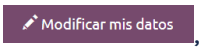
Menu available to all users accessing the IvSign platform, regardless of their permissions.

4.1 USER MENU - PERSONAL DATA

This section shows the basic data of the user account (Figure 10):

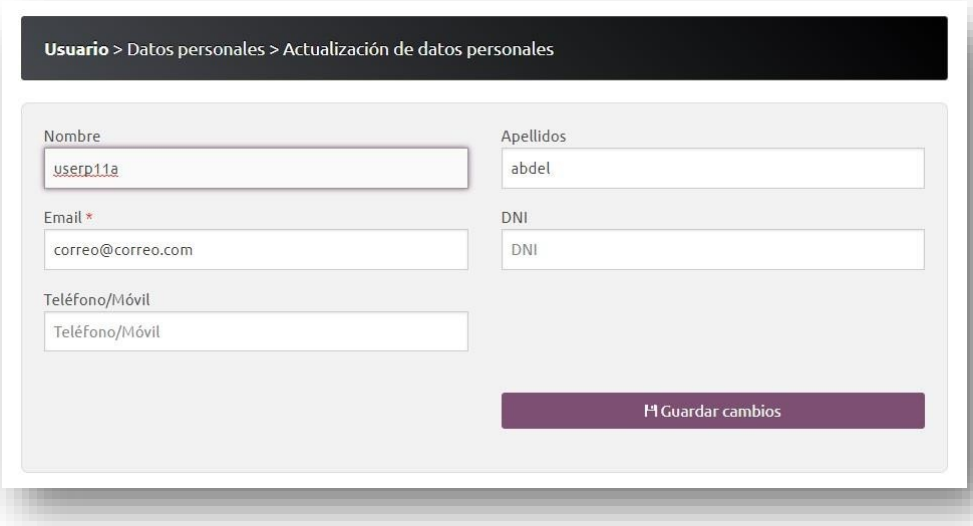
Illustration 10. Personal data



It has available the functionality of 

, which allows you to modify some account data. Only editable fields are shown (Illustration 11).

Illustration 11. Modification of personal data



4.2 USER MENU - CHANGE PASSWORD

This section allows you to modify the platform access password (Illustration 12).

Illustration 12. Change password

First, the current password will be entered. Then, the new password chosen to use will be inserted (indicating it in the "New password" field**,** re-entering it again in the "Repeat password" field**)**. To finish, press Guardar cambios to make the change effective.

The next time the Key Centralization Panel is accessed, this new password will be entered.

Note: In the case of having 'Authentication by User and password' in the Driver KeyController, this new password must be modified in the Configuration section.

4.3 USER MENU - CERTIFICATES

From the certificates menu, access to all functionalities and management tools is offered, as well as detailed information about them. (Illustration 13).

Illustration 13. Certificates

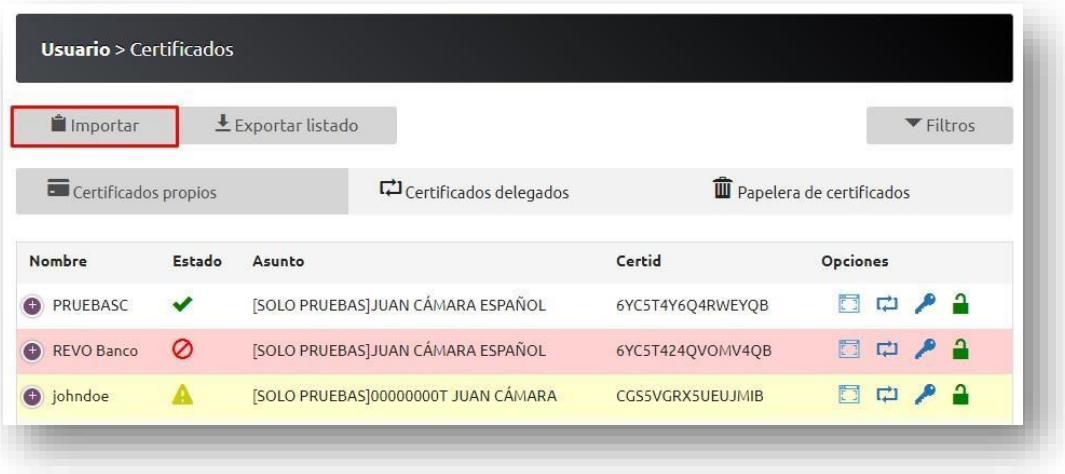
Three Certificate tabs are displayed:

- **Own certificates:** imported certificates are displayed, as well as automatically centralized certificates.
- **Managed certificates:** the certificates managed by the user are displayed.
- **Certificate Trash:** the deleted certificates are displayed, with the option of deleting them permanently or restoring them.

From this menu, the following actions can be performed:

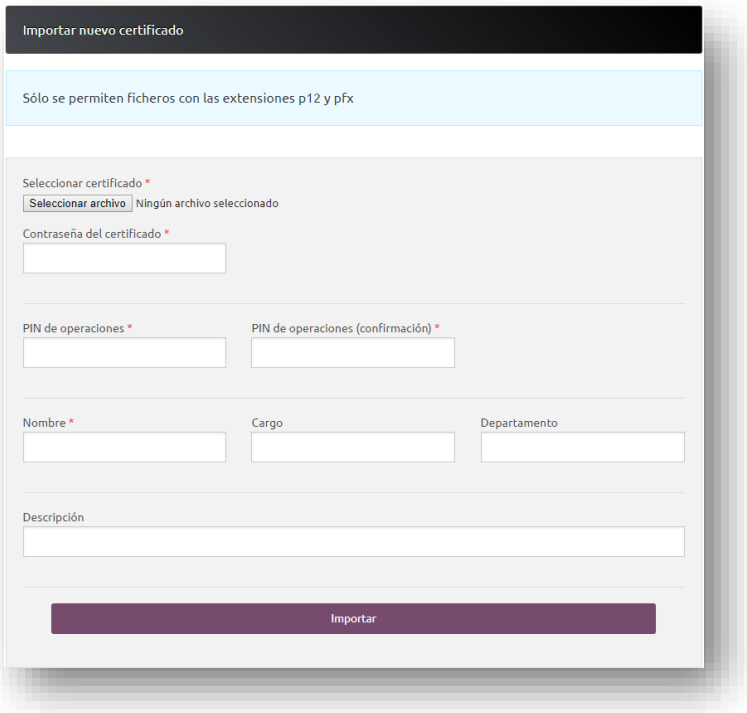
- **Import certificates**: allows you to centralize and store certificates in the panel, provided you have the .p12 or .pfx file of the certificate (Illustration 14).

Illustration 14. Import certificates



The following form is displayed (Illustration 15):

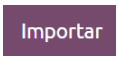
Illustration 15. Import form



Pressing Seleccionar archivo the device navigation windows are displayed to select the certificate file. **Only certificates with extensions can be imported .pfx and .p12.**

The following fields must be entered:

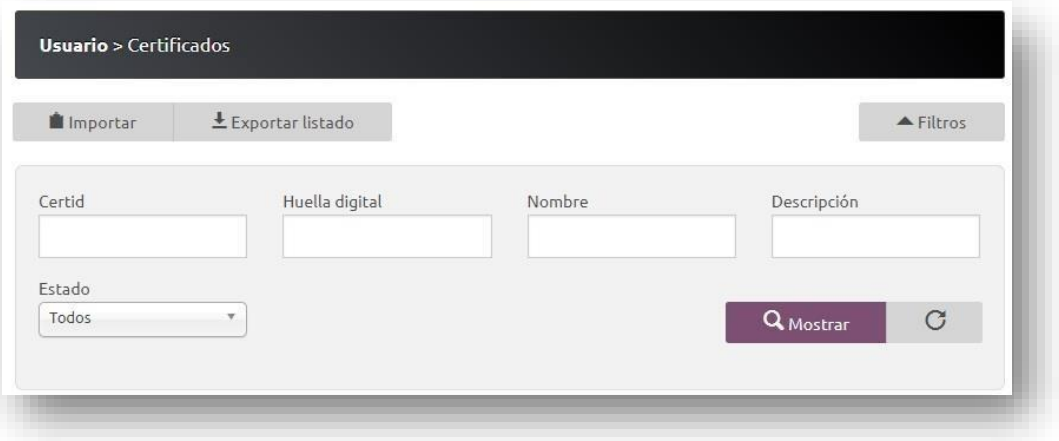
- **Certificate password** is the password issued with the certificate.
- **Operations PIN** is the password assigned to the certificate for its use. The pin must be confirmed in the **Operation pin (confirmation)** field.
- **Name** is the name of the certificate that will be displayed in the panel.
- The fields **Description**, **Title** and **Department** are not mandatory fields, but in case they are filled in, they will be displayed in the certificate information in the panel.

Click 

to complete the import of the certificate, which is then displayed in the **My Certificates** list.

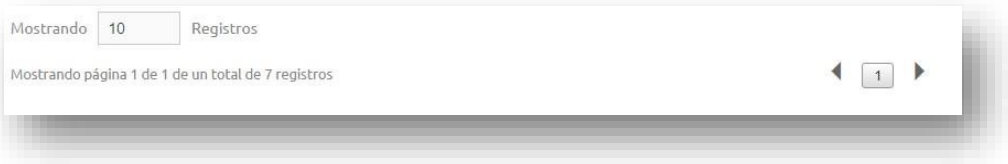
- **Filters**: allows you to filter certificates from any of the fields that appear in the list. Once the desired text data has been entered, click on the **Show** button (Figure 16).

Illustration 16. Certificate filter



- **Pagination**: allows the display of certificates located on different pages when the number of certificates exceeds the number displayed per page (Illustration 17).

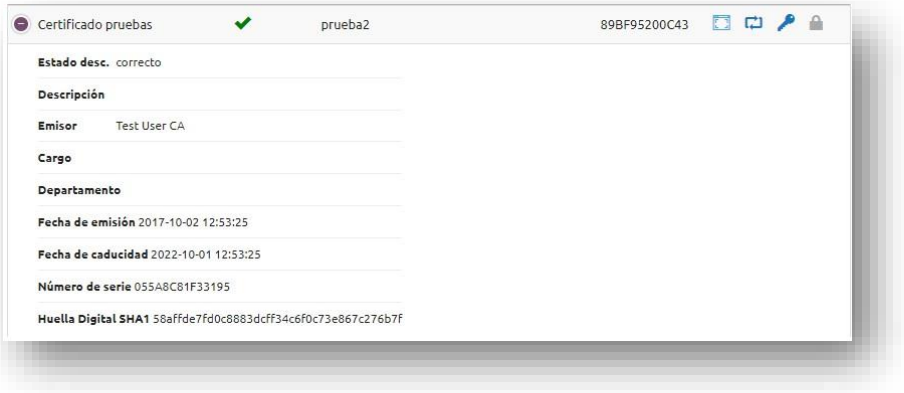
Illustration 17. Pagination



The following actions can be performed with each of the certificates:

- The icon allows you to view all the certificate data that are not directly displayed (Illustration 18). To hide them again, click on the icon .

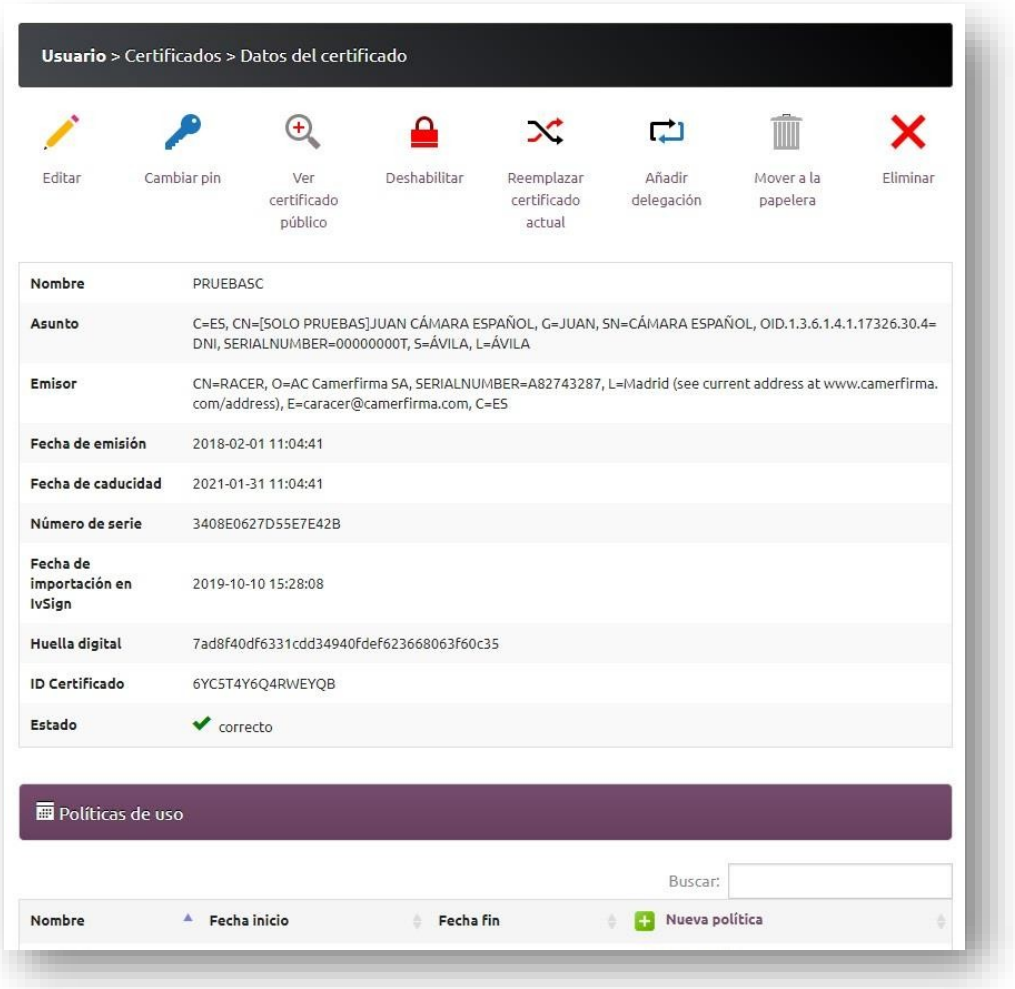
Illustration 18. Certified data



From the icons available in the **Options** column of each list, different actions can be performed (Illustration 19):

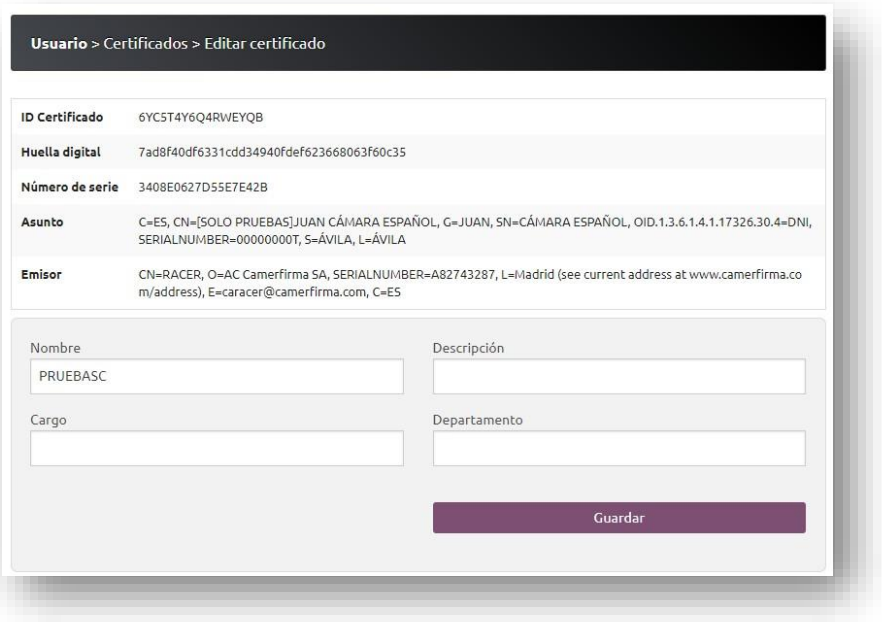
- **Manage certificate**. This section groups or contains all the management operations available on a certificate. (create usage policies, change pin, etc....) (see section How to apply usage policies to certificates).

Illustration 19. Certificate options



- **Edit certificate**. Allows modifying the following fields of the certificate information to be displayed in the panel: Name, Description, Title and Department (Illustration 20).

Illustration 20. Edit certificate



- **See public certificate**. Allows you to download the public key of the certificate (file .crt).

- **Change certificate PIN**. Allows you to modify the operations PIN assigned to the certificate. The current PIN must be entered and the new PIN confirmed in order to change it (Illustration 21).

Illustration 21. Change PIN

- **Add usage controls**. Allows to authorize the use of the certificate to another user of the organization, without losing control over it and limiting its use (see point Controls of use).

- **Replace current certificate**. It allows to replace a certificate by another one, in this section we can select from a list, the certificate by which we want to replace the current one.

- **Disable**. Allows you to temporarily disable the certificate.

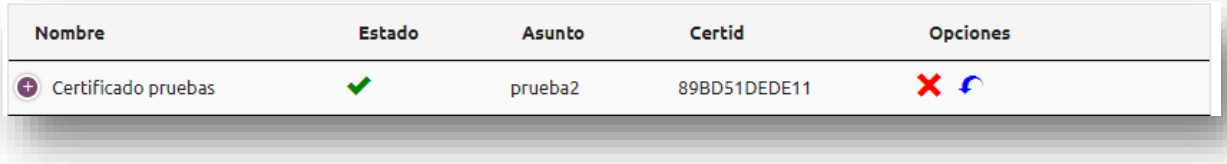
When a certificate is disabled, it will not be displayed to perform actions that require a certificate, such as signing in or logging in to a site.

In the centralization panel, it will still be displayed, but the line will be marked in a different color and the icon will change. To enable the certificate again, you must click on the new icon .

- **Move to trash.** Allows you to remove the certificate from the Own Certificates menu, and move it to the certificate trash, as long as it is not a controlled certificate. If the user has associated controlled certificates, the usage control must be removed first (see point Usage Control).

Once moved to the trash, after confirming the action, we will be able to see the certificates that we have moved to the trash by clicking and the following image will be displayed (Illustration 22):

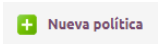
Illustration 22. Garbage can



The icon permanently deletes the certificate from the certificate garbage can. The icon allows you to restore the certificate, both operations require prior confirmation.

- **Delete certificate**. Allows the certificate to be removed from the platform, as long as it has no associated usage controls. In the case of a certificate belonging to another user, the usage control must be removed first (see point Usage control).

- If a certificate that has been automatically centralized (native in the centralization) is permanently deleted, it cannot be recovered.
- If a manually imported certificate is deleted, it can be imported again to keep it centralized.

- 

Create new usage policy. Allows you to restrict the use of each certificate, provided you have the necessary permissions (see section How to apply usage policies to certificates).

The certificate is automatically disabled if the PIN is entered more than 5 times incorrectly. It can be enabled by the user or by the organization's administrator.

4.4 USER MENU - USAGE CONTROLS

Function that allows the certificate holder to determine the uses of his certificate based on different control parameters, and allows the management of the certificate. Additionally, it can be applied to processes where the use of the certificate is required by different people within the same organization, as is the case with electronic seal certificates, setting specific uses and marking limits thanks to the control parameters offered.

Thus, it is possible to parameterize who can use the certificate and when, as well as to restrict its use to certain computers, processes and URLs. To do so, it will be necessary to activate the functionality by associating it with a certificate and adding both usage rules and target users (Illustration 23).

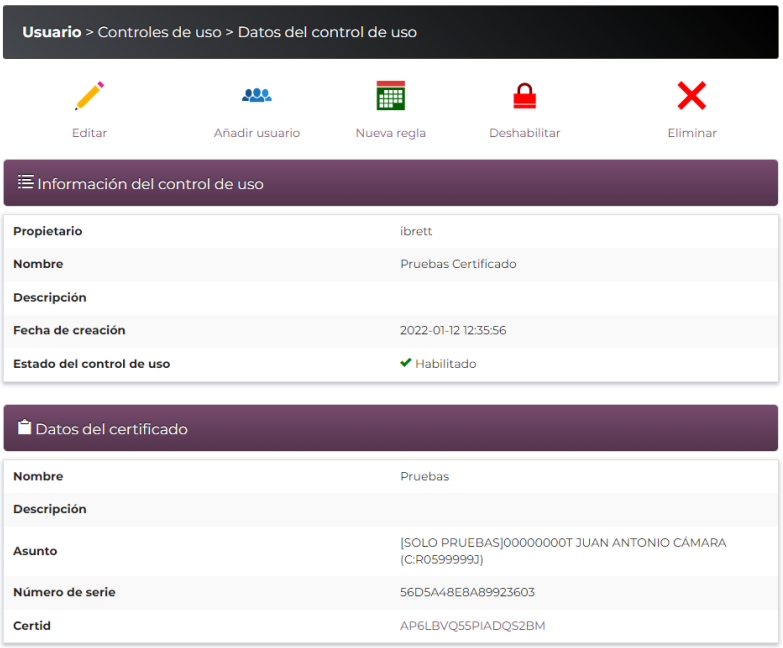
WARNING: the functionality "usage controls" of certificates may pose a risk to the user responsible for the certificate whose use is enabled in favor of another user of the organization. Although the platform offers control measures to reliably protect *ex ante* the electronic signature creation data and its limited use, as well as to control *ex post* the actual uses made by the authorized user (audit of uses), it is the user's responsibility to safeguard his private key and implement appropriate measures to prevent damage to himself and third parties in case of unauthorized use. IVNOSYS is not liable for damages caused by the improper use of the services, both against third parties and the user or, where appropriate, against the entity it represents if they are not duly authorized to do so.

Illustration 23. Usage controls

From the **Filters** field it is possible to search among the usage controls created, by any of the columns available in the list. By entering the desired text and pressing the button Mostrar only the matches will be displayed.
From the icons available in the list next to each usage control, you can:

- **View data of created usage controls**. You can access the basic data of the usage controls, associated users, certificate data and usage rules. In addition, you will be able to add new associated users, create new rules, delete and/or disable usage controls, as well as manage usage rules and associated users. (Illustration 24)

Illustration 24. Data usage controls



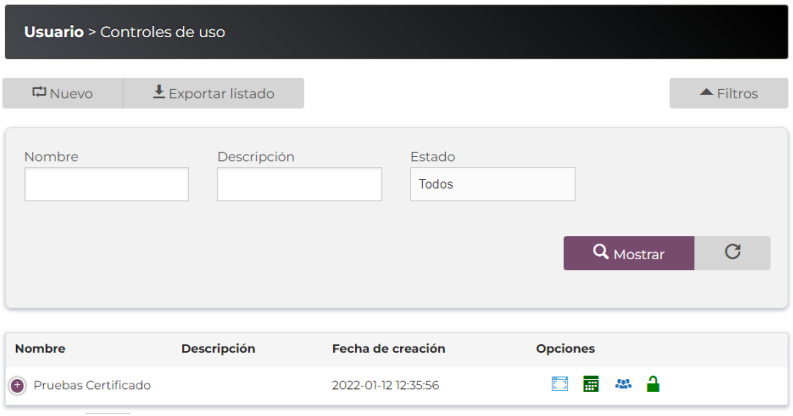
- **Create new usage rule**. Allows direct access to the form for creating a new usage rule, to limit the availability of the certificate (for more information, see point How to activate the usage control of a certificate).
- **Add user**. Allows direct access to the selection screen of users associated to the certificate (for more information, see point How to activate the control of the use of a certificate).
- **Disable usage control**. Allows you to deactivate the usage control temporarily (Illustration 25). This action can also be carried out from the display of the created usage control.

- When a usage control is disabled, the user associated with the assigned usage will

not have it available. To enable authorization again, click on the new icon .

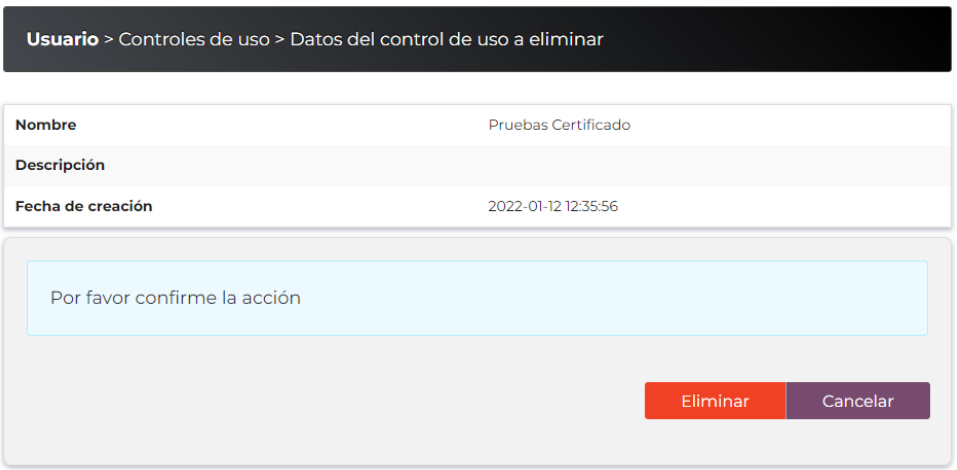
- In the certificate owner's centralization panel it will still be displayed, but it will be marked in a different color and the icon will change.

Illustration 25. Disable usage controls



- **Eliminate usage controls**. Allows you to delete the created usage control (Illustration 26). In case the usage control is associated to users, a message informing about this will be displayed. In case of confirmation, the link with the associated users will be automatically removed.

Illustration 26. Eliminate usage control



4.5 HOW TO ACTIVATE THE CERTIFICATE USAGE CONTROL?

To activate the control of the use of your own certificate to another user or users, you must perform the following steps:

1. Create the usage control.
2. Define the rules of use (optional).
3. Select the users who will use the certificate.

1. Usage control can be **created** from several menus:
   - Menu User> Certificates>clicking the **Manage certificate** button of the certificate and then **Add usage control**.
   - User Menu> Usage Controls, by pressing Nuevo.

In both cases, a window like the following one will be displayed (Figure 27):

Illustration 27. New usage control

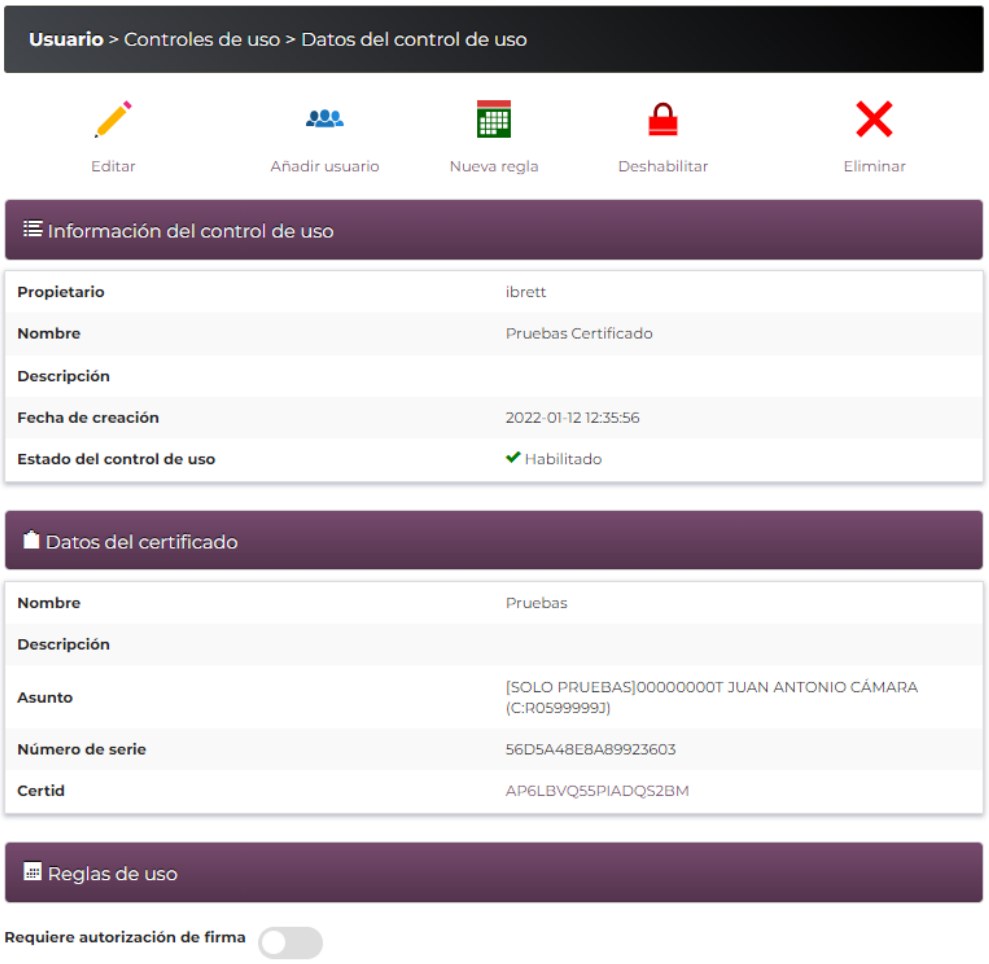
Fill in the name and description of the usage control, select the certificate* *in* question and click **OK**.

*(*The user's certificate list will be displayed. In the case of accessing from the Certificates menu, you will not be asked to select the certificate because it has already been selected previously).*

Once the usage control has been created, its details will be displayed.

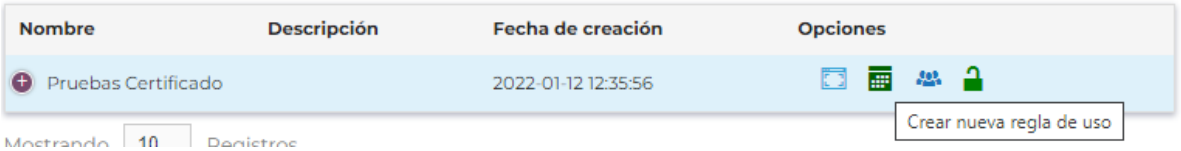
1. To **define the rules of use**, which allow you to limit the use of the certificate to be controlled, you can access from several menus:
   - From the activation detail shown when creating the control, by pressing .
   - When it has been previously created, from the User> Usage Controls menu, click on to display the data of the usage control in question (Figure 28).

Illustration 28. Usage control data



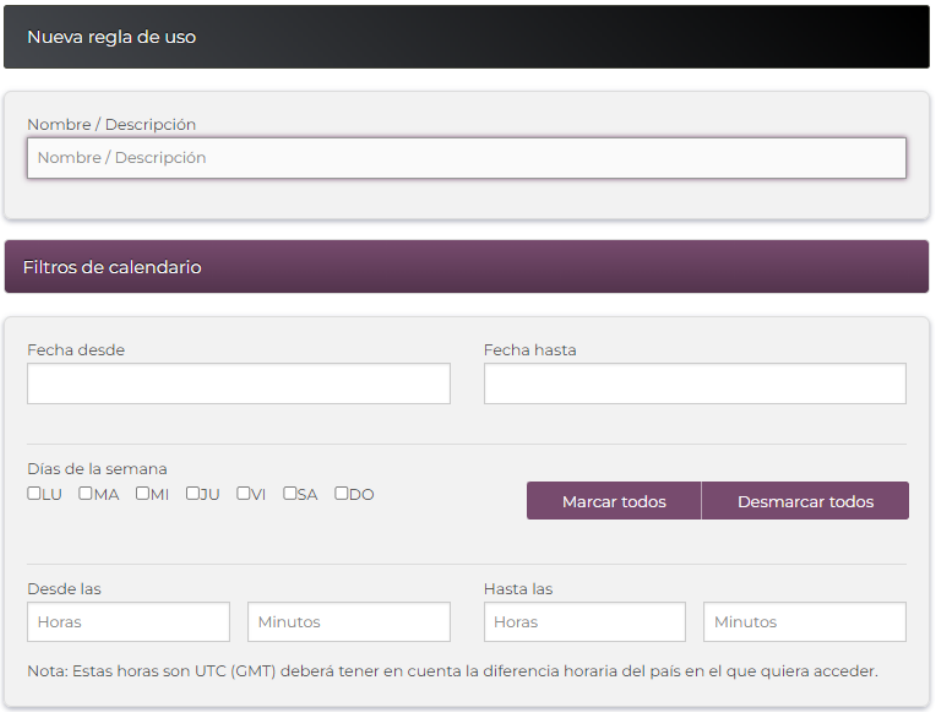
- From the User> Usage Controls menu, click on the Create new usage rule button  (Figure 29).

Illustration 29. Rules of use



In both cases a window like the following one will be displayed (Illustration 30):

Illustration 30. Usage control fields



The form consists of five sections that allow the use of the controlled certificate to be limited. The indicated filters will be cumulative (Illustration 30):

1. **Basic data (New usage rule)**: Name/Description. The name or description of the rule of use must be indicated.
2. **Calendar filters**. Allows you to set different filters to indicate when the certificate can be used.
   - **Date range**. Allows to define the date range in which the controlled certificate can be used.

By clicking on the 'Date from' or 'Date to' field, a calendar is displayed for the selection of start and end dates. *Outside the established range **no** will not be allowed.*

- **Days of the week**. Allows you to define the days of the week on which the certificate can be used.
- You can check/uncheck all the days of the week, from the available buttons, or you can check individual days by clicking directly in the box of the corresponding day.
- **Range of hours**. Allows you to indicate a time of use, choosing the hours and minutes from the drop-down fields. *Outside the established hours **no** use of the certificate will not be allowed.*

3. **Filter by URLs**. Allows you to define the accepted or rejected web addresses that may or may not be accessed with the controlled certificate.

- If the **Accept** option is checked, the URLs indicated will be the only ones that can be accessed with the certificate.
- If the **Reject** option is checked, all URLs will be accessible with the certificate, except those indicated.

In both cases the configuration "https://" must be used.

Once the URL address has been added, if you wish to add more, click on  . You can add as many URLs as you need, and they will be displayed as a list.

You can edit the content of the entered lines by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon  .

4. **Process filter**. Allows you to define which applications are accepted or rejected for use with the controlled certificate.
    - If the **Accepted** option is checked, the indicated applications will be the only ones that can be accessed with the certificate.
    - If the **Rejected** option is checked, the certificate will allow access to all applications except those listed above.

Some considerations to take into account:

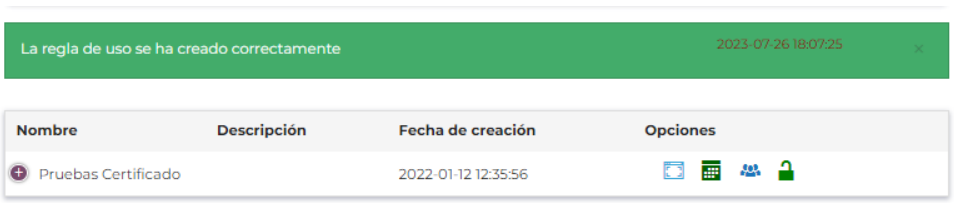
- To know the exact name of the process, access the 'Processes' tab. located in the 'Task Manager'.
- Once the name of the application has been added, if you wish to add more, click on the icon .
- You can add as many as you need, and they will be displayed as a list.
- You can edit the content of the entered lines by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon directly.

5. **Filter by equipment**. Allows you to define the computers from which the controlled certificate can be used.

- To know the complete name of the equipment access the properties of 'My Computer'.
- Added the name of the equipment, if you wish to add more, click on .
- You can add as many as you need and they will be displayed as a list.
- You can edit the content of the entered lines by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon directly.

Once the desired sections have been completed, click on **OK** to create the usage rule and it will be listed in the detail of the generated usage control (Illustration 31):

Illustration 31. Detail of usage control

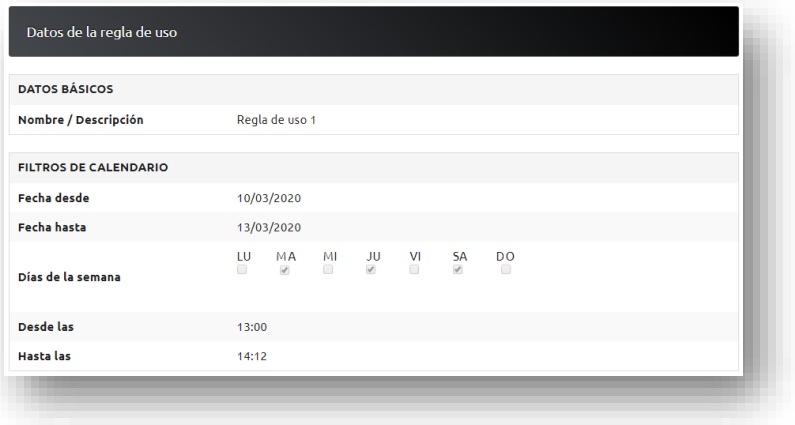


From the icons available next to each usage rule, different actions can be performed (Illustration 32):

Illustration 32. Actions rules of use

- See details of the rule of use. Displays the data entered in the form for creating the usage rule (Illustration 33).

Illustration 33. Usage rule data



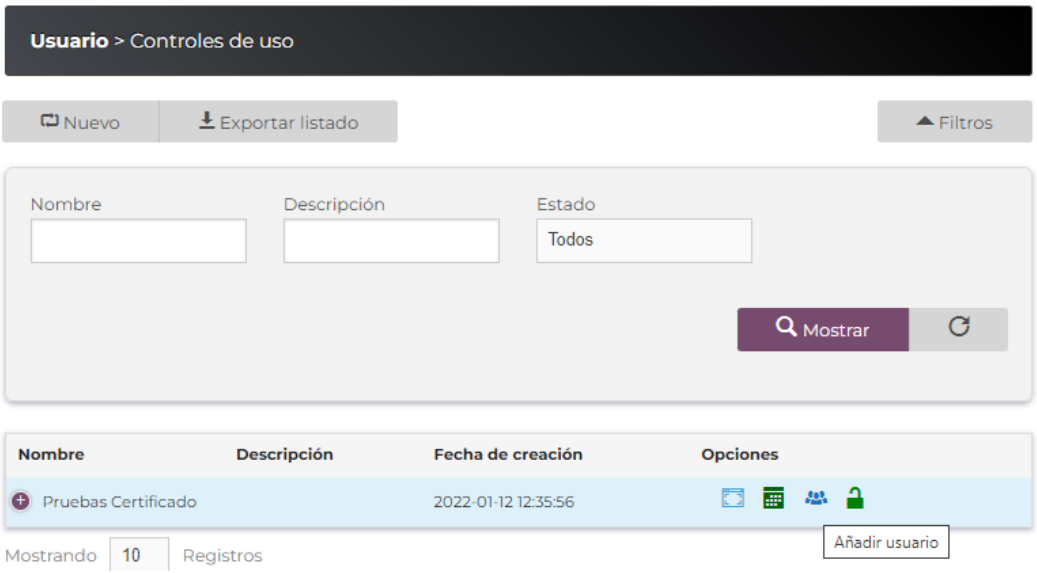
- **Modify usage rule.** Allows you to modify all the data entered in the form for creating the usage rule.

- **Eliminate usage rule.** Allows you to delete the created usage rule.

To **select the users** that will make use of the controlled certificate, you can proceed in two ways, depending on whether the usage control is being created at the same time as the users are added or depending on whether the control was already created:

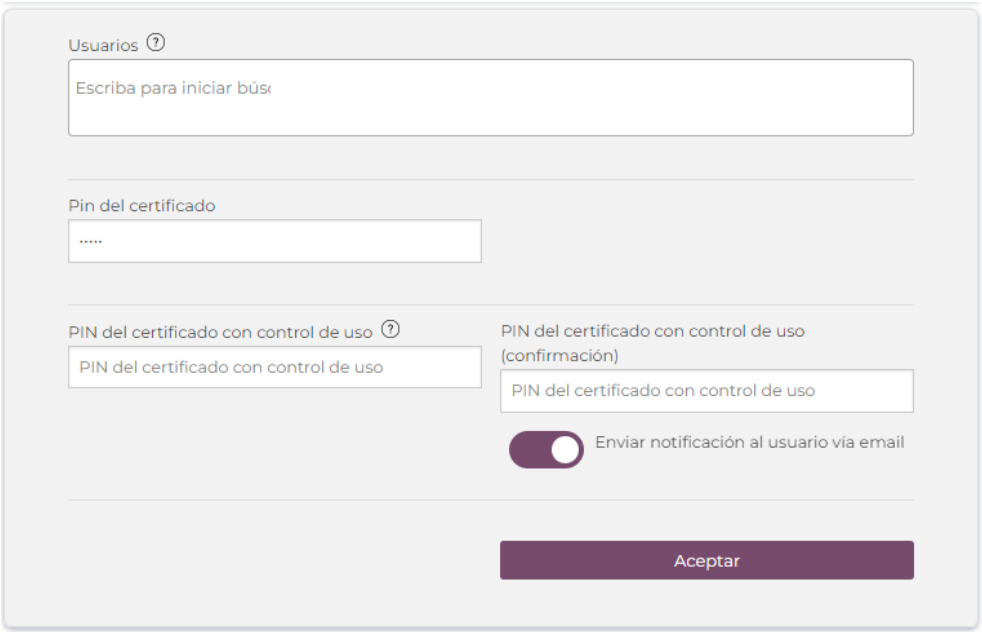
- From the detail of the usage control shown when creating it, by clicking Añadir usuario.
- From the User> Usage Controls menu, by pressing (Figure 34).

Illustration 34. Usage Controls - User Menu



In both cases, a window like the following one will be displayed (Figure 35):

Illustration 35. New user

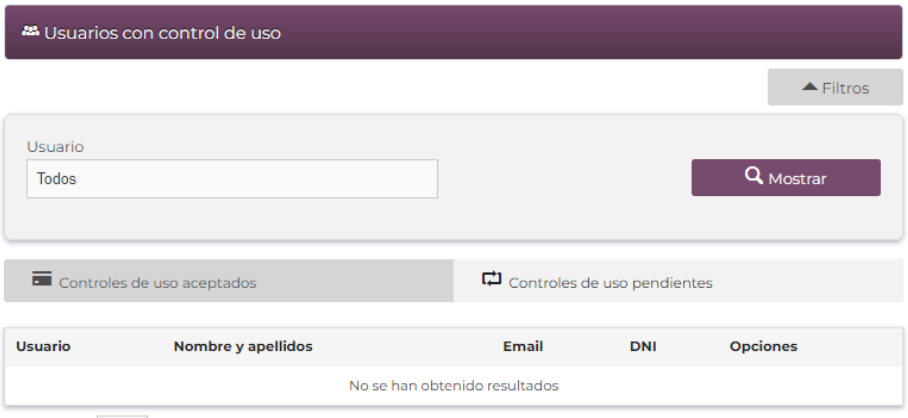

Usuarios
Escriba para iniciar búsc
Pin del certificado
.....
PIN del certificado con control de uso
PIN del certificado con control de uso
PIN del certificado con control de uso (confirmación)
PIN del certificado con control de uso
Enviar notificación al usuario vía email
Aceptar

The following fields must be filled in:

- **Users of the organization**. By clicking on the field, the list of all users in the organization will be displayed. To filter, you can type all or part of the user's name and only users that match the text entered will be displayed. You can select as many users as you wish by clicking on the name of each one of them. You can select multiple users by pressing the (ctrl) key and clicking on the list of users.
- **Certificate PIN**. The current operating PIN of the certificate must be indicated.
- **Controlled certificate PIN**. Allows to indicate a different PIN for operations, to be used by the recipients of the certificate, and not to use the holder's personal PIN.
- **Pin of the controlled certificate (confirmation)**. The pin of the controlled certificate to be used by the recipients of the certificate will be repeated again.
- **Send notification to user via email**: if this option is checked, an email will be sent to the user who has been assigned control of the certificate, informing of the controlled certificate and the controlled use pin. If you do not wish to inform the recipient by this means, the option should be unchecked.

Finally, click **OK** and the users will be listed in the usage control detail (Figure 36).

Illustration 36. Assigned users



If you access the usage control data by clicking on the icon in the list, you can remove the linkage of the assigned users, and they will no longer have access to the certificate.

We will also find in this section the option to disable and enable this user from the usage control, we will be able to do it from the icon .

4.6 USER MENU - REPORTS

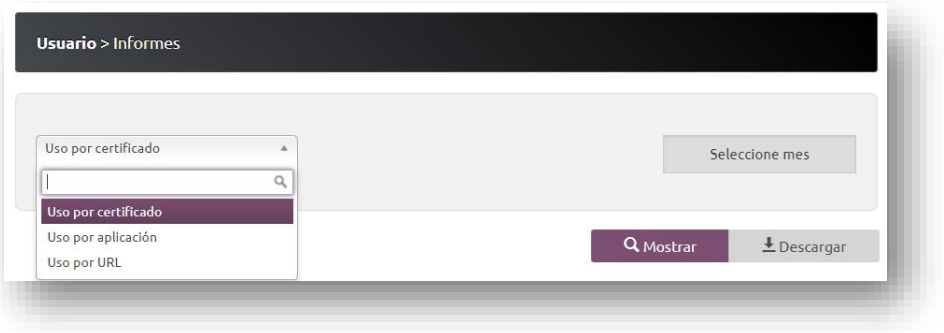
Allows to consult, in a differentiated way, the information related to signatures and authentications on the web with centralized certificates, performed by:

- The user/owner(Own*use*).
- Those performed by the user with certificates enabled by the user/owner*(Controlled Use*).

- Those carried out by other users with the certificates that the user/owner has enabled the controlled use *(External use)*.

The reports will be displayed in list format and graphically, according to the selected filters. There are two types of filters (Figure 38):

Illustration 34. Filter reports



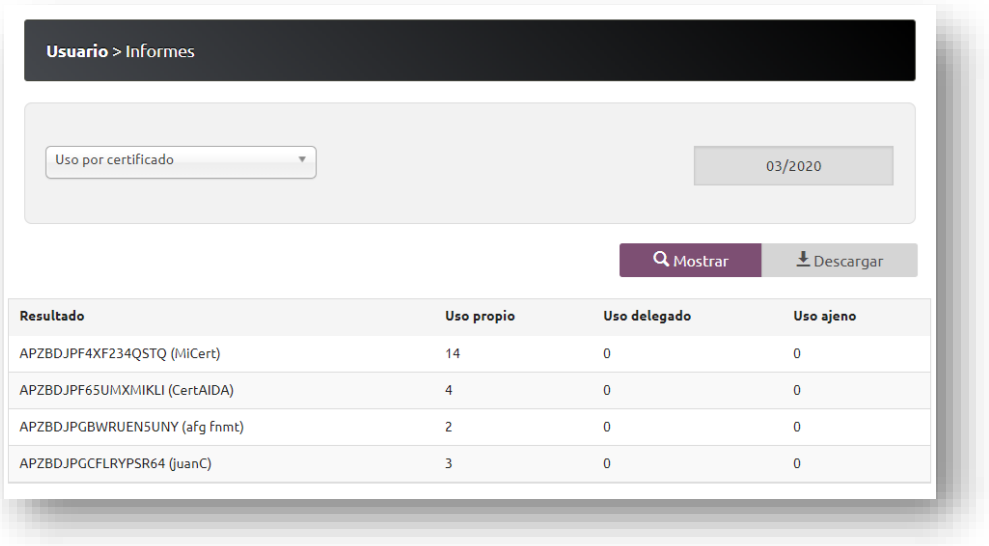
1. Filters by type of use. Select the filter to apply from the drop-down menu:
   - **Use by certificate**. The results are shown grouped by certificate.
   - **Use per application**. The results are shown grouped by the application that has made use of the certificate.
   - **Usage by URL**. The results are shown grouped by the url accessed with the certificates.

2. Filter by date. Select the month for which you wish to consult your usage. Once the desired filters have been selected, click on Mostrar to display the result of the filters applied and Descargar to obtain a *.csv* file of the result.

The results will be differentiated in (Illustration 39):

- Own use: uses carried out by the user/owner himself/herself, with his/her certificates.
- Third-party use: uses carried out by a third party, with the certificates that the user/owner has enabled the controlled use.
- Controlled use: uses made by the user with certificates that have been enabled by another user/holder.

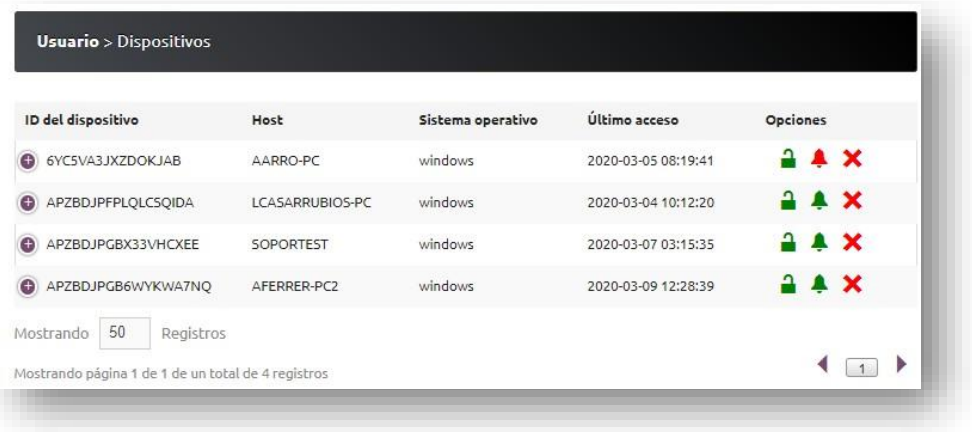
Illustration 35. Reports



4.7 USER MENU - DEVICES

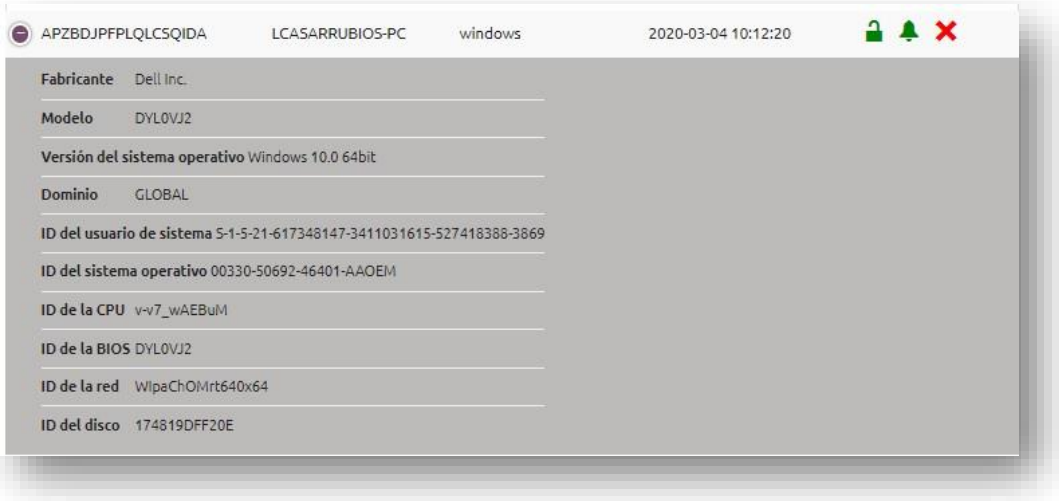
In this section we can see information related to the host, the device ID, the type of operating system the user is connected to, the last access and some options such as disabling or authorizing the device, disabling or enabling notifications and the option to delete the device from the list (Illustration 40):

Illustration 40. Devices.



If we click on the ⊕ tab we can see more information about each device that has been connected (Figure 41).

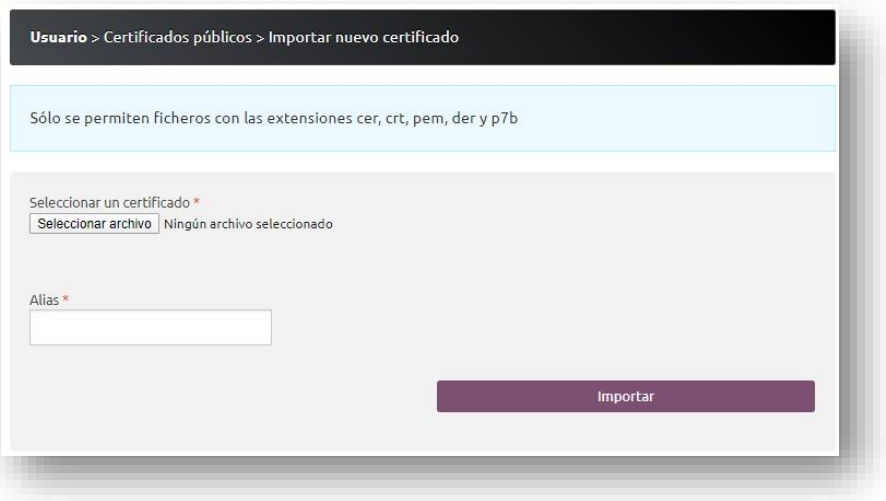
Illustration 41. Device Information.



4.8 USER MENU - PUBLIC CERTIFICATES

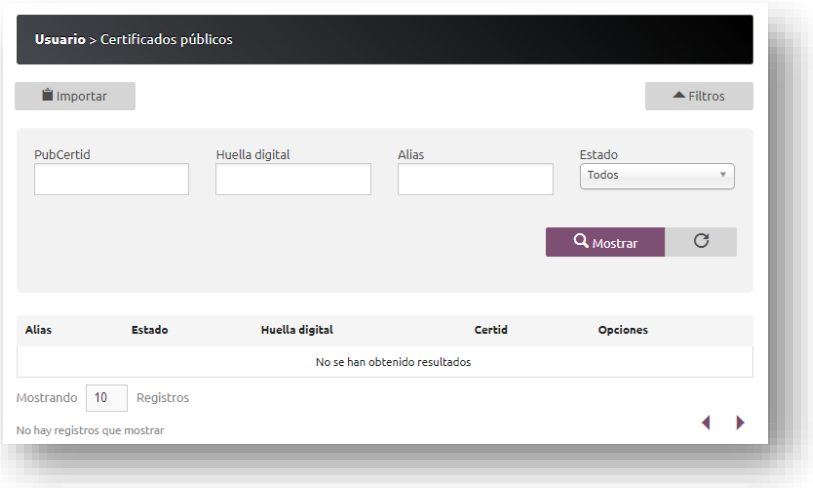
Allows importing a public certificate to the platform, only certificates with the extensions cer, crt, pem, der and p7b can be imported. Once the certificate has been added, we will be asked to create an alias (Illustration 42).

Illustration 42. Import public certificates.



The **Filters** button displays the fields by which we can filter these public certificates, such as PubCertid, fingerprint, alias and their status *(Illustration 43)*.

Illustration 43. Public certificate filtering.



4.9 USER MENU - AUDIT

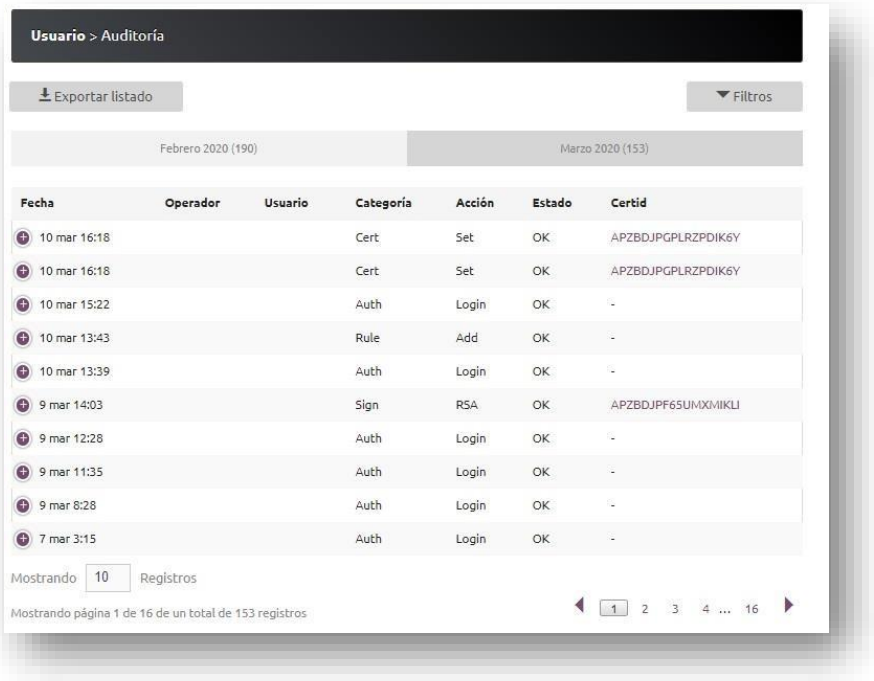
Allows to visualize all the actions differentiated by type performed with the user's centralized certificates.

NOTE: The actions of certificates that the user has installed on his own computer will not be displayed, only the actions performed with the centralized certificates.

In case of having the certificate installed in the equipment itself and also centralized in IvSign, the system itself will recover the key that you have locally, since the Serial Number and Fingerprint of the certificate are the same, so it is NOT recommended to have the certificate installed.

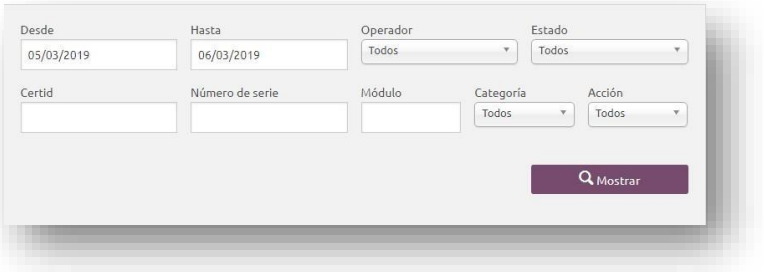
By default the last 5 days are shown, but it is possible to filter by a different date range. After indicating the date range, click Mostrar to display the result of the applied filters on the screen, and Exportar listado to obtain a file, in .xml format, of the result (Illustration 44).

Illustration 44. Audit



The **Filters** button displays more fields by which the audit information can be searched: certificate name, serial number, category, action and status (Figure 45).

Illustration 45. Audit filters



The icon allows you to view more information on each of the audited actions. To hide them again, click on the icon .

The actions to be audited are:

- Category: **Auth**. Related to the identification and access to the panel.
- Shares:
  - Login: user access to the panel.
  - LoginToken: access of an application to the panel.
  - Impersonate: user impersonation (seeUsers).
- Category: **User**. Related to user management.
  - Shares:
    - Add: user creation.
    - Set: user modification.
    - Del: user deletion.
    - Ren: User renaming.
    - OrgaMove: Move user from one organization to another.
- Category: **Cert.** Related to certificate management.
  - Shares:
    - Set: modification of the certificate (status, change of name or description...)
    - Del: Definitively deletes a certificate.
    - Move: Move a certificate to the trash can.
    - PinCheck: Checks the certificate pin.
    - PinSet: Change of certificate pin.
    - ImportPFX: import certificate.
    - Generate (GenRSA, GenCSR, InstallCER): certificate generation.
    - Reflink: related external certificate (pkcs11).
    - Replace: Replaces a certificate with another certificate.
- Category: **Deleg** (usage controls).

- Shares:
    - Add: creation of usage control.
    - Set: modification of usage control.
    - Del: deletion of usage control.
    - AddCert: certificate is added to the usage control.
    - DelCert: Deletes a certificate from a usage control.
    - UserAdd: Add user to the usage control.
    - UserDel: Remove user from usage control.

- Category: **Rule** (rules of use)
    - Shares:
        - Add: creation of usage rule.
        - Del: deletion of usage rule.
- Category: **Sign** (signature).
    - Shares:
        - RSA: web authentication and document signing.
- Category: **Notify** ().
    - Shares:
        - Accept: Notifications that have been accepted.
        - Set: Notifications marked as read.
- Category: **Orga** ().
    - Shares:
        - Add: Organizations that have been added.
        - From: Organizations that have been eliminated
        - Ren: Organizations that have been renamed
        - Set: Modification of the description field.
- Category: **Rule** ().
    - Shares:
        - Add: Add a usage rule to a usage control or certificate.
        - Del: Delete a usage rule to a usage control or certificate.
- Category: **Signature** ().
    - Shares:
        - Cades: CMS (Cryptographic message syntax) document signature.
        - Pades: Signature of PDF documents (PDF advanced electronic signature).
        - Xades: XML advanced electronic signature (XML advanced electronic signature).
        - TimestampPDF: Inclusion of time stamp in PDF document.
- Category: **TSP** ().
    - Shares:
        - Verify: Verify a time stamp protocol.
        - Sign: Signature with a time stamp (Time stamp protocol).

- Category: **Verify** ().
  - Shares:
    - TSP: Validates a time stamp protocol.
    - Pades: Validates a PDF document signature (PDF advanced electronic signature).
    - Xades: Validates an XML document signature (XML advanced electronic signature).
    - Cades: Validates a CMS (Cryptographic message syntax) document signature.
    - Cert: Validates a Keyman certificate.
    - CER: validates the public key of a certificate.

- Category: CertTrash:
  - Shares:
    - Del: Permanently delete the certificate from the certificate trash.
    - Rest: Restores a certificate from the certificate garbage can.

5. MENU ORGANIZATION

From the **Organization** menu you can access the following sections related to your organization (Illustration 46):

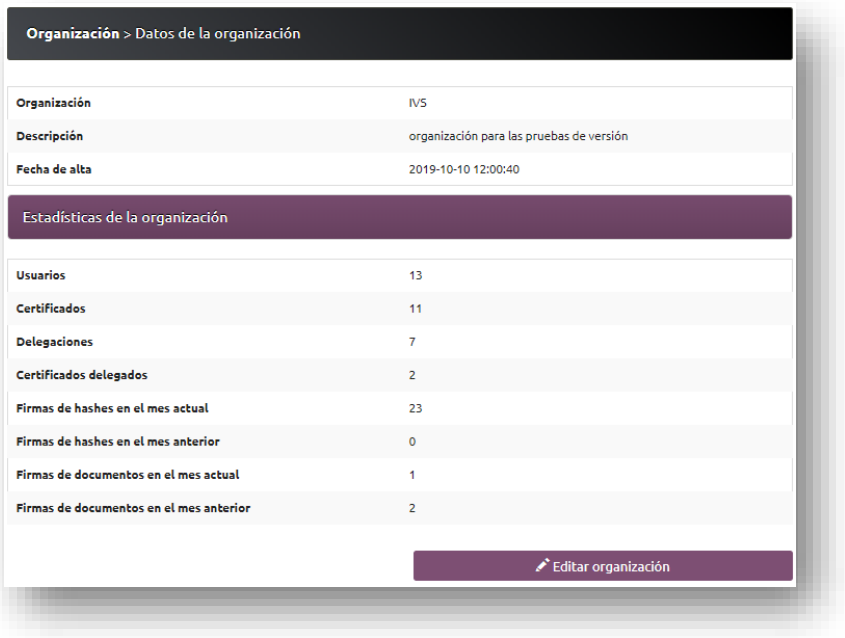
Illustration 46. Organization Menu

Note: The menu described below will only be available to users with administrator permissions.

5.1 ORGANIZATION MENU - INFORMATION

It shows the basic data of the organization to which the user in session belongs (Illustration 47).

Illustration 47. Organization data



The following functionalities will be available:

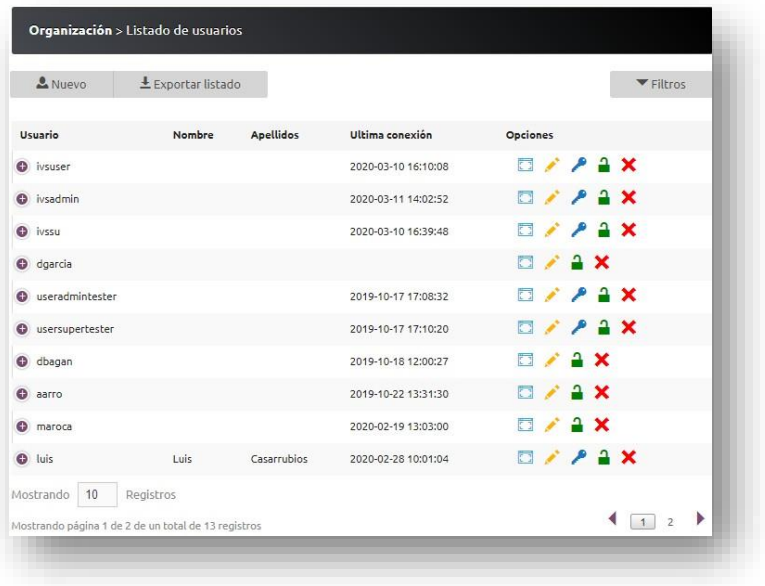
- Editar organización allows you to edit the description of the organization.

In the lower menu of organization statistics, information is displayed that refers to the number of certificates, Usage Controls, certificates with usage control, and signatures made by users in the previous and current month.

5.2 ORGANIZATION MENU - USERS

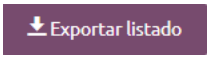
It shows the list of users belonging to the organization and allows you to go directly to other sections of the menu (Illustration 48).

Illustration 48. List of users



The users in the list can be displayed in different colors, depending on their status. Thus, disabled users are shown in gray and the padlock icon appears in red.

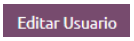
From the **Filters** field you can filter by any of the fields that appear in the list. When entering the desired text, only matches will be displayed.

By clicking on the button 

you can generate an XML file with the information of the organization's users.

For each of the users in the list, clicking on the icon displays all the fields of each user (those that do not fit in the width of the screen will be displayed). When clicked, it displays the list of non-visible fields and, to hide them again, click on the icon .

From the available icons it is possible to perform different actions with each user:

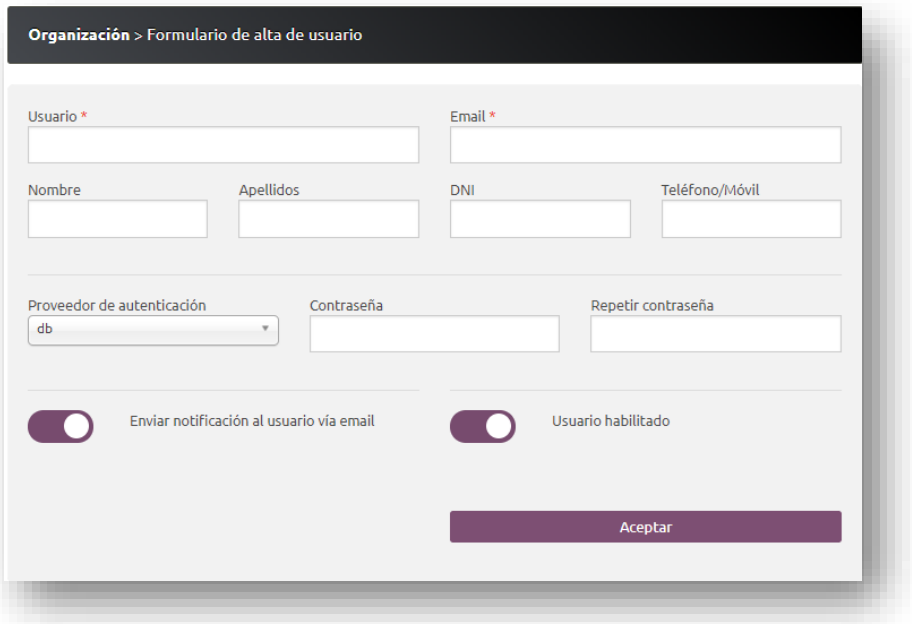
- See user.
  - Displays user data in detail. They can be edited with the 

- Modificar contraseña Allows you to change the access password by entering the new one directly.

- **Edit user**. Allows you to modify the user data, except for the User and Organization fields.
- **Modify password.** Allows you to change the access password by entering the new one directly.
- **Disable user**. Allows you to temporarily disable the user, blocking their access to IvSign. Disabling it marks the line in a different color and changes the icon. To enable the user again, click on the new icon .
- **Delete user.** Allows you to directly delete the user, when you click on delete user, it will ask for confirmation and will show the data of the user we are trying to delete.

In addition, the administrator can add new users to his organization by clicking Nuevo. Next, the user creation form is opened to complete the information (Illustration 49).

Illustration 49. User creation



*Note: The fields **User** (required) and **ID** (not required) must be unique in the organization. If an attempt is made to register a user that already exists with any of these data, it will return an error and will not allow the creation.*

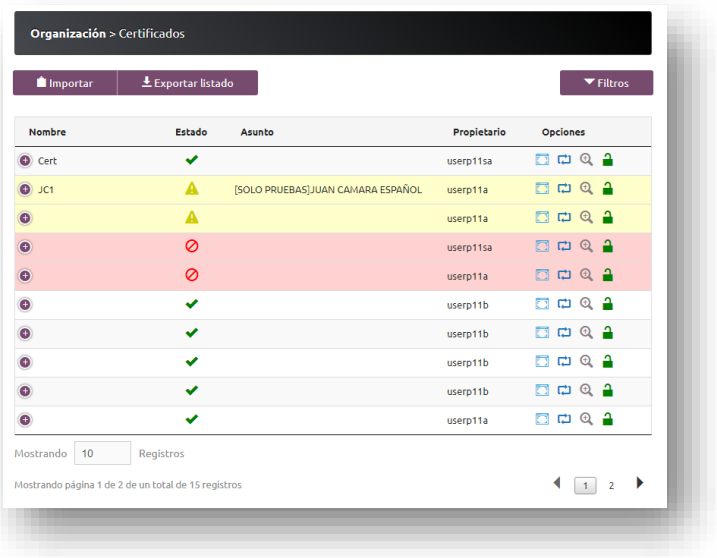
Once you have entered the required fields, click **OK** and the new user will be created.

- If you have checked the 'Send notification to user via email' option**,** an email will be sent to the new user with his or her credentials to access the platform.
- If this option is not checked, the administrator will be responsible for providing access credentials.

5.3 ORGANIZATION MENU - CERTIFICATES

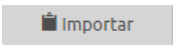
It shows the list of certificates of all the users of the organization and allows to go directly to other sections of the menu (Illustration 50).

Illustration 50. List of certificates



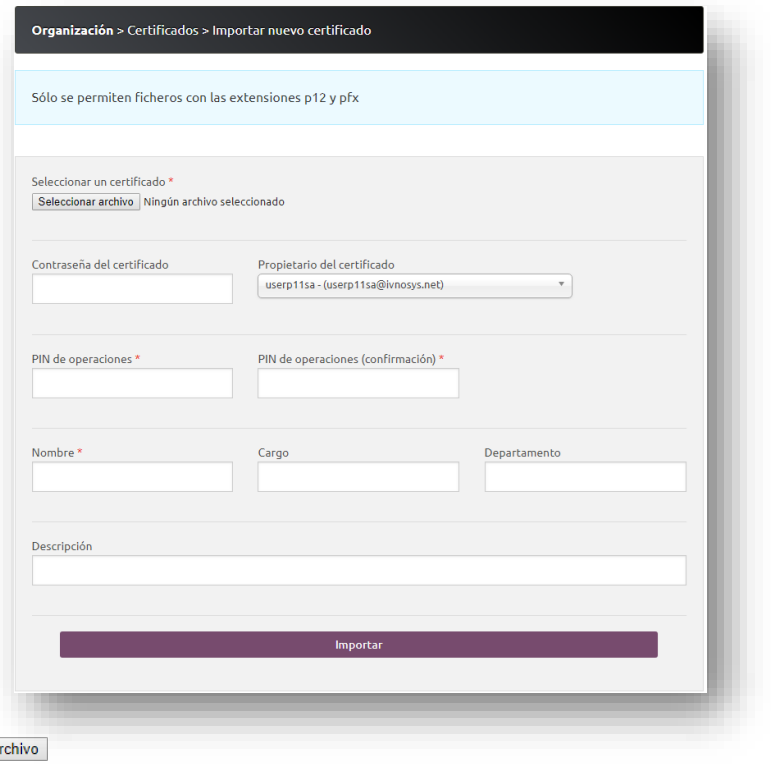
From the **Filters** field you can search the list of certificates, by any of the fields that appear in the list. When entering the desired text, only matches will be displayed.

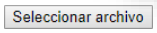
The icon ⊕ allows you to display the fields of each certificate that do not fit in the screen width. Pressing it will display the list of non-visible fields and, to hide them again, press the icon ⊖.

The button 

allows you to centralize and assign the certificates to the user of your organization as long as you have the .p12 or .pfx file of the same (Illustration 51).

Illustration 51. Import new certificate

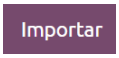




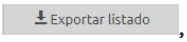
Pressing the browser windows of your computer are displayed for you to select the certificate file. **Only certificates with .pfx and .p12 extensions can be imported.**

The following fields must be filled in:

- **Certificate password** is the password issued with the certificate.
- **Certificate owner** we will be able to assign the certificate we are importing to the user of our organization that we consider convenient.
- **Operations PIN** is the password that the user assigns to the certificate for its use. The pin must be confirmed in the **Operation pin (confirmation)** field.
- **Name** is the name of the certificate that will be displayed in the panel.
- The fields **Description**, **Title** and **Department** are not mandatory fields, but in case they are filled in, they will be displayed in the certificate information in the panel.

Finally, click on 

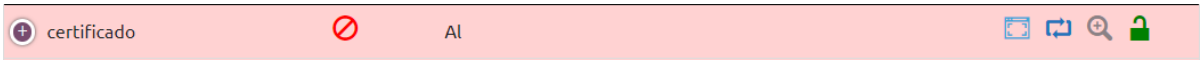
to complete the import of the certificate, which will be displayed in the list of **My Certificates**.

In the button 

, you can download an XML file with the information of all the organization's certificates.
The certificates, depending on their status, are displayed in one color:

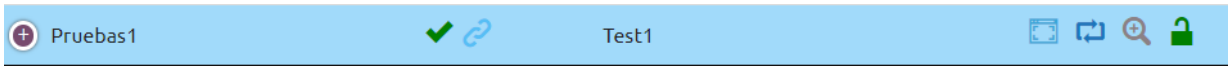
- **Disabled** certificates are shown in gray.

- **Revoked** certificates are shown in red.



- **Expired** certificates are shown in yellow.

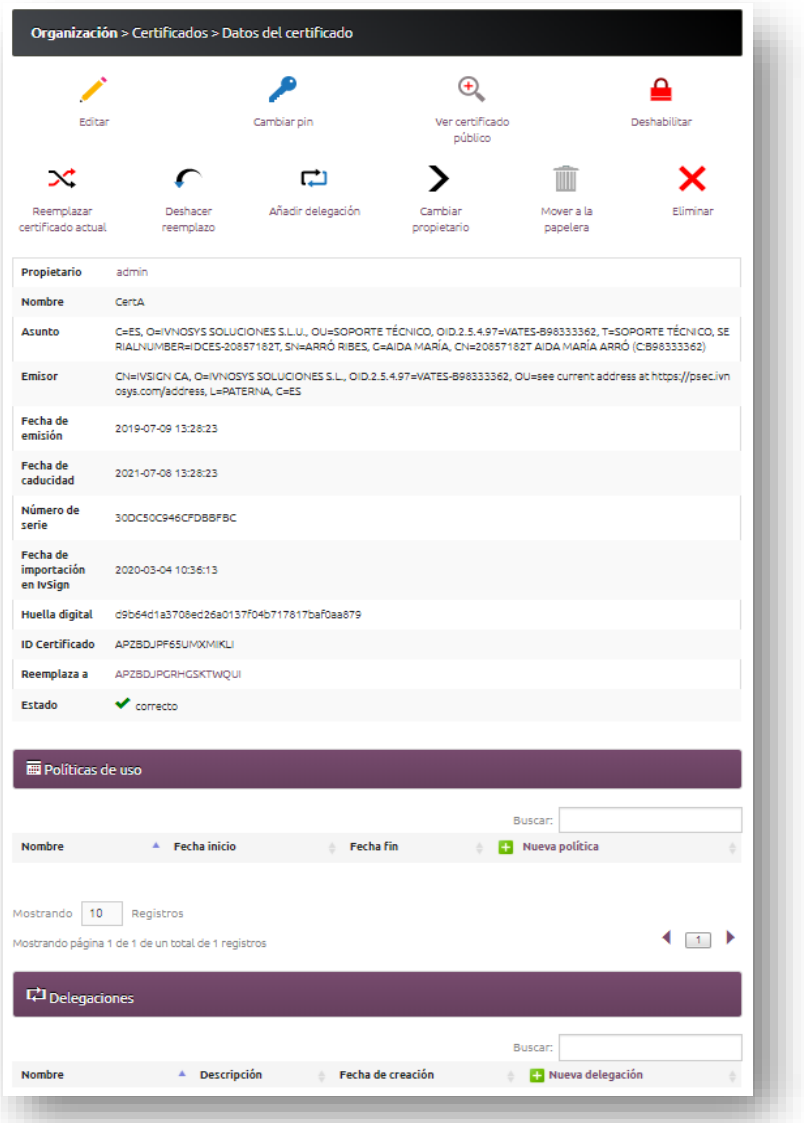
- The referenced or external certificates appear in blue.



From the available icons it is possible to perform different actions with each certificate:

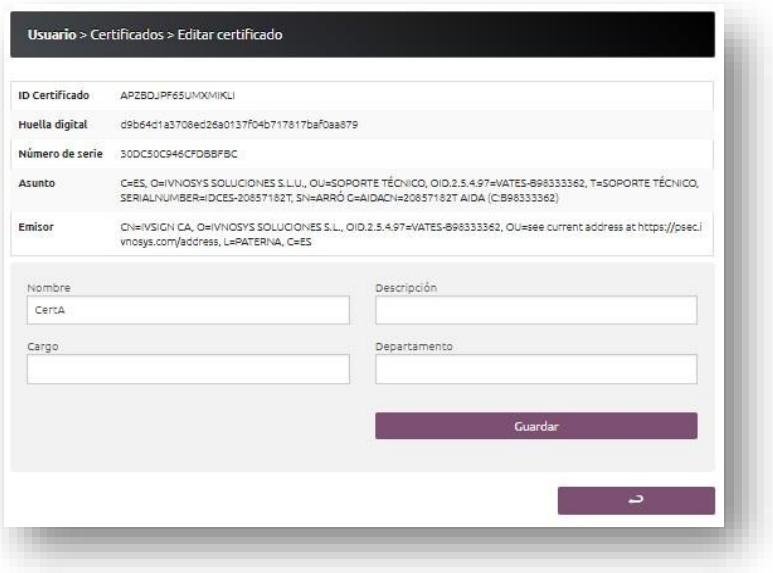
- **Manage certificate**. Displays the certificate data in read mode (Illustration 48). It will be possible to manage the usage policies that apply to the certificate (see item
How to apply usage policies to certificates).

Illustration 52. Certificate data



- **Edit certificate**. Allows you to modify the following fields of the certificate information to be displayed in the panel: Name, Description, Title and Department. It will also show information about the certificate, such as the ID, the fingerprint, its serial number, the subject and who the issuer is (Illustration 53).

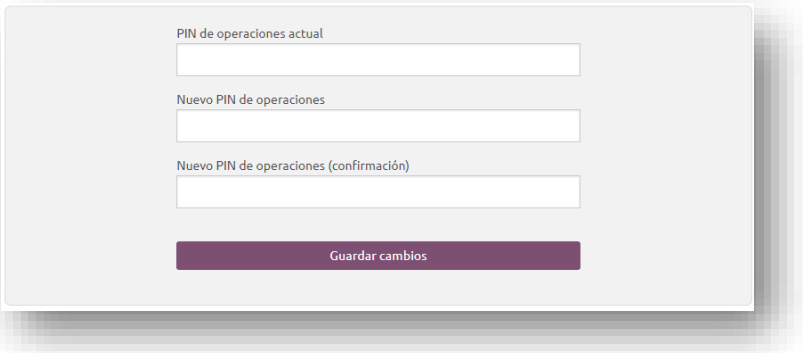
Illustration 53. Edit certificate



- **See public certificate**. Allows you to download the public key of the certificate (file .crt).

- **Change certificate PIN**. Allows you to modify the operations PIN assigned to the certificate. The current PIN must be entered and the new PIN confirmed in order to change it (Figure 54).

Illustration 54. Change PIN



Select the new owner of the certificate and click on "Change owner" to make it available to the new owner.
make the change.

- **Replace current certificate**. This can be very useful when a certificate with associated usage rules and usage controls expires. Once inside this option we will be asked for the certificate with which we want to replace the current one, then we will be asked to enter the pin of the old certificate and then the pin of the new certificate. This way the new certificate will be active and the controls and rules of use will be associated to it.
- **Add usage control**. Allows to authorize the use of the certificate to another user of the organization, without losing control over it and limiting its use (see point Control of use).
- **Change of ownership.** From this option we can assign a new owner to the certificate, a list of all available users will be shown.
- **Move to trash.** Allows you to send the certificate to a trash garbage can, you will be asked for confirmation. They will not be deleted directly, but will be stored in a recycle garbage can where we can later delete them permanently or restore them.
- **Disable certificate**. Allows you to temporarily disable the certificate.

When a certificate is disabled, it will not be displayed to perform actions that require a certificate, such as signing in or logging in to a site.

In the centralization panel, it will still be displayed, but the line will be marked in a different color and the icon will change. To enable the certificate again, click on the new icon .

The certificate can be enabled by the user or the organization's administrator, and is automatically disabled if the PIN is entered more than 5 times incorrectly.

- **Delete certificate**. Allows the certificate to be removed from the platform, as long as it does not have associated usage controls enabled. If you have associated usage controls, you must first delete the usage control (see section on Usage Controls).

    - If a certificate that has been automatically centralized is permanently deleted, it cannot be recovered.
    - If a manually imported certificate is deleted, you can import it again to have it centralized.

- Nueva política **Create new usage policy**. Allows you to restrict the use of each certificate, provided you have the necessary permissions (see section How to apply usage policies to certificates).

5.4 HOW TO APPLY USAGE POLICIES TO CERTIFICATES?

Usage policies allow you to limit the use of certificates, both for your own use and for authorized use (usage controls).

A user may apply usage policies for its own certificates and, in case of usage control, these usage policies are transferred to the controls, thus also applying to the authorized user. In case the usage control of a certificate has usage rules, they will be accumulated with the usage policies, applying the most restrictive in each case.
An organization may apply usage policies to its users' certificates to restrict their use.

To define the policies for the use of certificates, either your own or the certificates of the organization's users (only available to users with administrator permissions), you can access from several menus:

To apply usage policies to your own certificates, you can access from:

- User menu > Certificates > Manage certificates, clicking on the icon **Manage certificate**, will display the certificate details.
    - If there are use policies associated to that certificate or not, the list will be shown and the button Nueva politica will be available and in the section Use policies in the icon (Illustration 55).

Illustration 55. Usage Policy

- User menu> Usage Controls, from **View usage control data**, if the selected certificate has usage policies, a message will be displayed that will allow direct access to the certificate details (Illustration 56).

Illustration 56. Certificate detail

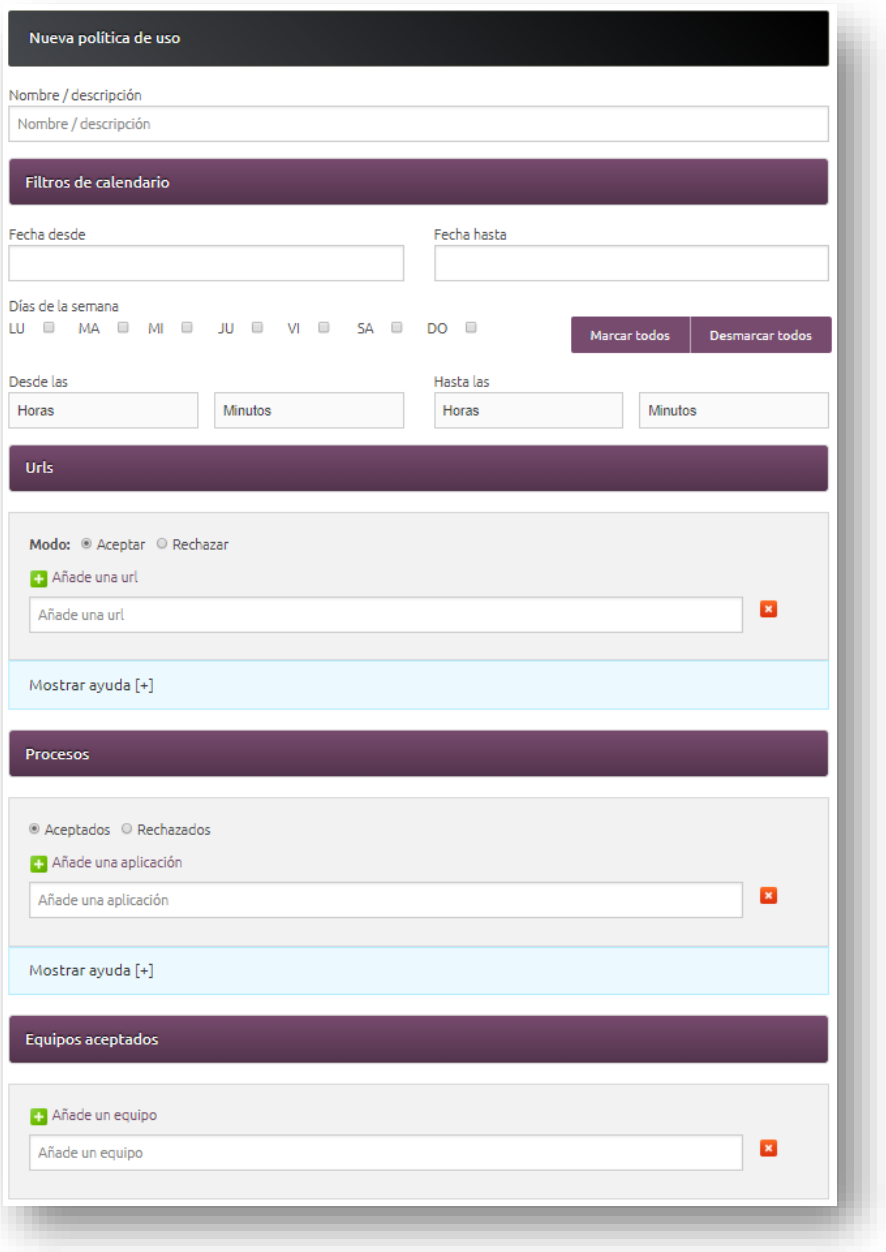
And to the list of policies for the use of such certificate, where you will have available the button

Nueva politica

- To apply usage policies to the certificates of the organization's users, you can access from.
  - Organization menu > Certificates > Manage certificates, by clicking the icon **Manage certificate**, will show the certificate details.
    - If there are use policies associated to that certificate or not, the list will be shown and you will also have available the button Nueva politica and in the section Use policies, in the icon

In both cases, a window like the following will be displayed (Illustration 57):

Illustration 57. New usage policy



The form consists of 5 sections that allow you to limit the use of the certificate, both for your own use and for authorized uses of the certificate.

- **Basic data**. The name or description of the rule of use must be indicated.
- **Calendar filters**. Allows you to set different filters to indicate when the certificate can be used.

- **Date range**. Allows you to define the date range in which the certificate can be used.

By clicking on the 'Date from' or 'Date to' field, a calendar is displayed for the selection of start and end dates. *Outside the established range **no** will not be allowed.*

- **Days of the week**. Allows you to define the days of the week on which the certificate can be used.

You can check/uncheck all the days of the week, from the available buttons, or you can check individual days by clicking directly in the box of the corresponding day.

- **Range of hours**. Allows you to indicate a time of use, choosing the hours and minutes from the drop-down fields. *Outside the established hours **no** use of the certificate will not be allowed.*
- **Filter by URLs**. Allows you to define the accepted and rejected web addresses that can be accessed or not, with the certificate.
    - If the **Accepted** option is checked, the indicated URLs will be the only ones that can be accessed with the certificate.
    - If the **Rejected** option is checked, all URLs will be accessible with the certificate, except for those indicated.

In both cases the configuration "https://" should be used.

Once the url has been added, if you wish to add more, click on  . You can add as many as you need and they will be displayed as a list.

You can edit the content of the entered lines by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon  directly.

- **Process filter**. Allows you to define which applications are accepted or rejected for use with the certificate.
    - If the **Accepted** option is checked, the indicated applications will be the only ones that can be accessed with the certificate.
    - If the **Rejected** option is checked, the certificate will allow access to all applications except those listed above.

To find out the exact name of the process, access the 'Task Manager', 'Processes' tab. The name of the application has been added, if you wish to add more, click  .

You can add as many as you need and they will be displayed as a list, and you can edit the content of the lines entered by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon directly.

- **Filter by equipment**. Allows you to define the computers from which the certificate can be used.

  - To find out the complete name of the equipment, you must access the properties of 'My Computer'.
  - Once the name of the equipment has been added, if you wish to add more, click . You can add as many as you need and they will be displayed as a list.
  - You can edit the content of the entered lines by clicking on the text directly and changing the desired information. You can also delete any of the lines by clicking on the icon directly.

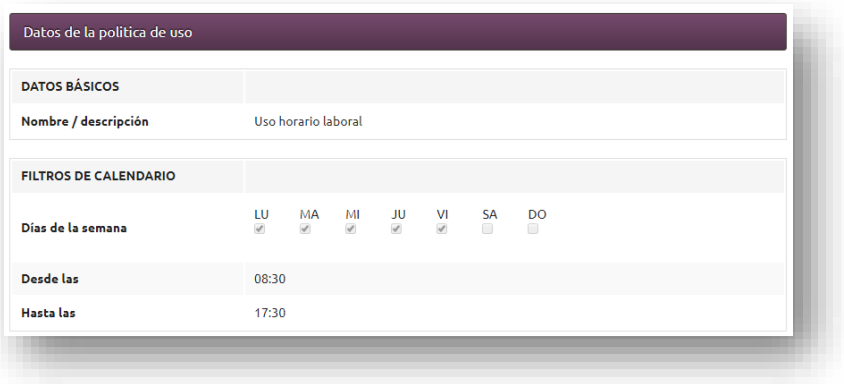
Once the desired sections have been completed, click on OK to create the usage policy and it will be listed in the certificate detail (Illustration 58).

Illustration 58. Create usage policy

From the icons available next to each usage policy, you can perform different actions:

- **See details of the use policy**. Displays the data entered in the form for creating the usage policy (Illustration 59).

Illustration 59. Details of use policy



- **Modify usage policy**. Allows you to modify all the data entered in the form for creating the usage policy.
- **Remove usage policy**. Allows you to delete the usage policy.

5.5 EXAMPLE OF CERTIFICATE USAGE POLICIES

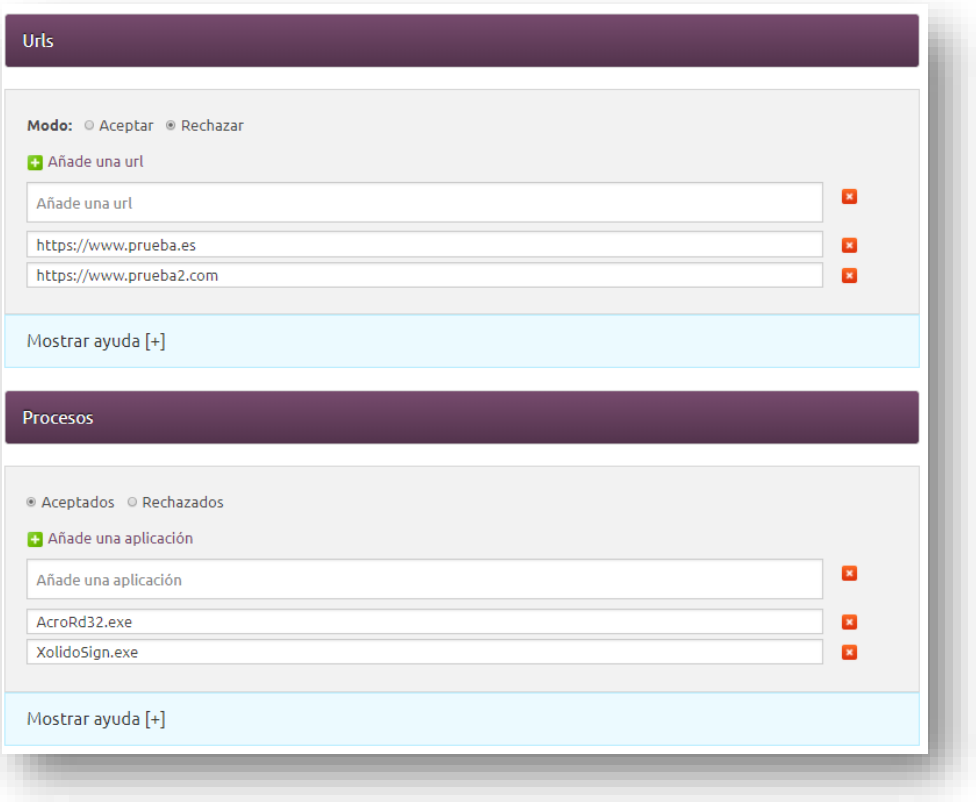
The configuration of the usage policies can be inclusive or exclusive depending on how the usage policies are configured:

- **Inclusive:** When configuring several limitations within the same rule of use, all of them must be complied with in order to carry out the signature process *(example 01)*.
- **Exclusive:** In order to be less restrictive, there is the option to configure two usage rules for a certificate to comply with one of the two *(example 02)*.

INCLUSIVE USE POLICIES: EXAMPLE 01

Restriction of use so that they cannot sign on certain URLs and, in addition, can only use certain signing applications.
For this limitation, a single usage rule will be created with all the restrictions as shown in the following image (Illustration 60).

Illustration 60. Inclusive policies



EXCLUSIVE USE POLICIES: EXAMPLE 02

Restriction so that they cannot sign on certain URLs or can only use certain signature applications.

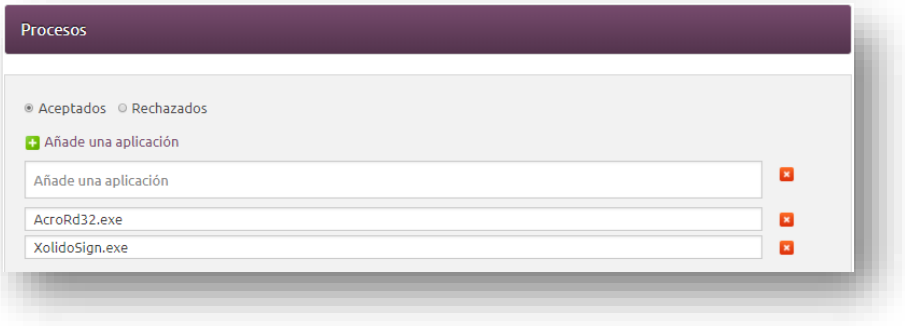
In this case, two usage rules must be created, each with its own limitation. When a signature process is performed, the restrictions are checked and if either of the 2 complies, the limitation will be applied.

- Creation of Rules of Use (Illustration 61):

Illustration 61. Rules of use

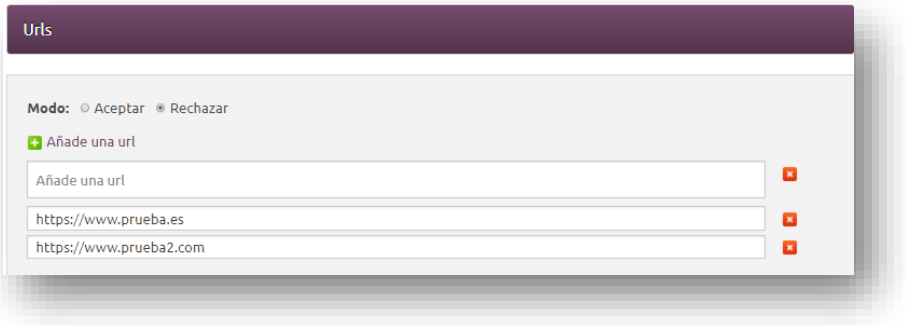
- Accepted processes to use only the processes assigned to that usage policy (Illustration 62).

Illustration 62. Usage policy processes



- Rejected URLs so that they cannot sign on the URLs indicated (Illustration 63).

Illustration 63. URL usage policies



5.6 ORGANIZATION MENU - USAGE CONTROLS

It shows the list of certificate usage controls performed by users of the organization to other users, and allows the management of these.

Usage control is used to authorize the use of one's own certificate to another user of the same organization. It is possible to parameterize who and when can use the certificate with authorization of use, in addition to limiting the use in certain computers, processes and URLs. To do this, it is necessary to create the usage control and add both usage rules and target users (Illustration 64).

Illustration 64. Organization menu - Usage controls

From the **Filters** button it is possible to search among the usage controls created, by any of the fields available in the list. By entering the desired text and pressing the button Mostrar, only the matches will be displayed.

From the icons available in the list next to each usage control, you can perform different actions:

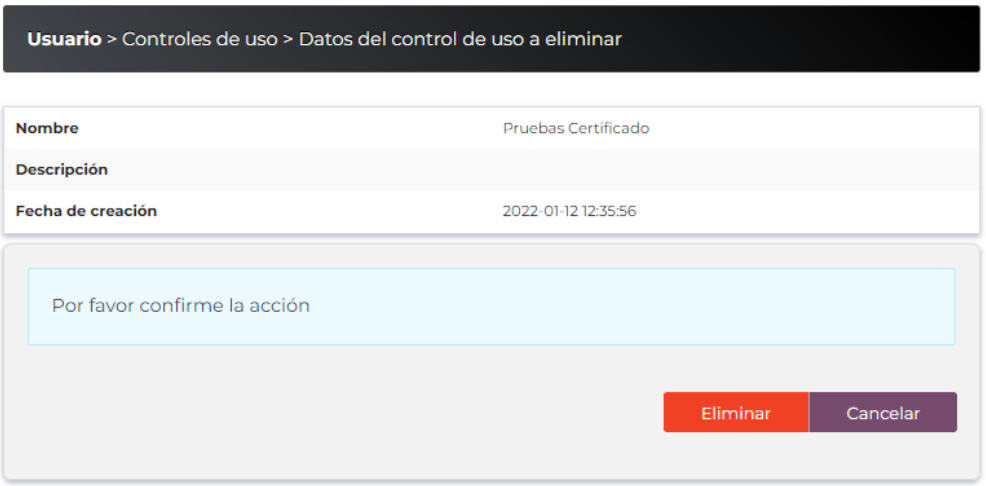
- **View usage control data** Allows access to the basic data of a usage control, as well as the linked users/certificates and usage rules. In addition, you will have the possibility to remove the usage control and/or disable it, as well as to manage the usage rules and the linked users.
- **Create new usage rule**. Allows direct access to the form for creating a new usage rule, to limit the availability of the certificate with usage control (for more information, see point How to authorize the use of a certificate).
- **Add user**. Allows direct access to the screen for selecting the users authorized to use the certificate (for more information, see point How to authorize the use of a certificate).
- **Disable Usage Controls**. Allows you to deactivate the usage control temporarily. This action can also be carried out from the usage control display (View usage control data button).

When a usage control is disabled, the user for whom the certificate has been allowed to be used will not have it available. In the certificate owner's centralization panel it will still be displayed, but it will be marked in a different color and the icon will change.
To enable the use again, click on the new icon (Illustration 65).

Illustration 65. Enable Usage Control

Eliminate usage control. Allows you to delete the created usage controls. In case the selected usage control is associated to users, a message informing about this will be displayed. In case of confirmation, the link with the users will be automatically removed. This action can also be carried out from the usage control display (View usage control data button) (Figure 66).

Illustration 66. Eliminate usage control



5.7 HOW TO AUTHORIZE THE USE OF A CERTIFICATE OF A USER OF THE ORGANIZATION?

To authorize the use of a certificate of another member of the organization to another user or users, you must perform the following steps:

1. Create usage control

Usage control can be **created** from several menus:

- Organization menu> Usage controls>Manage certificate by clicking on of the certificate to be authorized.
- Organization menu > Usage controls, by pressing Nuevo.

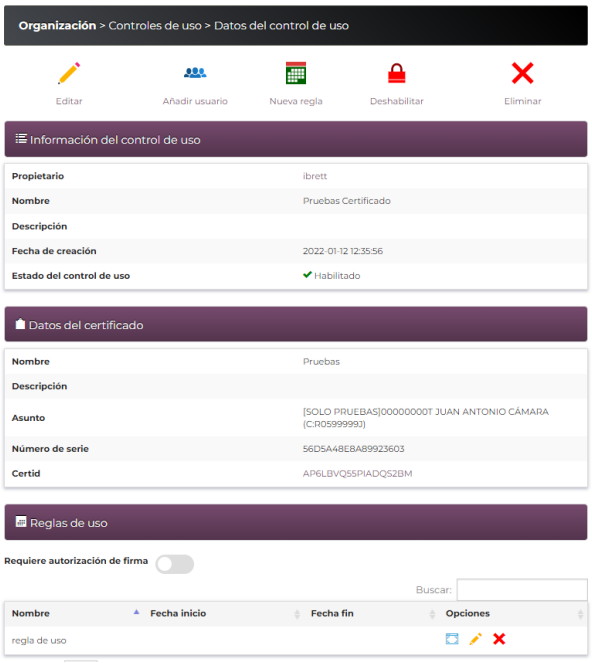
In both cases you must follow the same steps as for authorizing the use of your own certificate (see point How to authorize the use of a certificate?).

2. Define the rules of use (Optional).

To **define the rules of use**, which allow you to limit the use of the certificate with authorization, you can access from several menus (Figure 67):

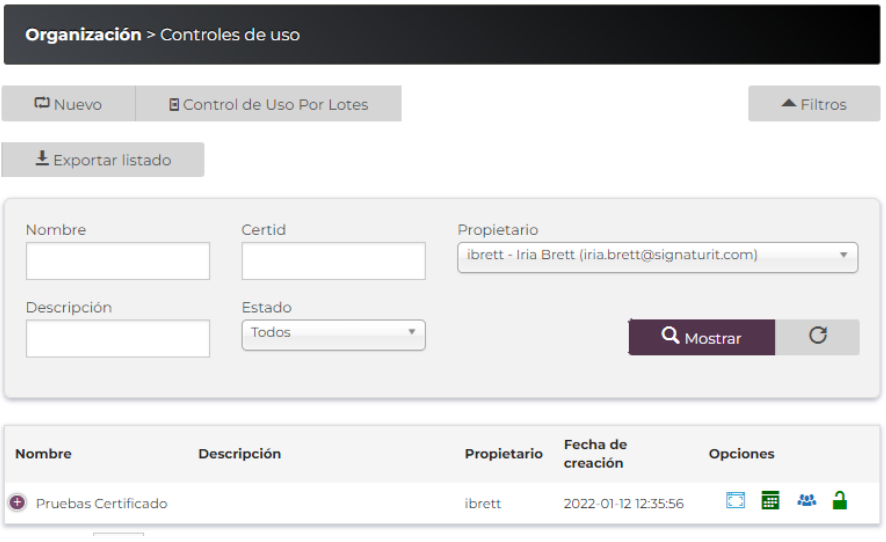
- From the detail of the usage controls shown when creating it, pressing .
- When the usage control has been created previously, from the menu Organization> Usage Controls, you must click on to display the usage control data.

Illustration 67. Define rules of use



From the Organization > Usage Controls menu, by clicking (Figure 68).

Illustration 68. Organization menu - Usage controls



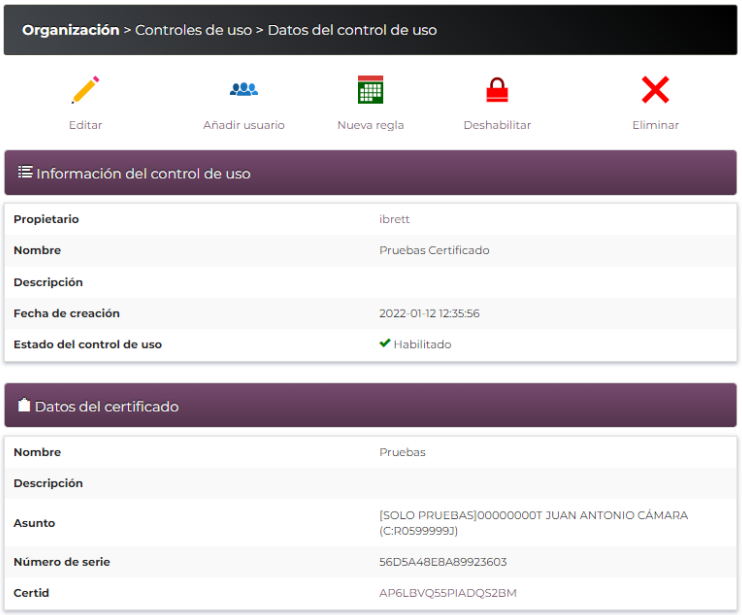
In both cases you must follow the same steps as for authorizing the use of your own certificate (see section How to authorize the use of a certificate).

1. Select the users that will use the certificate.

To **select the users** who will make use of the authorized certificate through usage control, you can proceed from several points:

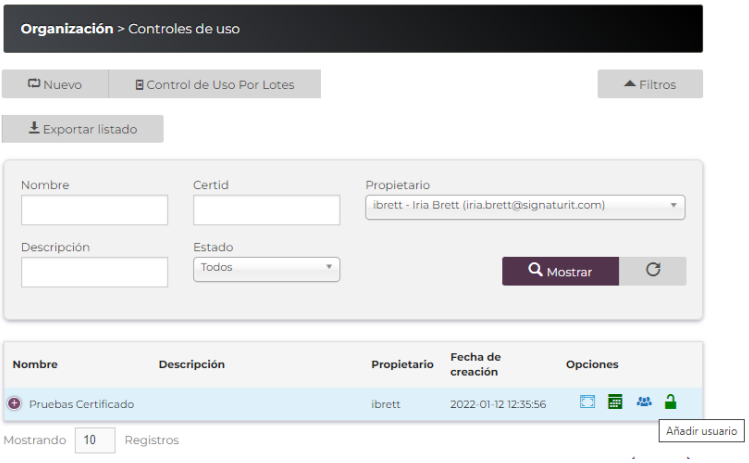
- From the detail of the usage control shown when creating it, by clicking Añadir usuario.
- If the usage control already has a user assigned to it (if the usage control has been created previously), click on to display the usage control data (Figure 69).

Illustration 69. Display usage control data



- From the Organization > Usage Controls menu, press (Illustration 70).

Illustration 360. Organization menu - New usage control



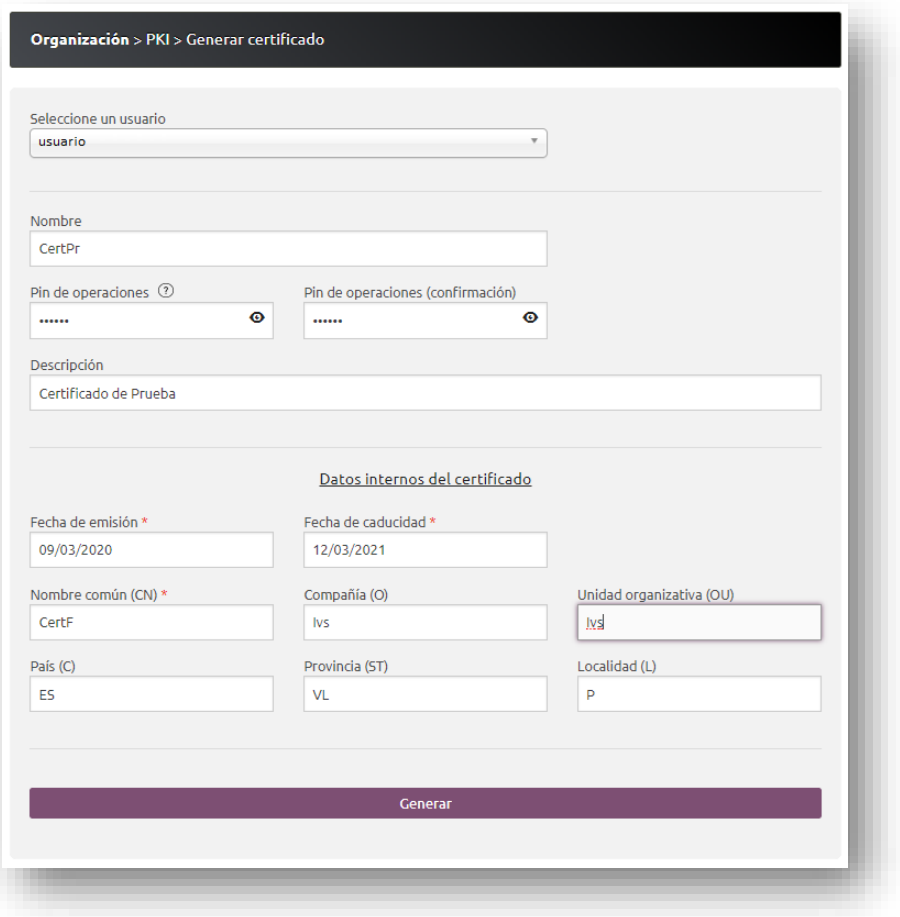
In both cases you must follow the same steps as for authorizing the use of your own certificate (see section How to authorize the use of a certificate).

5.8 ORGANIZATION MENU - PKI

It allows to generate our certificates, for it will be acceded to Generar certificado where a series of data will be requested that will have to be filled up to be able to generate it. First, the user must be selected and then given a name.
Then an operation pin must be entered and confirmed, if an operation pin is not established, it will be generated automatically and will be notified by e-mail to the user receiving the certificate. In case a pin is established, no e-mail notification will be sent.

Next, the internal data of the certificate will be entered, it will be mandatory to enter the date of issue, expiration date and common name (CN). Similarly, company (O), organizational unit (OU), country (C), province (ST) and locality (L) can be added (Illustration 71).

Illustration 71. Generate certificate

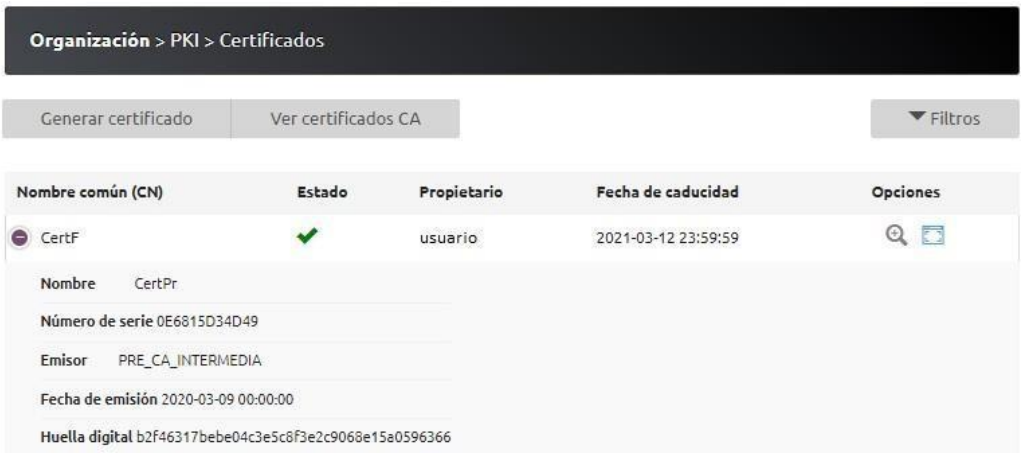


Next, a message is displayed informing that '**The certificate has been successfully generated and imported**' (Illustration 72).

Illustration 72. Confirmation

Next, the generated certificate is displayed, and when selecting the icon all the details of the certificate will be displayed, showing the common name (CN), its status, the owner, the expiration date and the options that we have on it (Illustration 73).

Illustration 73. Confirmation

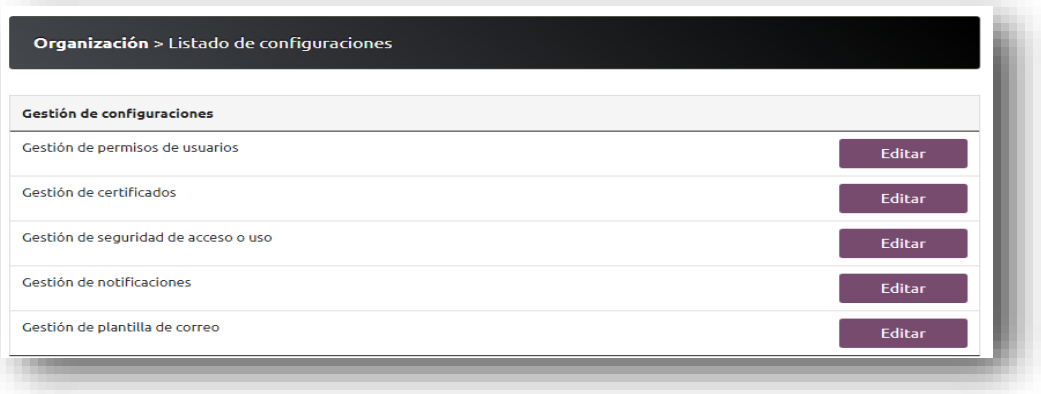


By clicking on the icon to download the public certificate, and selecting manage certificate, you can access the menu from where you can revoke this certificate, delete it or manage it.

5.9 CONFIGURATION MANAGEMENT

It allows you to configure the parameters of your organization, and to access the options of each menu by clicking on the "Edit" button. (Illustration 74).

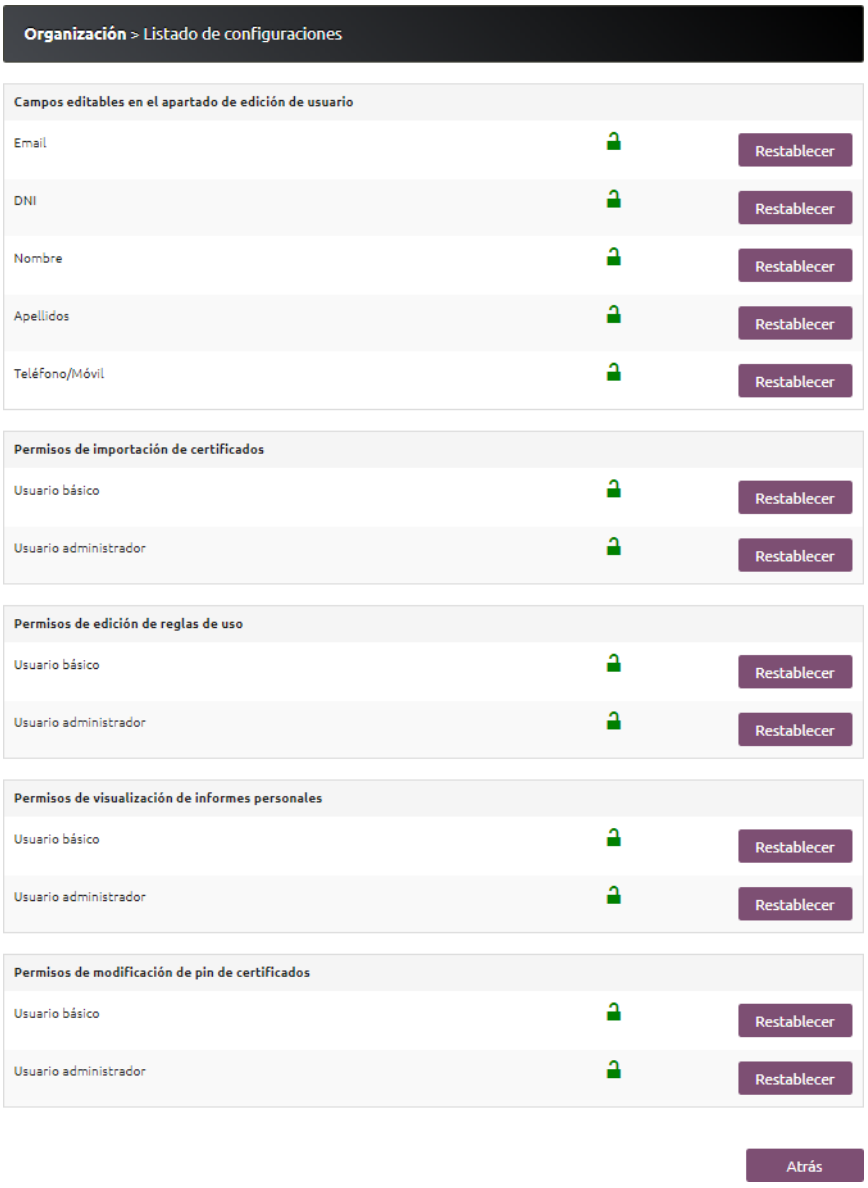
Illustration 74. Organization menu - List of configurations



User permissions management.

Allows you to configure the actions that can be performed by the organization's users (Illustration 75).

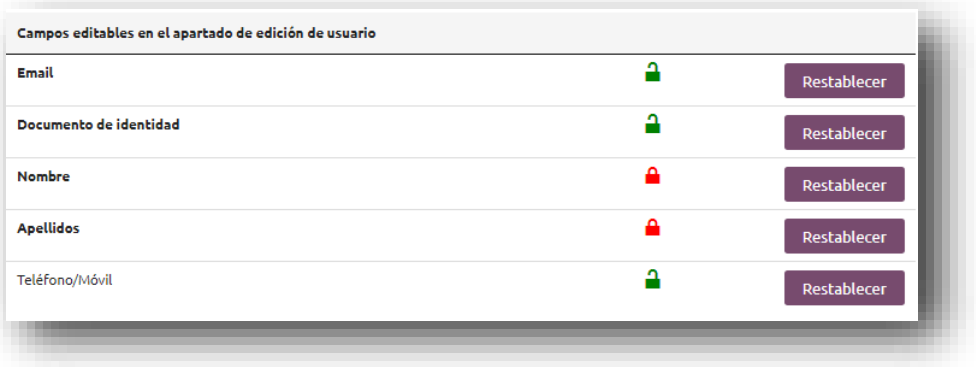
Illustration 75. User permissions



- **Editable fields in the user edition section.**

Allows you to configure which fields in the "User > Personal data" section can be edited by the user. users of the organization (Illustration 76).

Illustration 76. User data

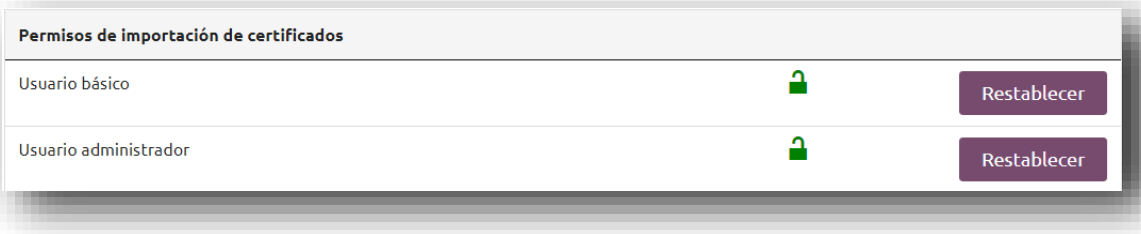


This icon indicates that editing of the field is allowed.
This icon indicates that editing of the field is not allowed.
From the reset button we return to the default configuration for the organization. If a default value is changed in the panel, it will give a visual warning by marking the field in bold.

- **Certificate import permits.**

Grant permissions to the organization's users, so that they can import certificates into their IvSign account (Illustration 77).

Illustration 77. Import certificates



Permissions are set by roles (basic user with normal permissions and administrator user who would be in charge of managing the organization), i.e. these permissions cannot be applied individually per user.

- **Editing permissions of usage rules.**

Permissions to the organization's users, so that they can create and modify usage rules that limit the use of certificates that are authorized to other users (Illustration 78).

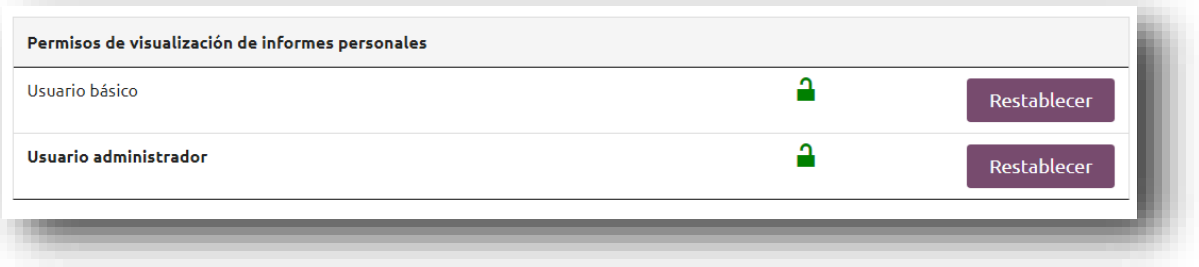
Illustration 78. Rules of use

Permissions are set by roles (basic user with normal permissions and administrator user, who would be in charge of managing the organization), i.e. these permissions cannot be applied individually.

- **Personal report display permissions.**

Assigns permissions to users in the organization so that they can view usage reports. If you do not have permissions, this submenu will not be available in the user menu (Figure 79).

Illustration 79. Personal reports



Permissions are set by roles (basic user with normal permissions and administrator user, who would be in charge of managing the organization), i.e. these permissions cannot be applied individually.

- **Certificate pin modification permissions.**

It allows to give permissions to the users of the organization, to modify the pin of the certificates. If the user does not have permissions, he will not be able to modify the certificate pins. (Illustration 80).

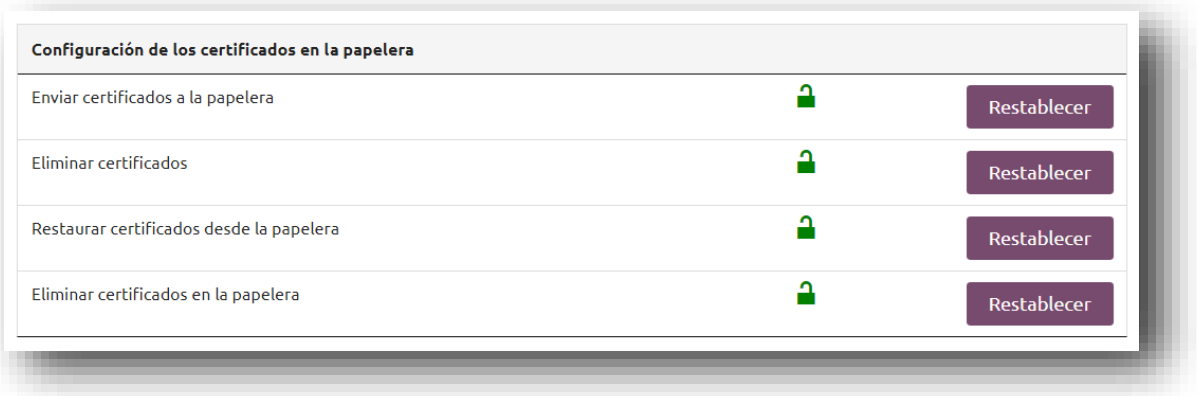
Illustration 80. Personal reports

Certificate management

o Configuration of the certificates in the recycle garbage can.

Grant permissions to the organization's users, so that they can delete and send certificates to the trash. If you do not have permissions, you will not be able to send certificates to the recycle garbage can (Illustration 81).

Illustration 81. Certificates in paper garbage can



It applies to all users regardless of their role.

o Visibility of certificates in KeyController.

Configure the behavior of the KeyController to display both expired and revoked certificates (Figure 82).

Illustration 82. KeyController

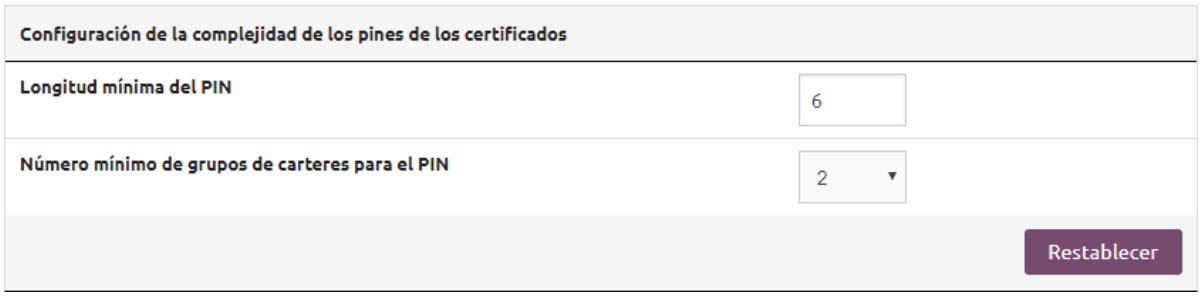
It applies to all users regardless of their role.

Access or use security management.

- **Configuration of the complexity of the certificate pins.**

Sets the minimum pin length used in certificates. The value ranges from 1 to 50. Part of the length, you can modify the minimum complexity of the pin (Illustration 83).

Illustration 83. Certified pin

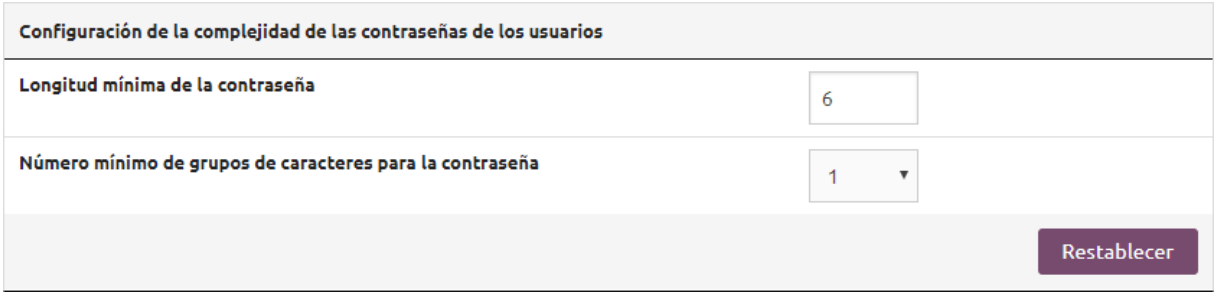


The complexity indicates the number of character groups to be used (lowercase, uppercase, uppercase),
numbers and symbols ($, %, & ...)):
With complexity 1, one of the groups must be used, with complexity 2, two of the groups, with complexity 3, three of the groups and with complexity 4, all the groups).
It applies to all users regardless of their role.

- **Configuration of the complexity of user passwords.**

Sets the minimum length of the password used by users to access the platform; the value ranges from 1 to 50 (Illustration 84).

Illustration 84. User password



The complexity can be modified. The complexity indicates the number of character groups to be used:

- ☒ Lowercase
- ☒ Capitalization
- ☒ Numbers
- ☒ Symbols ($, %, & ...)

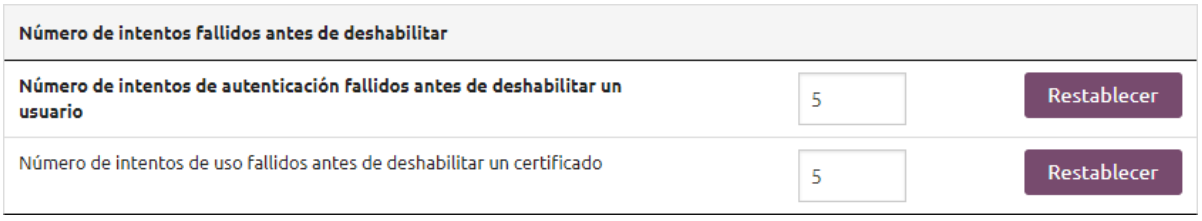
With complexity 1, one of the groups must be used, with complexity 2, two of the groups, with complexity 3, three of the groups and with complexity 4, it must contain 1 character from each of the 4 groups).

It applies to all users regardless of their role.

- **Number of failed attempts before disabling.**

As an extra security measure to prevent brute force attacks1 , configure the consecutive failures allowed before disabling both a user and a certificate (Illustration 85).

Illustration 85. Failed attempts



[1] A brute-force attack is a way of recovering a key by trying all possible combinations until the one that allows access is found.

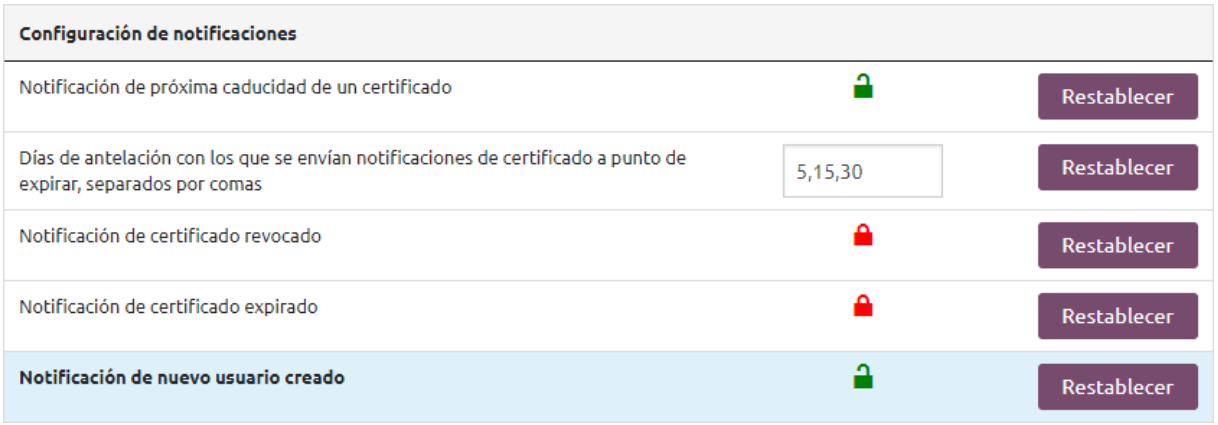
The default is 5 attempts for both users and certificates. The value ranges from 1 to 100. It applies to all users regardless of their role.

Notification management.

o Configuration of notifications.

Controls the way the platform notifies (Illustration 86) and informs the organization's users of certain events such as certificates about to expire, revoked or expired certificates, creation of new users...

Illustration 86. Configuration of notifications



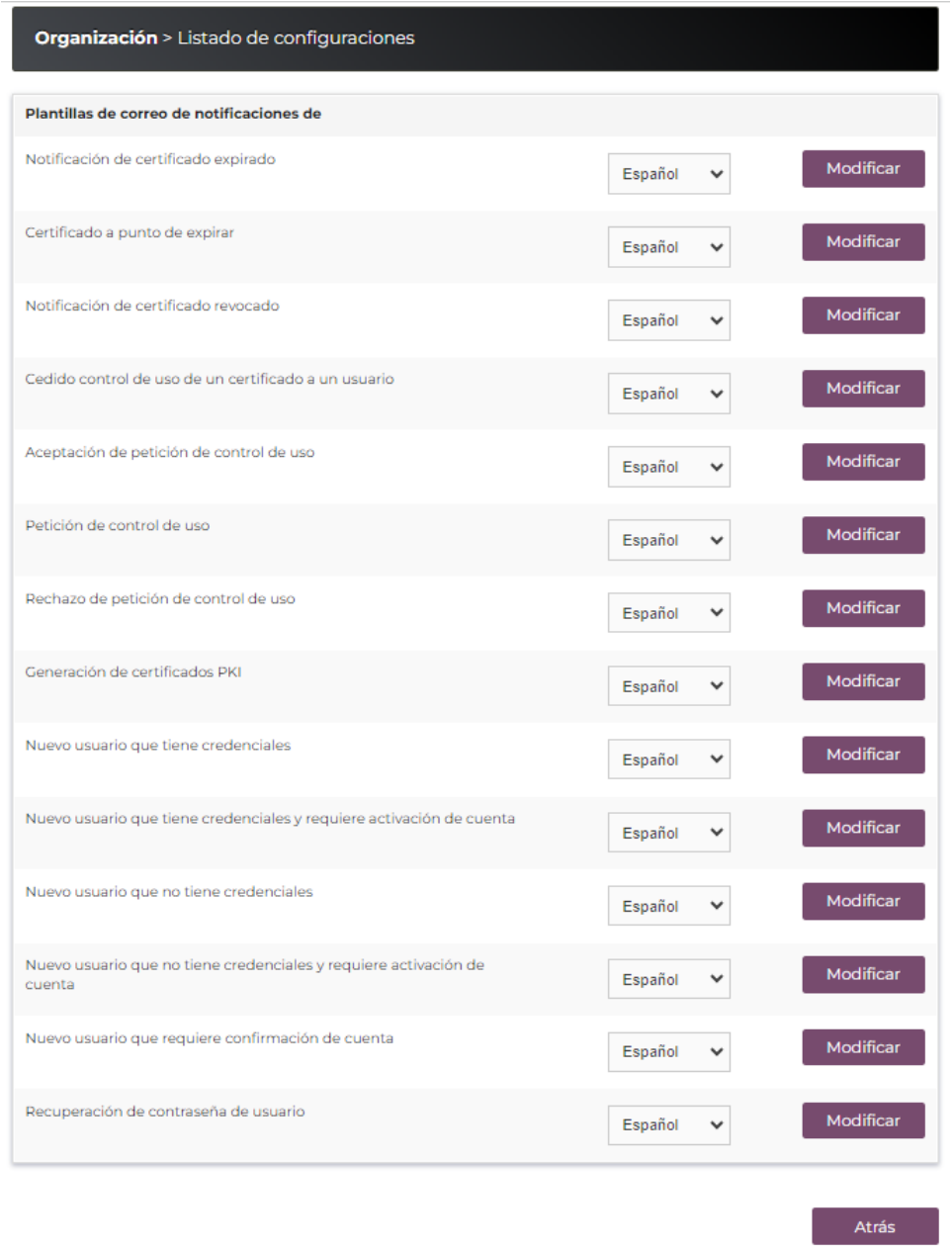
It applies to all users regardless of their role.

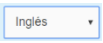
Mail template management.

o Mail templates.

Configure the content of the notifications sent by the platform, both in Spanish and English (Illustration 87).

Illustration 87. Mailing Templates



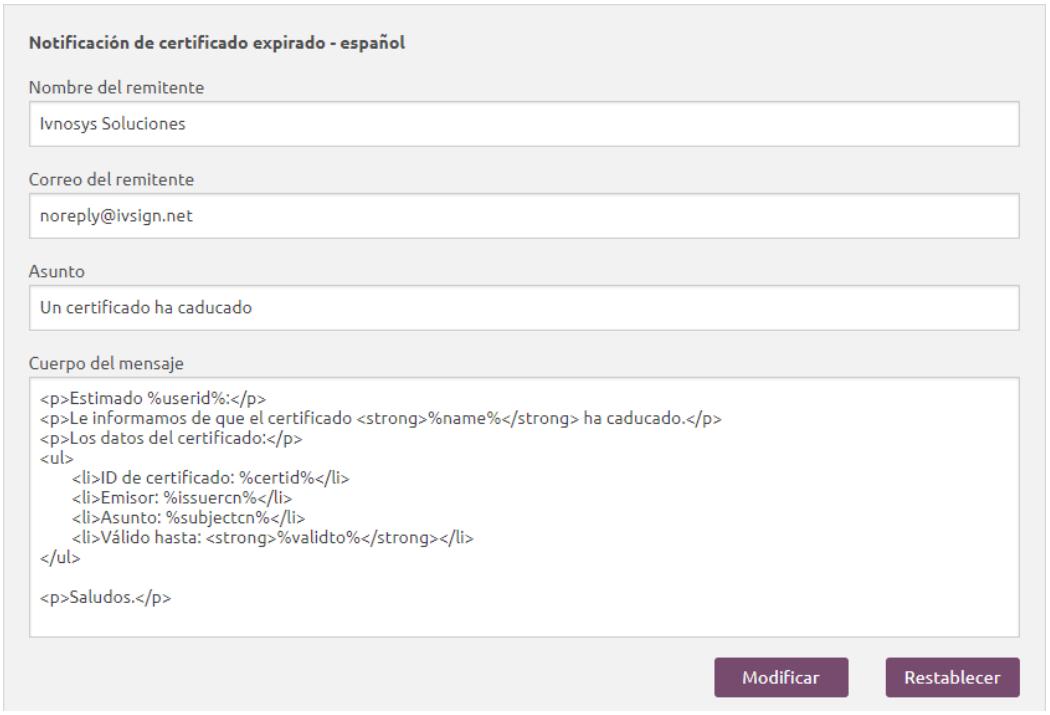
To modify the templates in English, select the "English" option in the drop-down menu 

and click on "Modify".

If you click on 

modifies the notification template (Illustration 88).

Illustration 88. Modification of notifications

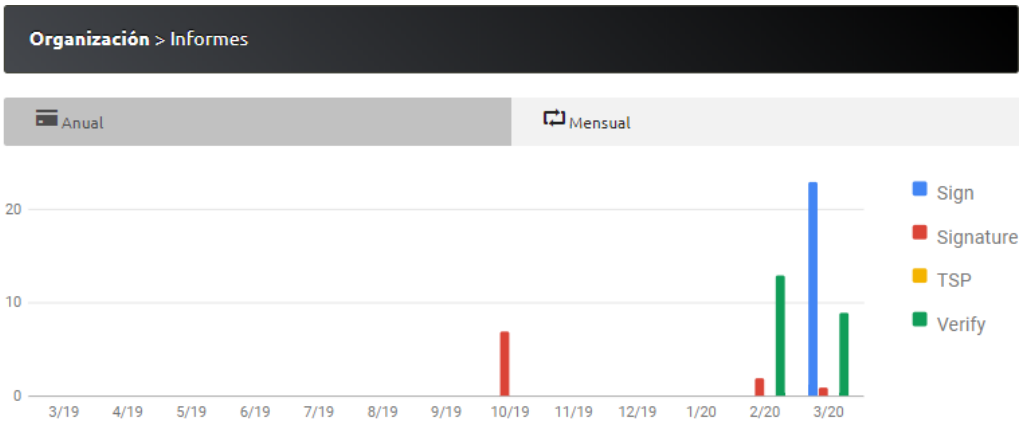


It has a series of keywords that allow you to compose templates. These keywords will be replaced by the corresponding values.

5.10 ORGANIZATION MENU - REPORTS

It allows to consult, in a differentiated way, the information related to signatures and authentications on the web with centralized certificates (Illustration 90).

Illustration 90. Organization menu - Reports



Fecha	Sign	Signature	TSP	Verify
3/19	0	0	0	0
4/19	0	0	0	0
5/19	0	0	0	0
6/19	0	0	0	0
7/19	0	0	0	0
8/19	0	0	0	0
9/19	0	0	0	0
10/19	0	7	0	0
11/19	0	0	0	0
12/19	0	0	0	0
1/20	0	0	0	0
2/20	0	2	0	13
3/20	23	1	0	9

Sign: Firmas simples de hashes, realizadas por el KeyController
Signature: Firmas de documentos, realizadas por el motor de firma
TSP: Sellados de tiempo
Verify: Verificaciones de certificados y documentos firmados

We have two tabs: Annual and Monthly:

- In the "Annual" tab, we can see in general terms the actions carried out in our organization and covers one year backwards from the current date organized by months.
- In the "Monthly" tab we can obtain reports of the user himself and those made by users with authorized certificates through the usage control.

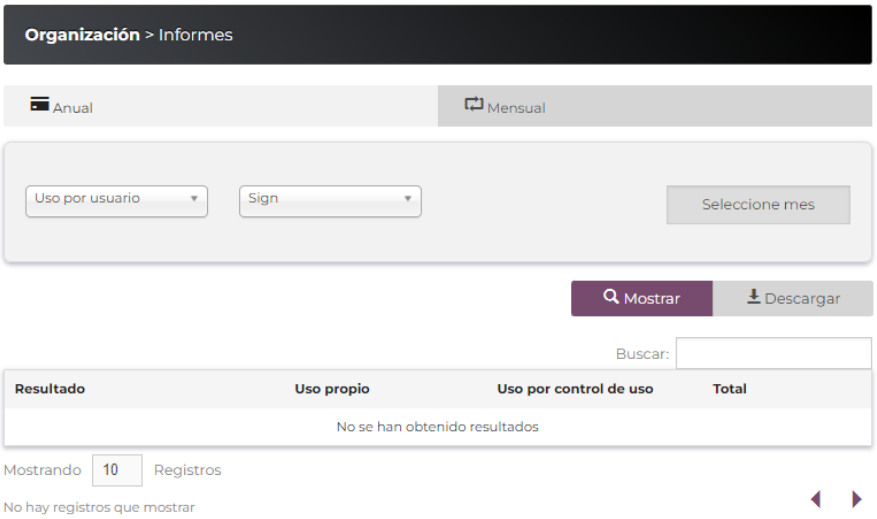
The reports will be displayed in list format and graphically, according to the selected filters. There are three types of filters (Illustration 91):

- Filters by type of use. The filter to be applied will be selected from the drop-down menu.
  - **Usage per user**. The results are displayed grouped by user.
  - **Use by certificate**. The results are shown grouped by certificate.
  - **Use per application**. The results are shown grouped by the application that has made use of the certificate.

- **Usage by URL**. The results are shown grouped by the url accessed with the certificates.

- Filter by action. Select the action on which you wish to consult its use.
- Filter by date. Select the month for which you wish to consult your usage.

Illustration 91. Filter reports



Click on Mostrar to display the result of the applied filters and Descargar to obtain a .csv file of the result.

Example of use by user (Illustration 92):

Illustration 92. Example of use

The results will be differentiated in:

- **Own use:** signatures made by the user himself, with his certificates.
- **Authorized use:** signatures made with authorized certificates through use control.

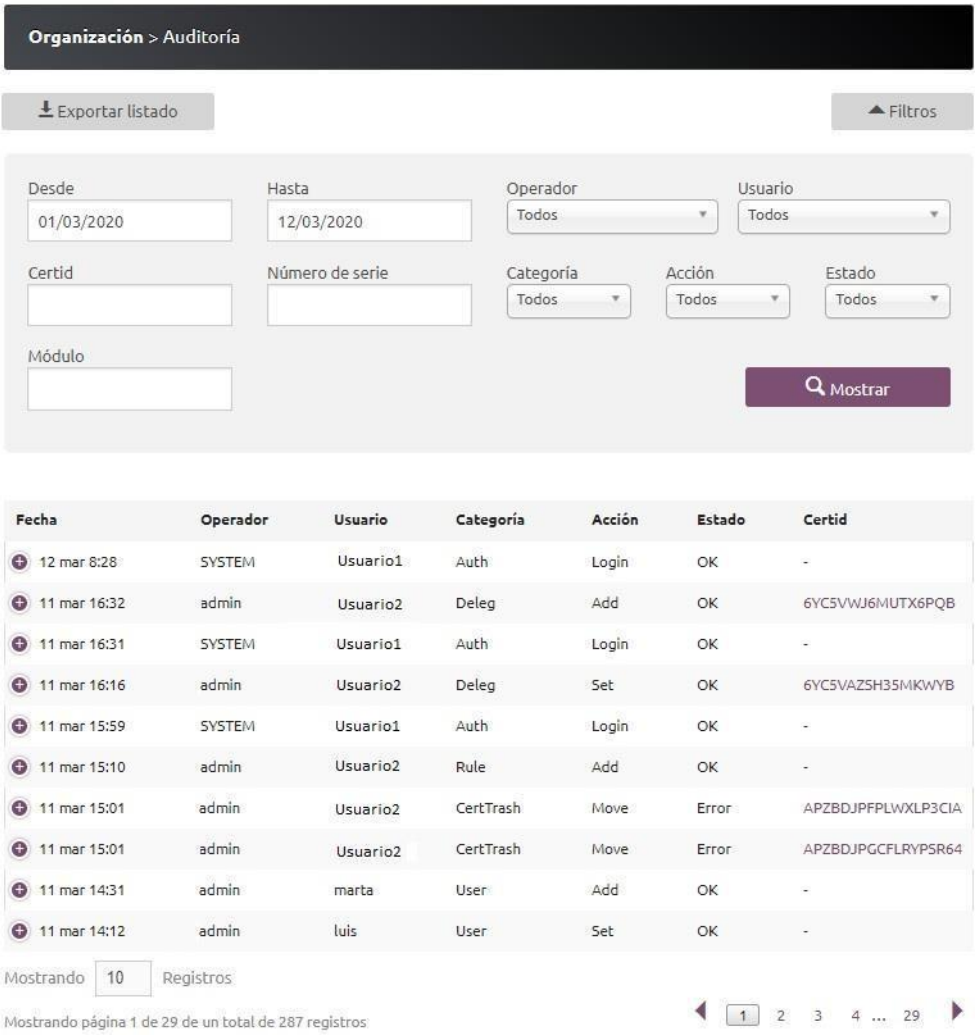
5.11 ORGANIZATION MENU - AUDIT

Allows to visualize all the actions, differentiated by type, performed with the centralized certificates of all the users of the organization.

Note: The actions of certificates that the user has installed on his own computer will not be displayed, only the actions performed with the centralized certificates.
In case of having the certificate installed in the equipment itself and also centralized in IvSign, the system itself will recover the key that you have locally, since the Serial Number and Fingerprint of the certificate are the same, so it is NOT recommended to have the certificate installed.

By default, the last 5 days and the actions of all users are displayed. It also allows filtering by a different date range and by a specific user.
First go to Filtros, select the user and indicate the date range, click on Mostrar to display the result of the applied filters on the screen, and Descargar to obtain a file, in .xml format, of the result (Figure 93).

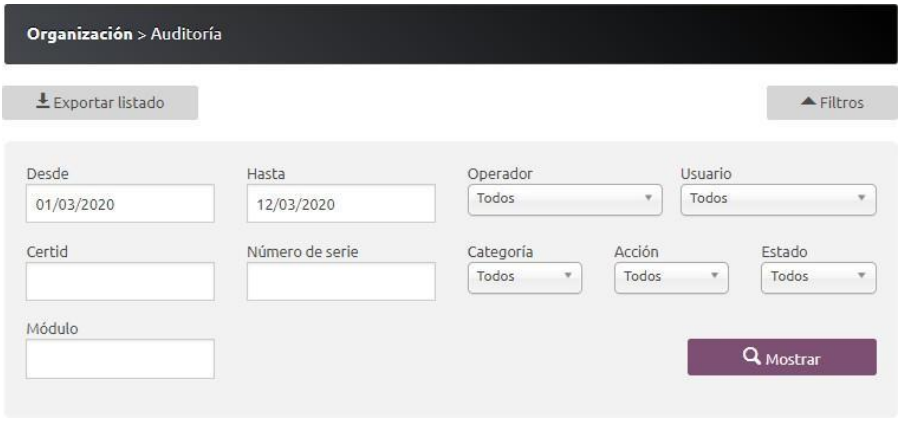
Illustration 93. Organization menu - Audit



The icon allows you to display the fields of each action that do not fit in the screen width. When clicked, it will display the list of non-visible fields and, to hide them again, click on the icon.

The **Filters** button allows you to display more fields by which you can filter for information (Figure 94).

Illustration 94. Audit filters



The actions to be audited are:

- Category: **Auth**. Related to the identification and access to the panel.
  - Shares:
    - Login: user access to the panel.
    - LoginToken: access of an application to the panel.
    - Impersonate: user impersonation (see point - Users).
- Category: **User**. Related to user management.
  - Shares:
    - Add: user creation.
    - Set: user modification.
    - Del: user deletion.
    - Ren: User renaming.
    - OrgaMove: Move user from one organization to another.
- Category: **Cert.** Related to certificate management.
  - Shares:
    - Set: certificate modification (status, change of name or description...)
    - Del: Definitively deletes a certificate.
    - Move: Move a certificate to the trash can.
    - PinCheck: Checks the certificate pin.
    - PinSet: Change of certificate pin.
    - ImportPFX: import certificate.
    - Generate (GenRSA, GenCSR, InstallCER): certificate generation.
    - Reflink: related external certificate (pkcs11).
    - Replace: Replaces a certificate with another certificate.

- Category: **Deleg** (Controls of use).
  - Shares:
    - Add: creation of usage control.
    - Set: modification of usage control.
    - Del: deletion of usage control.
    - AddCert: certificate is added to the usage control.
    - DelCert: Deletes a certificate from a usage control.
    - UserAdd: Add user to the usage control.
    - UserDel: Remove user from usage control.
- Category: **Rule** (rules of use)
  - Shares:
    - Add: creation of usage rule.
    - Del: deletion of usage rule.
- Category: **Sign** (signature).
  - Shares:
    - RSA: web authentication and document signing.
- Category: **Notify** (notifications).
  - Shares:
    - Accept: Notifications that have been accepted.
    - Set: Notifications marked as read.
- Category: **Orga** ().
  - Shares:
    - Add: Organizations that have been added.
    - From: Organizations that have been eliminated
    - Ren: Organizations that have been renamed
    - Set: Modification of the description field.
- Category: **Rule** .
  - Shares:
    - Add: Add a usage rule to a usage control or certificate.
    - Del: Delete a usage rule to a usage control or certificate.
- Category: **Signature** .
  - Shares:
    - Cades: CMS (Cryptographic message syntax) document signature.
    - Pades: Signature of PDF documents (PDF advanced electronic signature).
    - Xades: XML advanced electronic signature (XML advanced electronic signature).
    - TimestampPDF: Inclusion of time stamp in PDF document.
- Category: **TSP** ().
  - Shares:
    - Verify: Verify a time stamp protocol.

        - Sign: Signature with a time stamp (Time stamp protocol).
- Category: **Verify** ().
    - Shares:
        - TSP: Validates a time stamp protocol.
        - Pades: Validates a PDF document signature (PDF advanced electronic signature).
        - Xades: Validates an XML document signature (XML advanced electronic signature).
        - Cades: Validates a CMS (Cryptographic message syntax) document signature.
        - Cert: Validates a Keyman certificate.
        - CER: validates the public key of a certificate.
    - Category: CertTrash:
        - Shares:
            - Del: Permanently delete the certificate from the certificate trash.
            - Rest: Restores a certificate from the Certificate Bin.

6. HELP MENU

User manuals are available for download from the **Help** menu.