



TAREA PSP06

Módulo de Programación de Servicios y Procesos en modalidad a distancia
del I.E.S. Augusto González de Linares.



24 DE ENERO DE 2023
DIEGO GONZÁLEZ GARCÍA

Índice

1. Firmar digitalmente la aplicación..... 2
2. Que sólo pueda leer los datos del directorio c:/datos..... 6

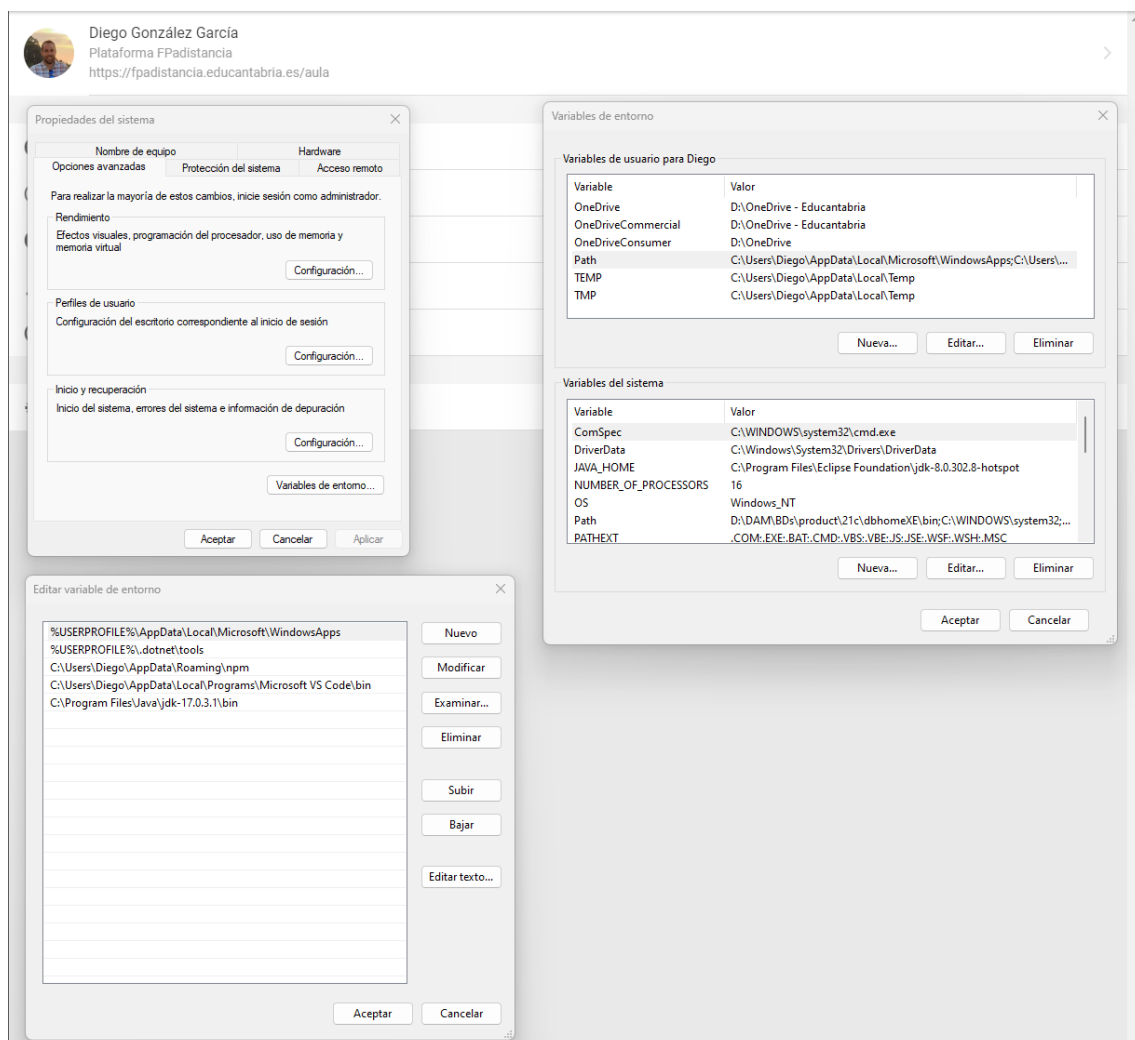
Enunciado.

Utilizando la aplicación desarrollada en la actividad anterior, configura las políticas de acceso para (muestra en un pdf con imágenes y comentarios los pasos realizados), también entrega los proyectos y ficheros usados en la tarea.

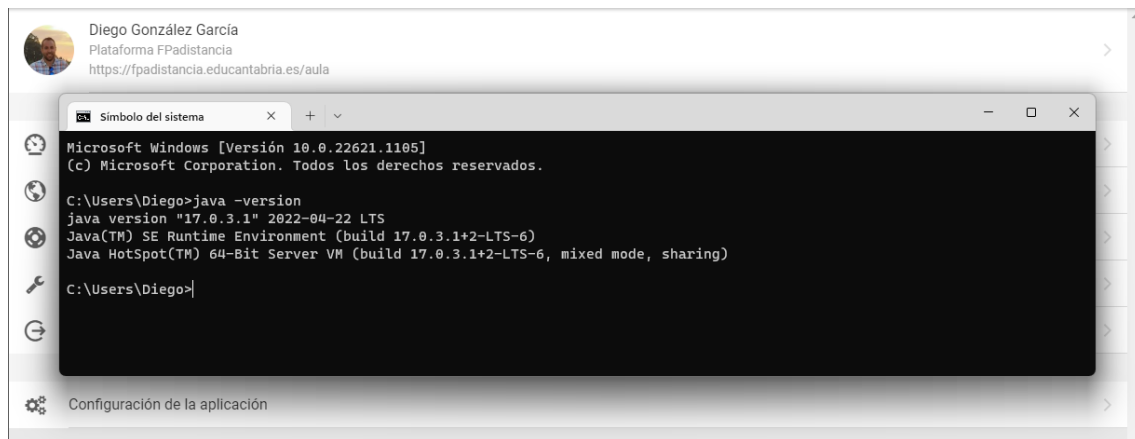
***En las imágenes del pdf debe aparecer el nombre del alumno para su identificación.

1. Firmar digitalmente la aplicación.

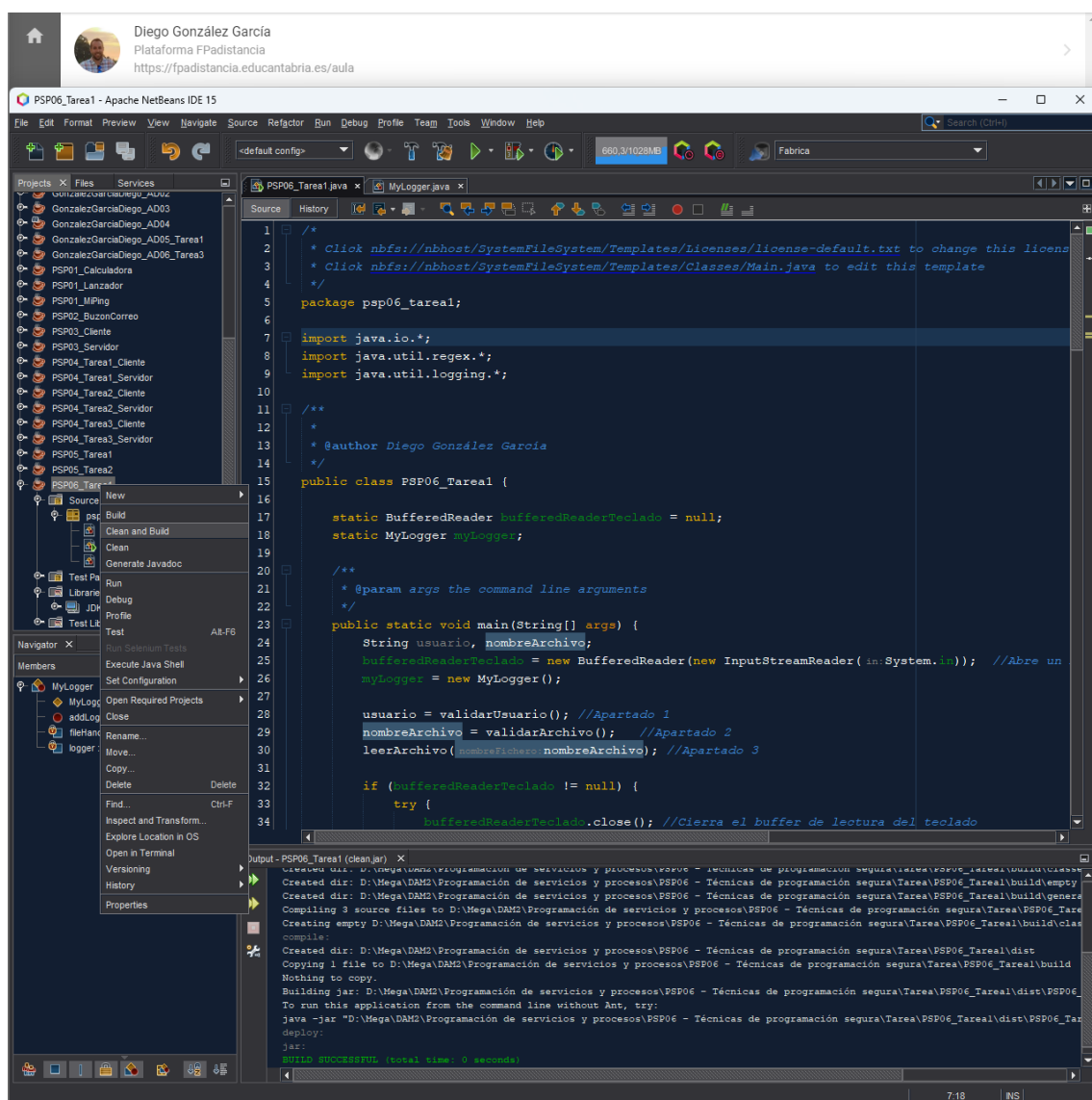
1. Comprobamos que tenemos bien configuradas las variables de entorno para la ruta de JAVA.



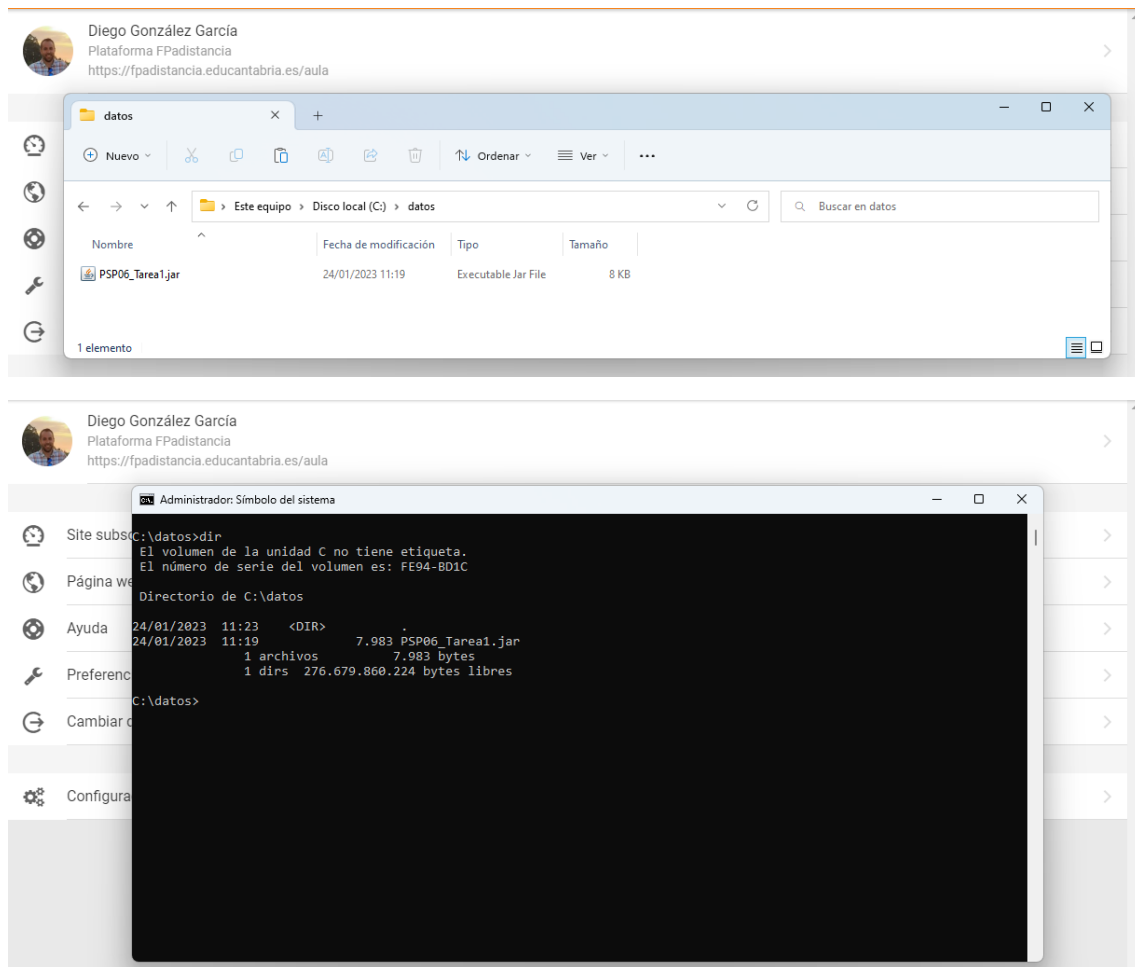
2. Verificamos que todo está correcto ejecutando en un terminal el comando `java -version`.



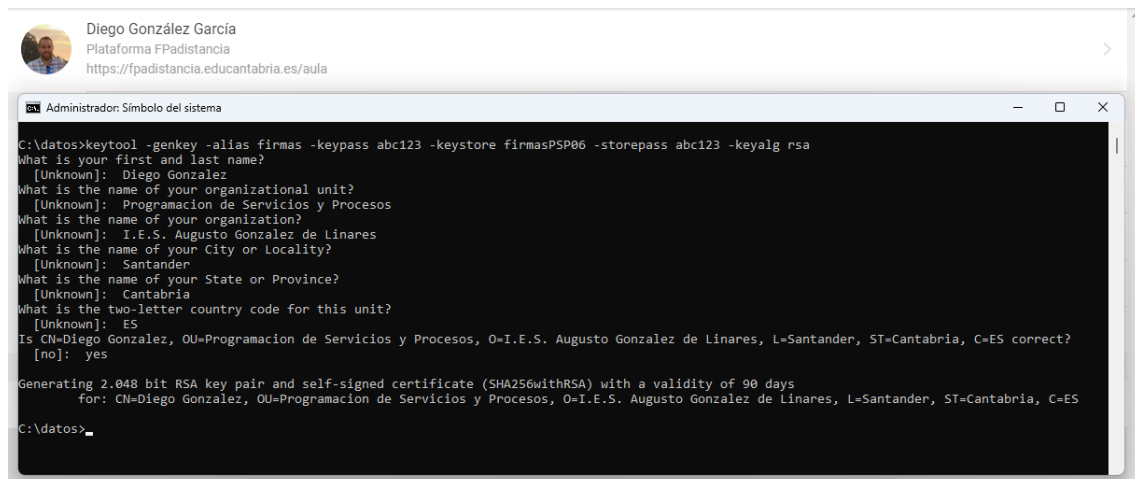
3. Obtenemos el archivo *.jar* del proyecto compilándolo desde *NetBeans*. Este nos aparecerá en una carpeta llamada *dist*, que se encontrará dentro de la carpeta del proyecto.



4. Copiamos el archivo generado a la ruta especificada en el enunciado, *c:\datos*.



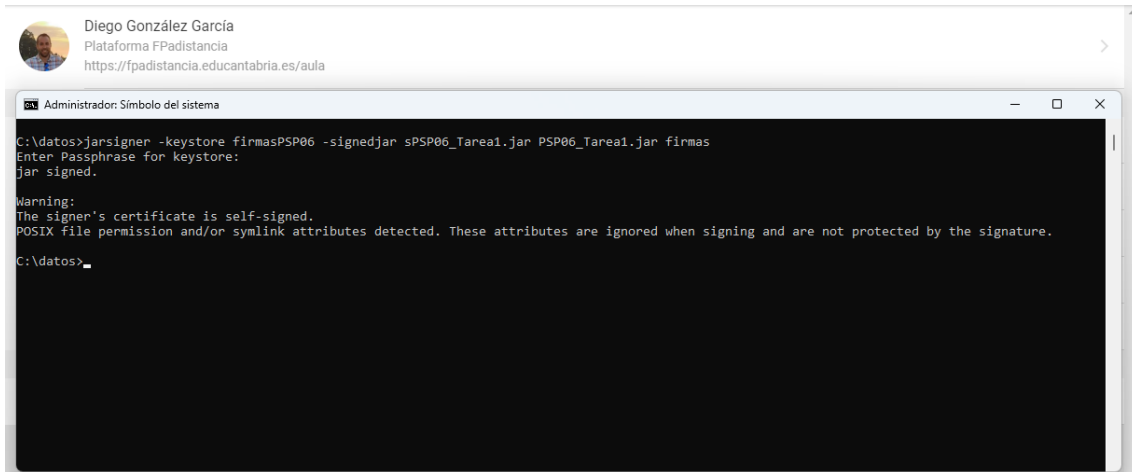
5. Creamos el archivo de certificado.



- **-alias** Indica el alias que se va a utilizar para referirnos al keystore, que es donde se van a almacenar las llaves generadas.
- **-keypass** indica la contraseña de la llave privada.
- **-keystore** indica el keystore que se está creando.
- **-storepass** indica la contraseña del keystore.
- **-keyalg** indica el tipo de algoritmo a utilizar.

Tras esto nos pide contestar a unas preguntas y al finalizar confirmamos con un **yes**.

6. Firmamos digitalmente nuestra aplicación con el certificado creado.



```
Diego González García
Plataforma FPadistancia
https://fpadistancia.educantabria.es/aula

Administrador: Símbolo del sistema

C:\datos>jarsigner -keystore firmasPSP06 -signedjar sPSP06_Tarea1.jar PSP06_Tarea1.jar firmas
Enter Passphrase for keystore:
jar signed.

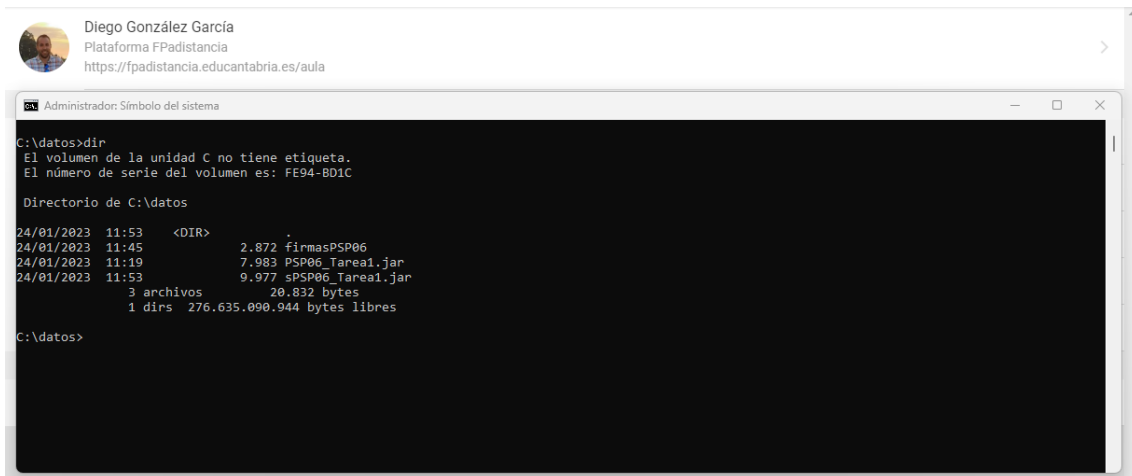
Warning:
The signer's certificate is self-signed.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when signing and are not protected by the signature.

C:\datos>
```

- *-keystore* indica el keystore creado anteriormente.
- *-signedjar* indica el nombre del fichero firmado.
- A continuación, se indica el fichero a firmar.
- Por último, se indica el alias que se ha creado anteriormente para referirnos al keystore.

Tras esto nos solicita la contraseña creada anteriormente y a continuación firma el archivo solicitado.

7. Comprobación de los ficheros generados con el comando *dir*.



```
Diego González García
Plataforma FPadistancia
https://fpadistancia.educantabria.es/aula

Administrador: Símbolo del sistema

C:\datos>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: FE94-BD1C

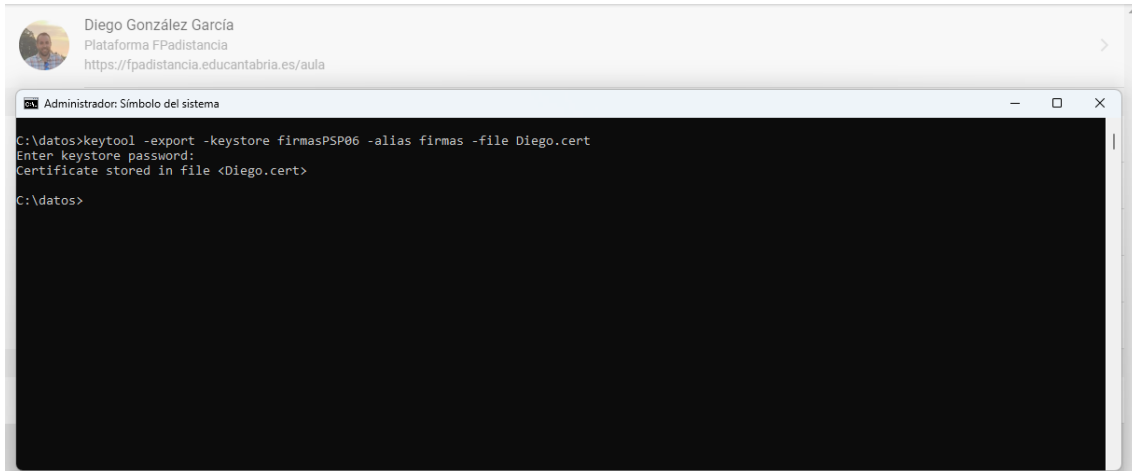
Directorio de C:\datos

24/01/2023  11:53    <DIR>          .
24/01/2023  11:45                2.872  firmasPSP06
24/01/2023  11:19                7.983  PSP06_Tarea1.jar
24/01/2023  11:53                9.977  sPSP06_Tarea1.jar
               3 archivos                28.832 bytes
               1 dirs  276.635.090.944 bytes libres

C:\datos>
```

Podemos ver como en nuestro directorio ya tenemos nuestro fichero .jar original (PSP06_Tarea1.jar), el archivo .jar firmado (sPSP06_Tarea1.jar) y el contenedor de firmas (firmasPSP06).

8. Exportamos la llave pública del certificado ejecutando.



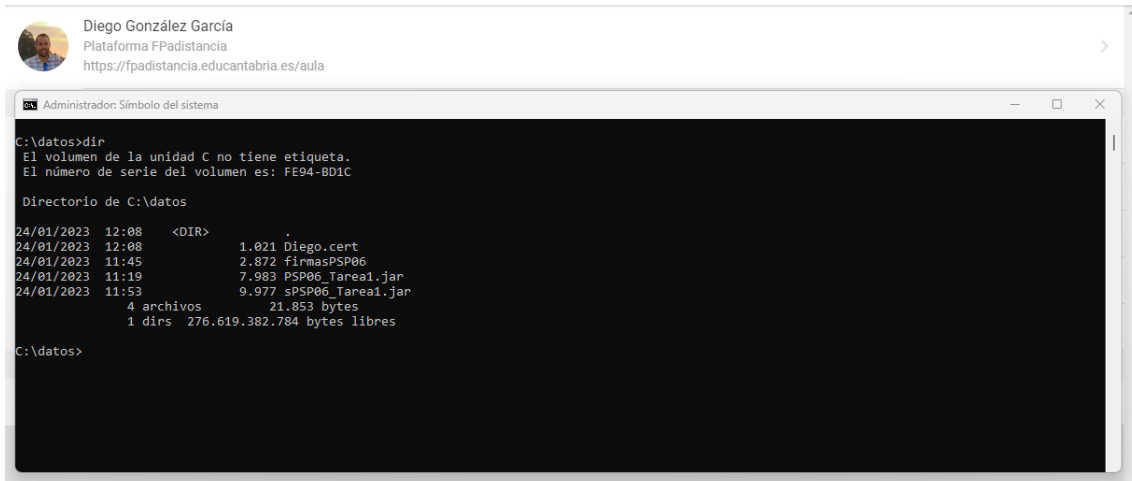
```
Administrador: Símbolo del sistema

C:\datos>keytool -export -keystore firmasPSP06 -alias firmas -file Diego.cert
Enter keystore password:
Certificate stored in file <Diego.cert>

C:\datos>
```

- *-keystore* indica el keystore creado anteriormente.
- *-alias* indica el alias que se ha creado anteriormente para referirnos al keystore.
- *-file* indica el nombre del certificado que vamos a crear.

9. Comprobación de los ficheros generados con el comando *dir*.



```
Administrador: Símbolo del sistema

C:\datos>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: FE94-8D1C

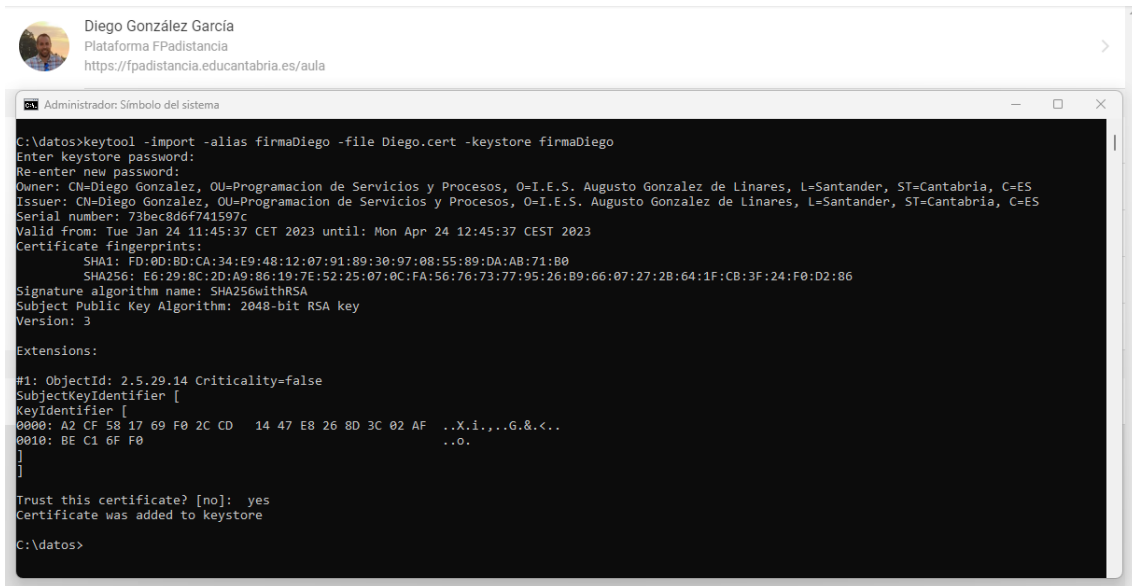
Directorio de C:\datos

24/01/2023  12:08    <DIR>          .
24/01/2023  12:08                1.021 Diego.cert
24/01/2023  11:45                2.872 firmasPSP06
24/01/2023  11:19                7.983 PSP06_Tarea1.jar
24/01/2023  11:53                9.977 sPSP06_Tarea1.jar
               4 archivos                21.853 bytes
               1 dirs  276.619.382.784 bytes libres

C:\datos>
```

2. Que sólo pueda leer los datos del directorio c:/datos.

1. Importar el certificado.



```
C:\datos>keytool -import -alias firmaDiego -file Diego.cert -keystore firmaDiego
Enter keystore password:
Re-enter new password:
Owner: CN=Diego Gonzalez, OU=Programacion de Servicios y Procesos, O=I.E.S. Augusto Gonzalez de Linares, L= Santander, ST=Cantabria, C=ES
Issuer: CN=Diego Gonzalez, OU=Programacion de Servicios y Procesos, O=I.E.S. Augusto Gonzalez de Linares, L= Santander, ST=Cantabria, C=ES
Serial number: 73bec8d6f741597c
Valid from: Tue Jan 24 11:45:37 CET 2023 until: Mon Apr 24 12:45:37 CEST 2023
Certificate fingerprints:
  SHA1: FD:0D:BD:CA:34:E9:48:12:07:91:89:30:97:08:55:89:DA:AB:71:B0
  SHA256: E6:29:8C:2D:A9:86:19:7E:52:25:07:0C:FA:56:76:73:77:95:26:B9:66:07:27:2B:64:1F:CB:3F:24:F0:D2:86
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

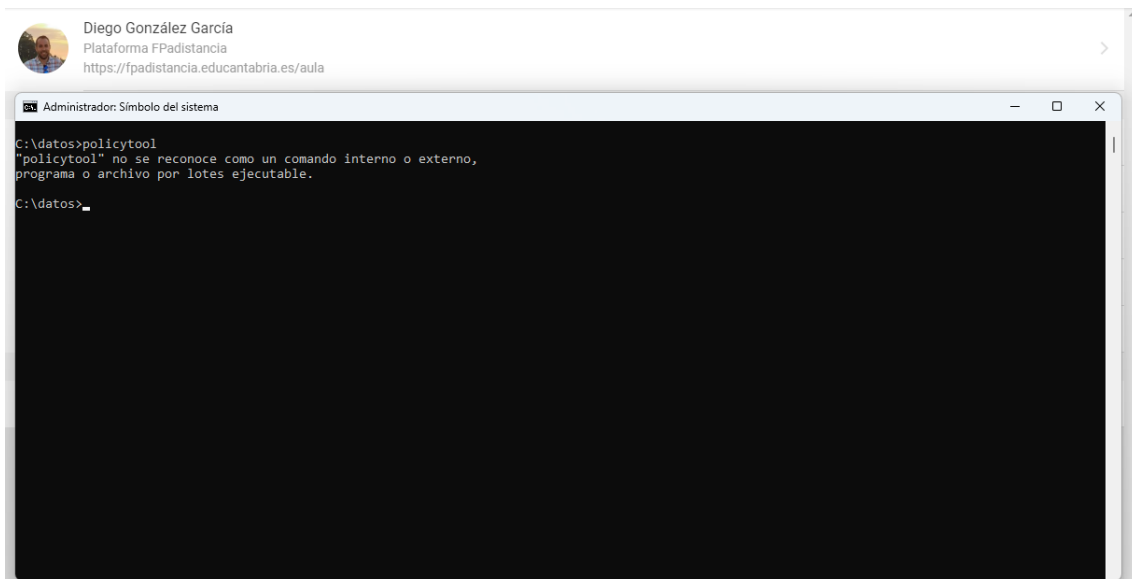
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A2 CF 58 17 69 F0 2C CD 14 47 E8 26 8D 3C 02 AF ..X.i,...G.&.<..
0010: BE C1 6F F0 ..O.
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore

C:\datos>
```

- *-alias* Indica el alias que se va a utilizar para referirnos al certificado importado.
- *-file* indica el nombre del certificado que vamos a usar.
- *-keystore* indica el keystore donde se guarda el certificado.
- Tras esto nos pide introducir una contraseña para el keystore por duplicado y al finalizar confirmamos con un yes.

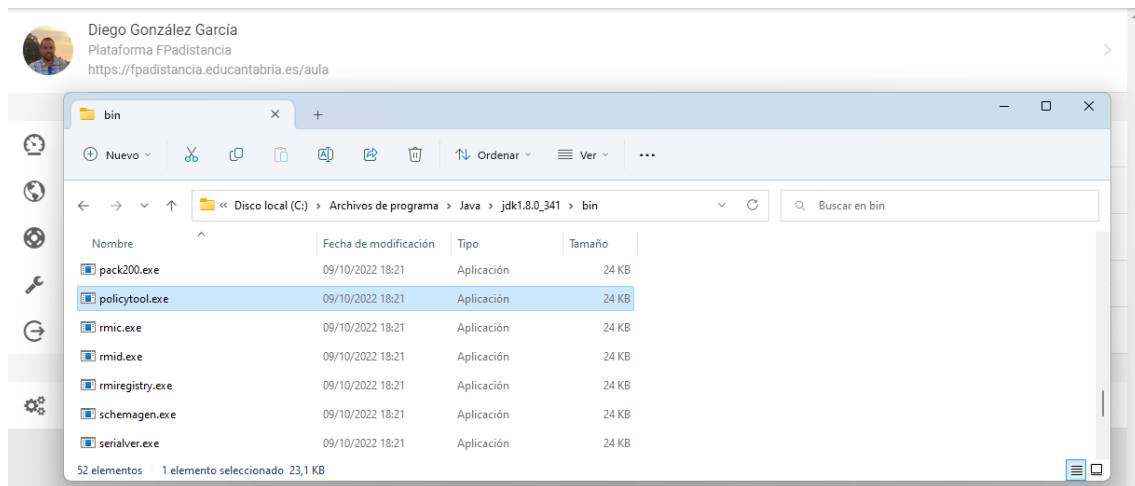
2. Abrir policytool.



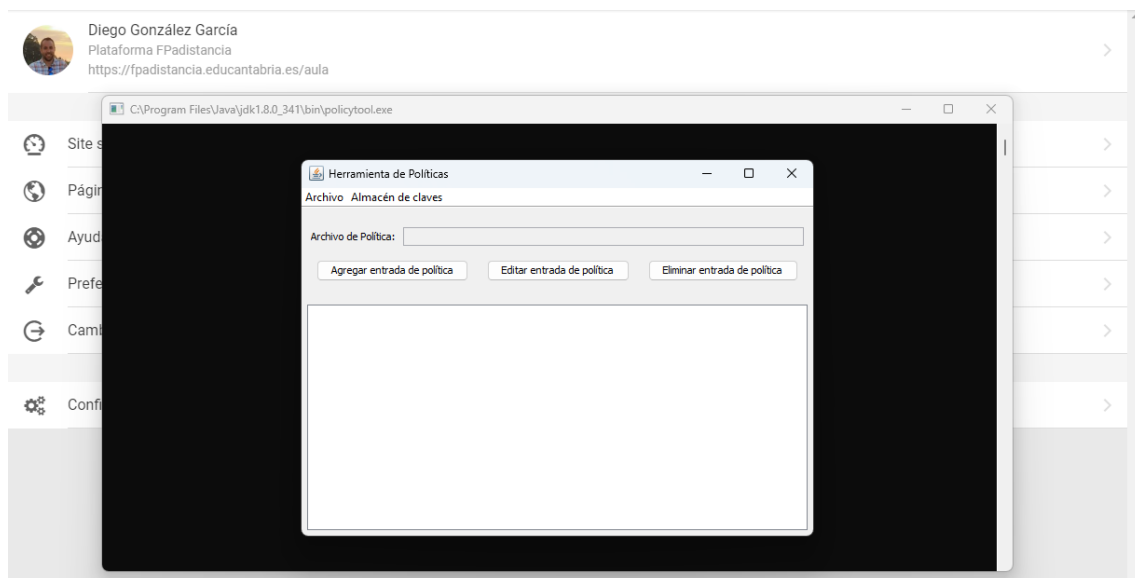
```
C:\datos>policytool
"policytool" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\datos>
```

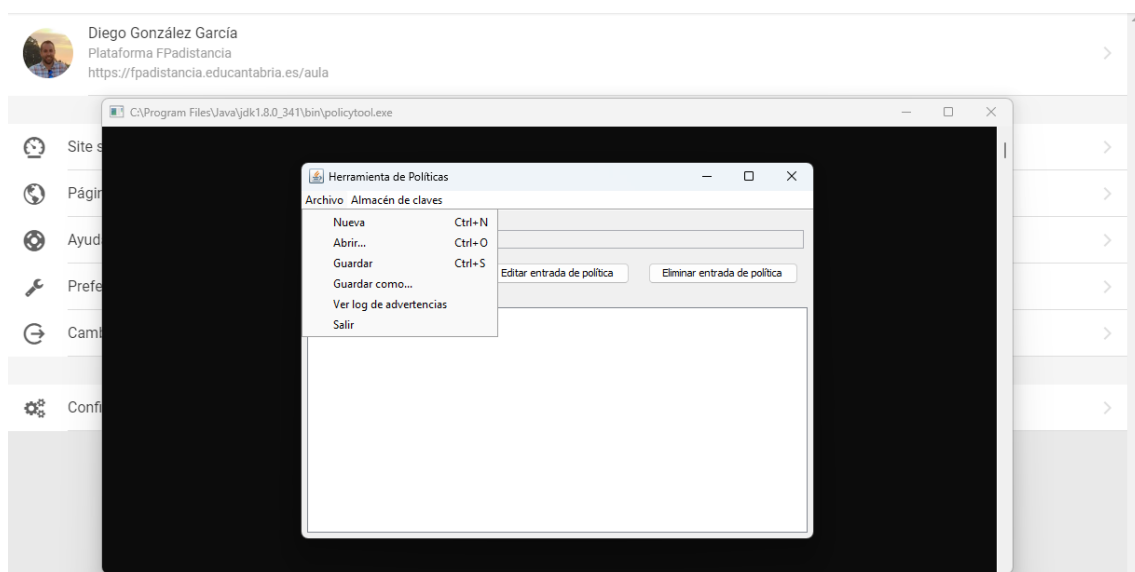
Si intentamos ejecutarlo por comando, nos da un error que es debido a que el JDK que estamos utilizando no contiene esta herramienta.

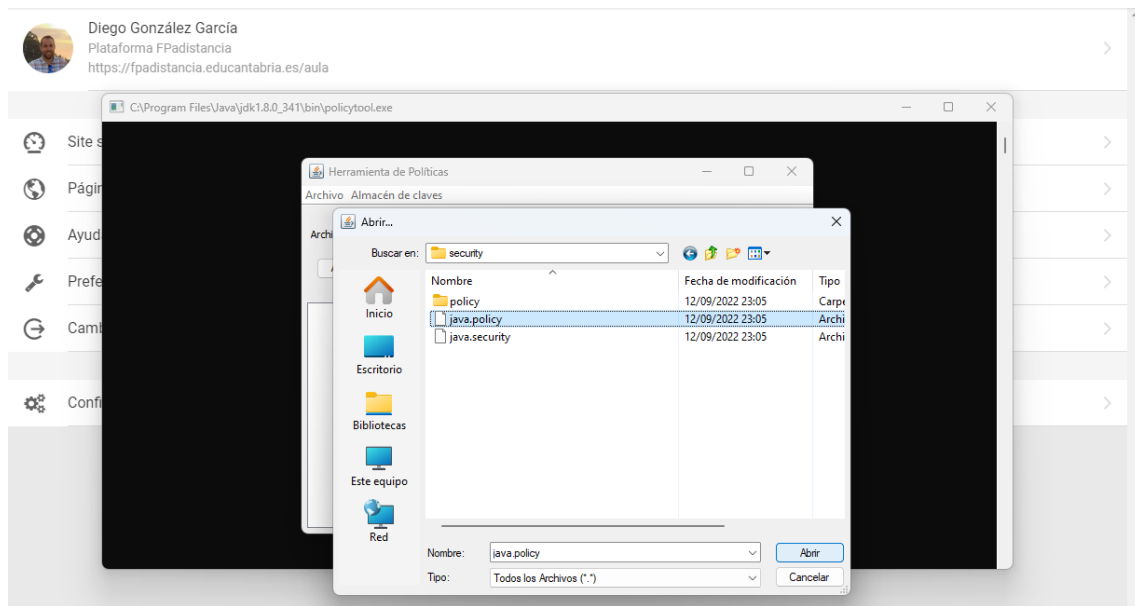


Como tengo diferentes versiones de JDK instaladas en mi sistema, me voy a la versión 1.8 que si incluye esta herramienta y la ejecuto como administrador.

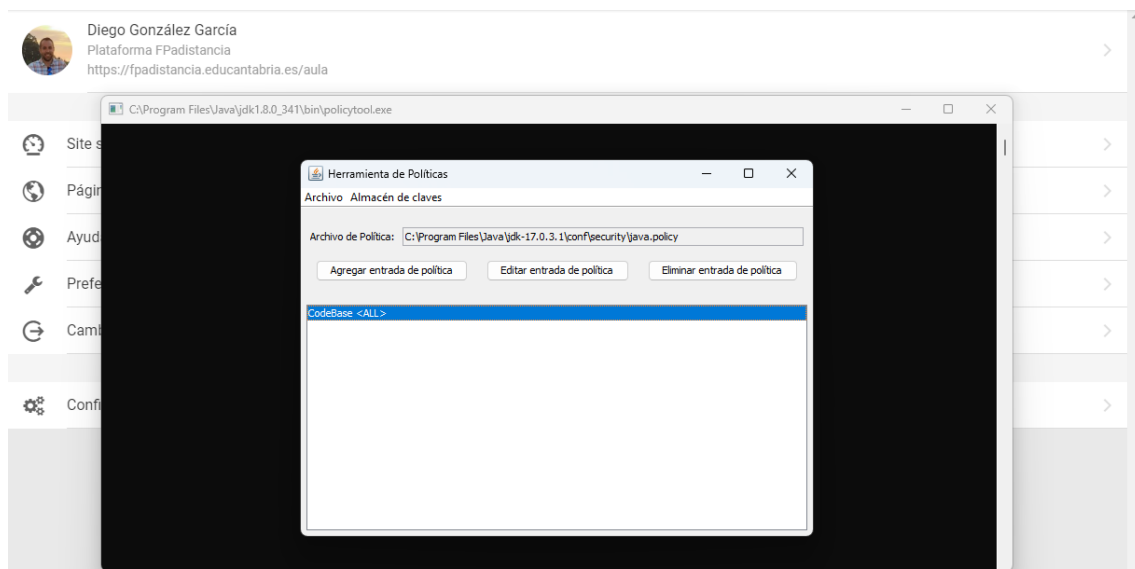


3. Abrir el archivo de políticas de seguridad.

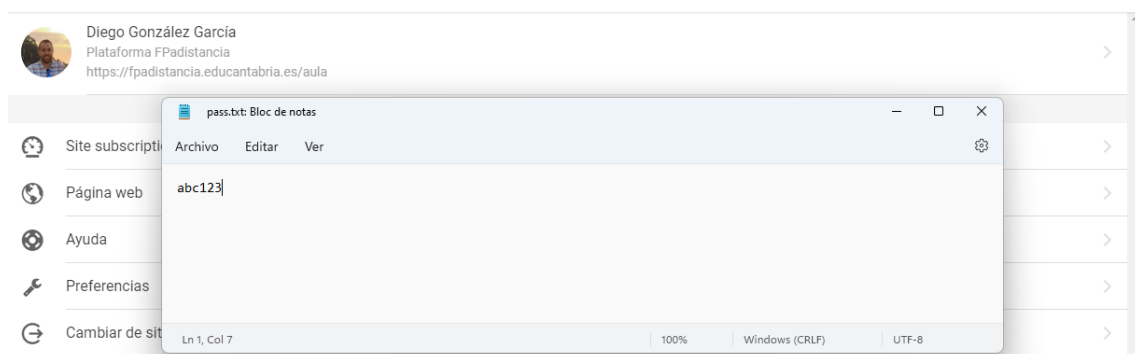




Abro el archivo `java.policy` que tengo en el JDK que he usado desde el comienzo de la tarea, la versión 17. En mi caso, se encuentra en la ruta `C:\Program Files\Java\jdk-17.0.3.1\conf\security`.

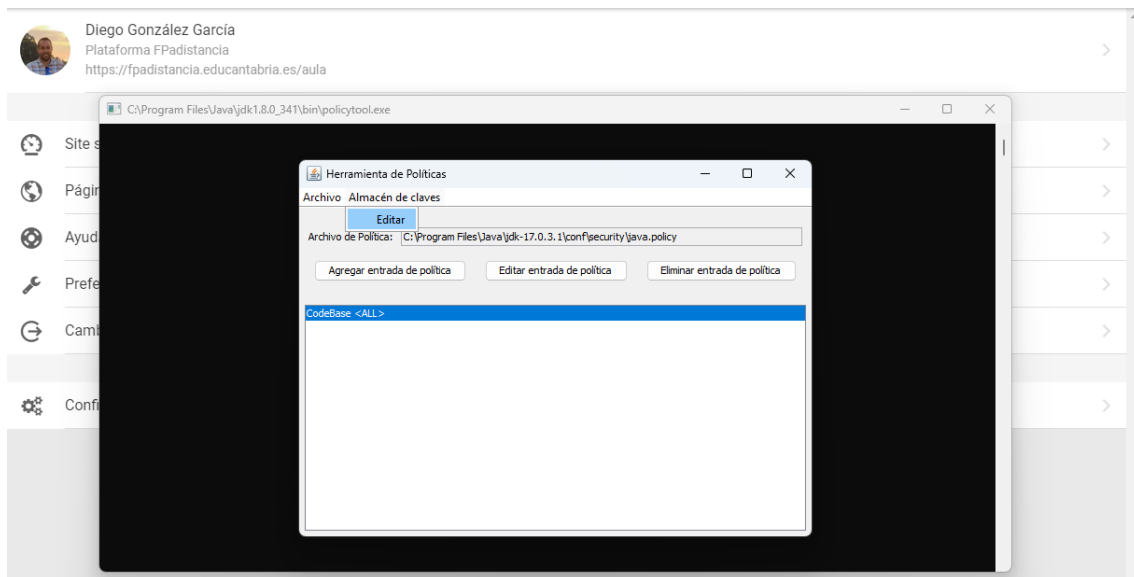


4. Crear archivo de contraseña.

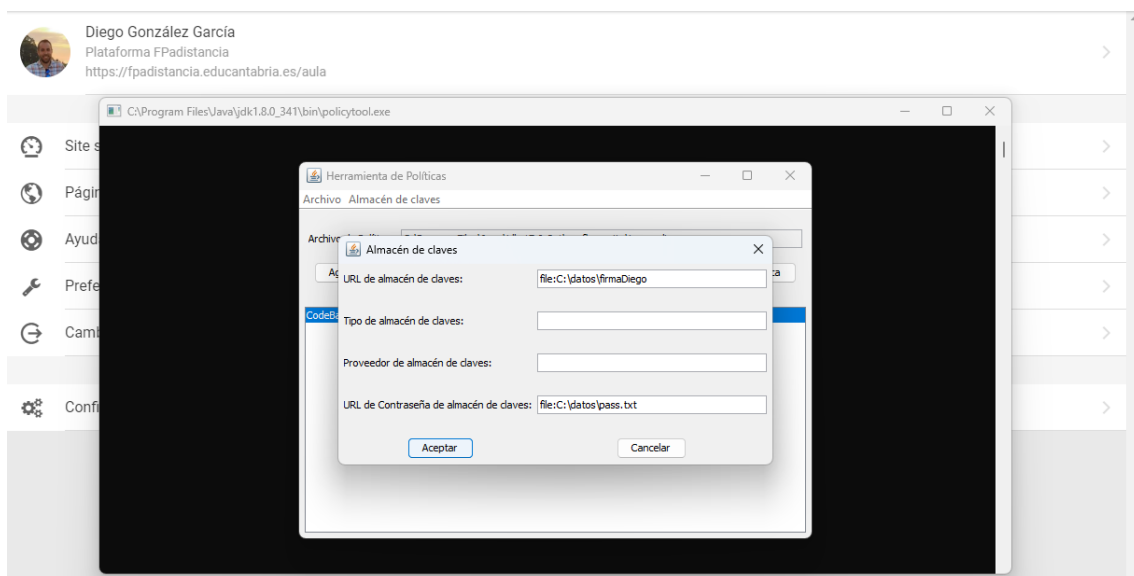


Para poder especificar la contraseña del keystore, es necesario escribirla en un archivo para posteriormente indicar su ruta. En mi caso he creado un archivo `pass.txt` en el mismo directorio.

5. Indicar el keystore que vamos a utilizar.

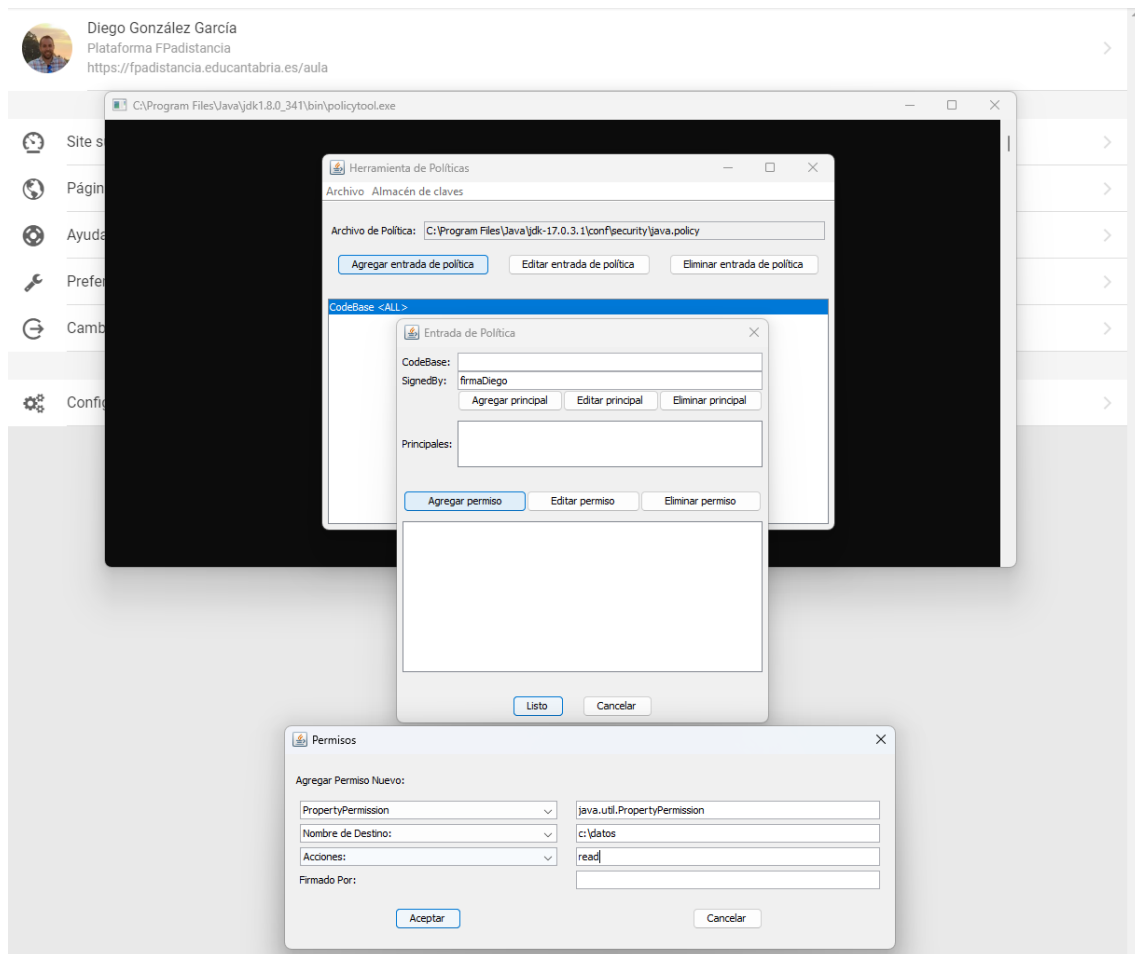


Desde el menú *Almacén de claves*, lo editamos.



Indicamos las rutas del almacén de claves y del archivo de contraseña. Pulsamos *Aceptar*.

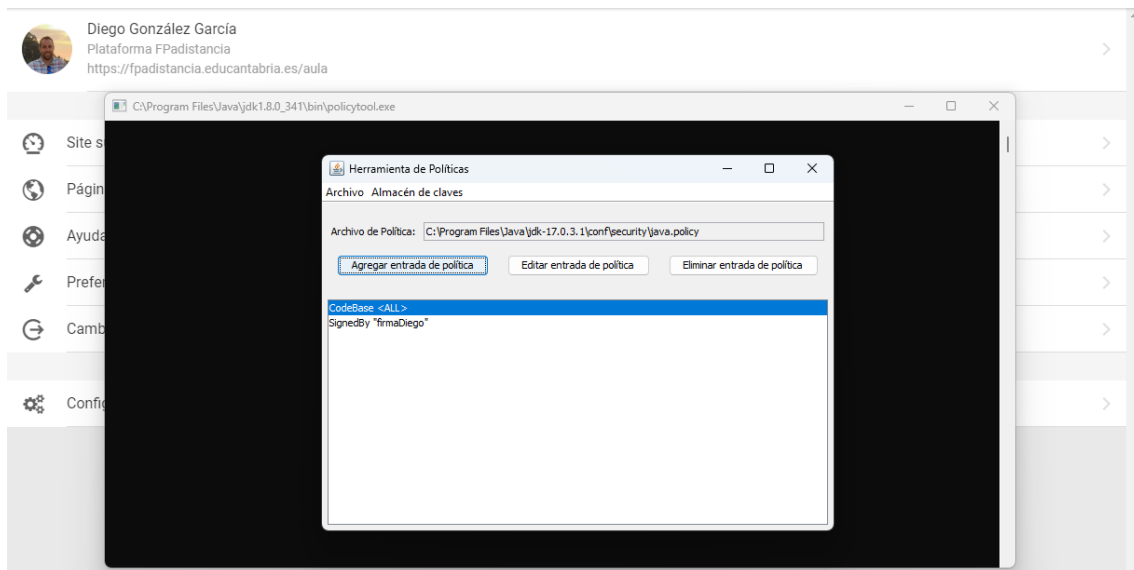
6. Agregar política de seguridad.



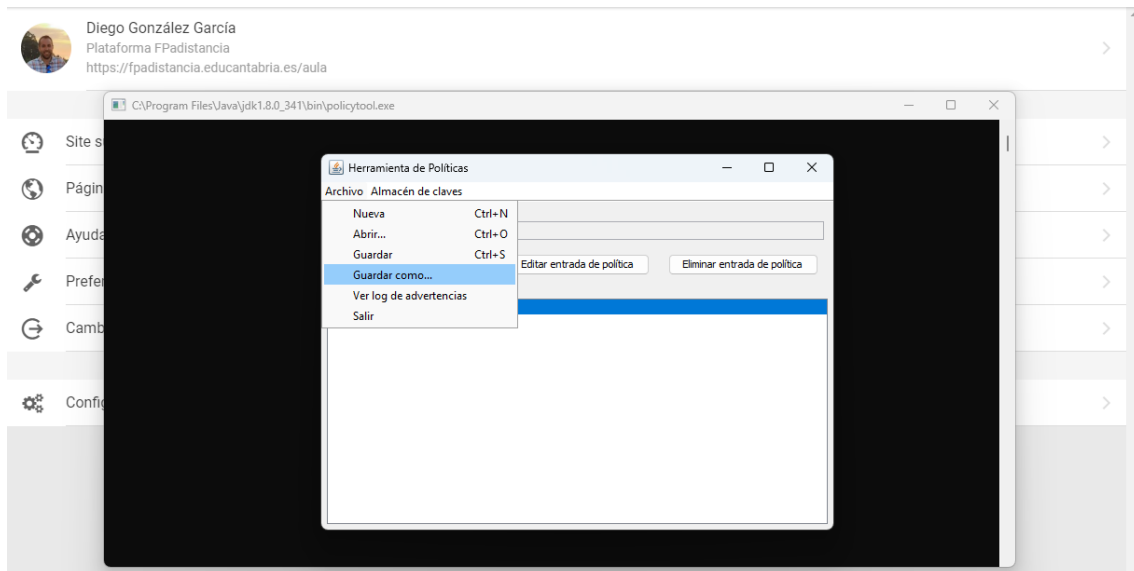
Pulsamos sobre *Agregar entrada de política*, a continuación, en la siguiente pantalla sobre *Agregar permiso* y en esta última, rellenamos los datos necesarios para conceder los permisos solicitados.

En nuestro caso, queremos permitir que los ficheros firmados con nuestra firma puedan acceder al directorio `c:\datos` y leer sus datos.

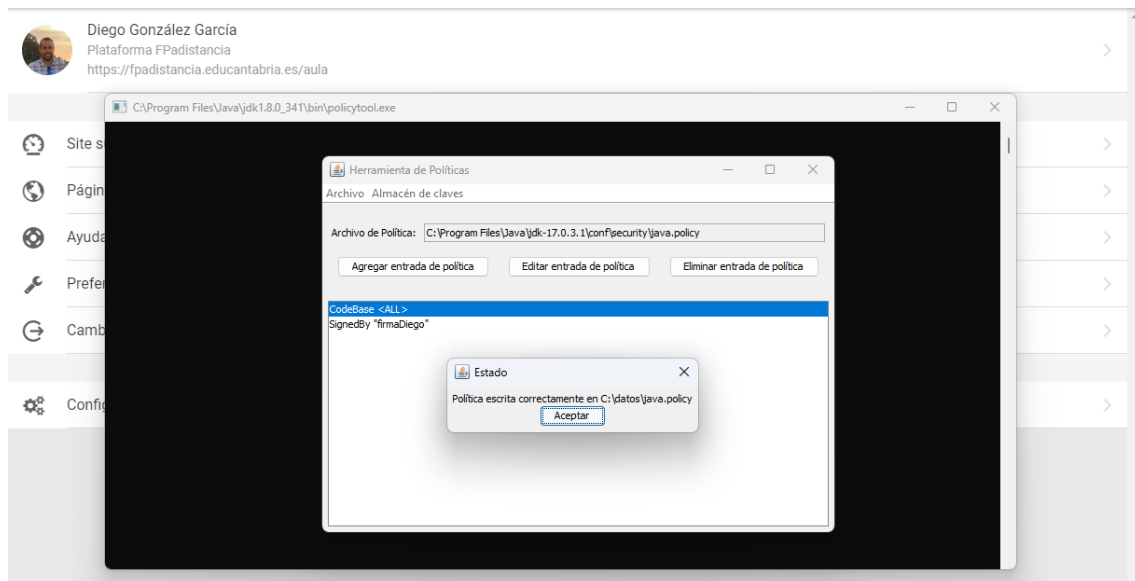
Muy importante, en la ventana de *Entrada de Política*, en el apartado *SignedBy*, hay que indicar el alias con el que se ha importado el certificado, en mi caso *firmaDiego*.



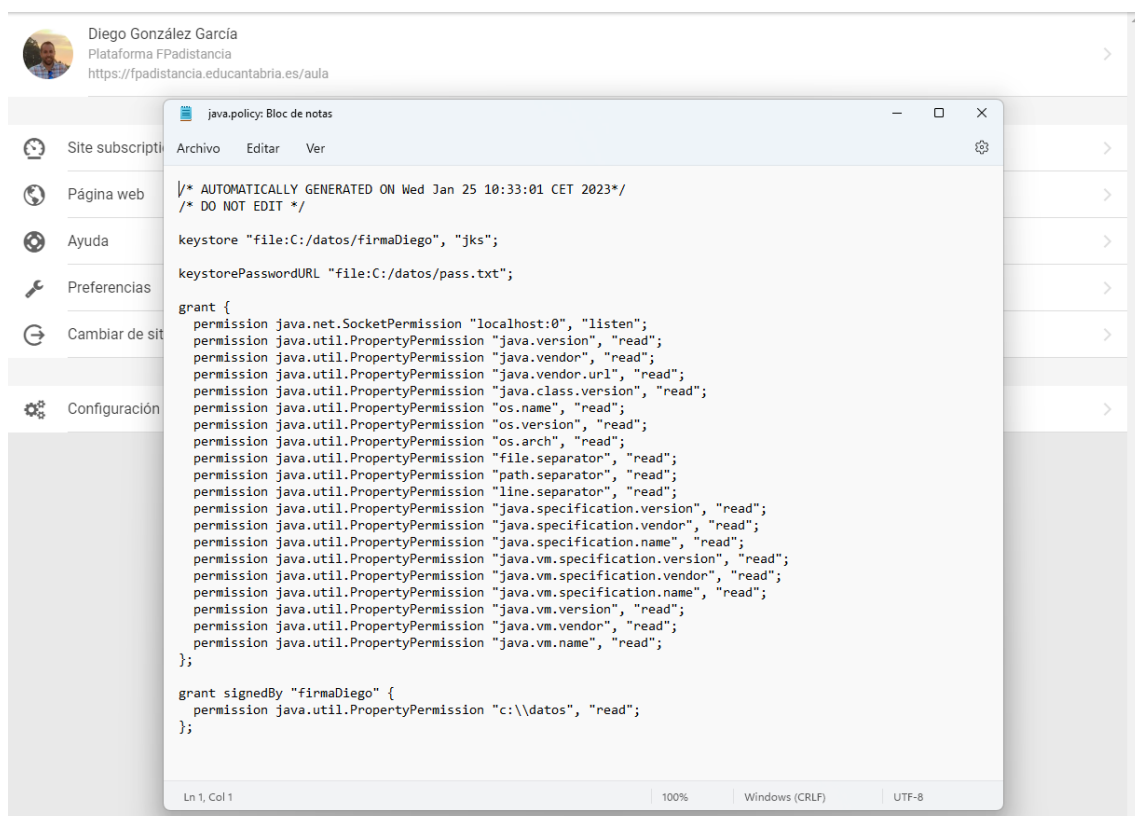
Una vez pulsado sobre *Aceptar* y *Listo*, en sus respectivas pantallas, ya podemos ver que aparece nuestra nueva entrada política.



Para finalizar, guardamos los cambios. En mi caso he preferido guardar el fichero en otro directorio (c:\datos) y no sobre escribir el fichero del JDK que estábamos modificando.



Tras esto, me confirma que se ha guardado correctamente. Ha partir de ahora, con la política que hemos creado, todos los proyectos firmados con este certificado podrán leer en el directorio *c:\datos*.



Para confirmarlo, abrimos el archivo *java.policy* y vemos como se ha añadido nuestra política al final del archivo.