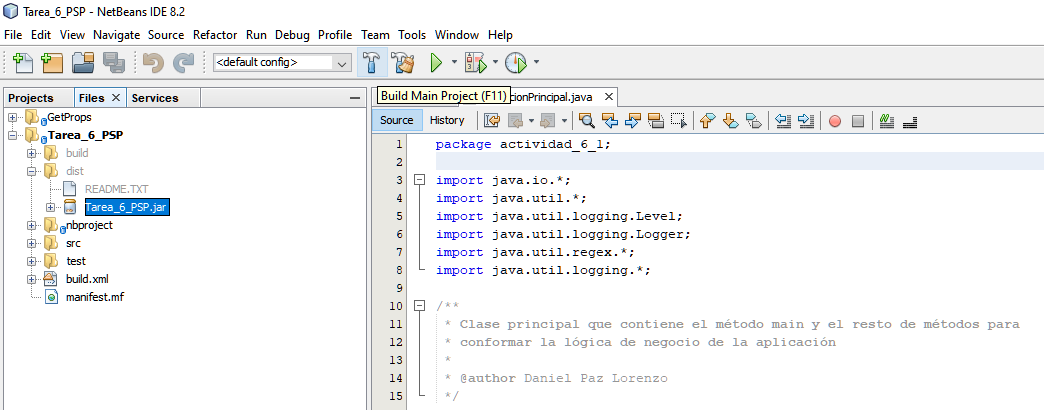
**ACTIVIDAD 6.1**

**ACTIVIDAD 6.2**

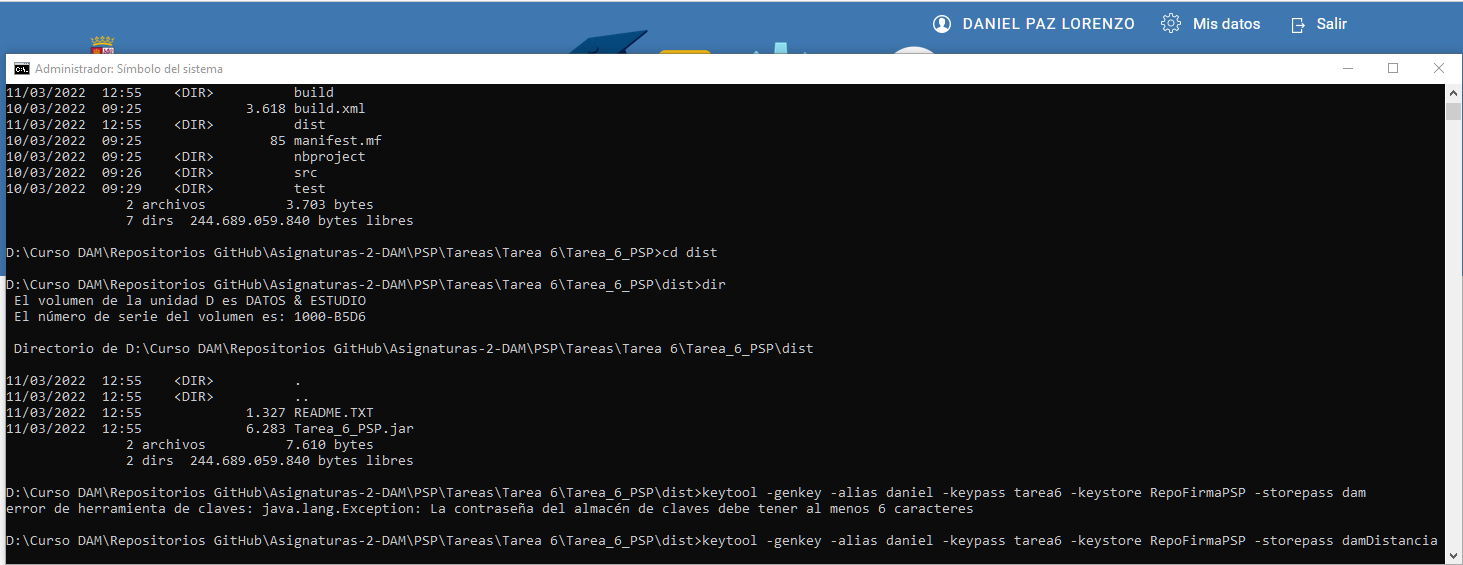
En este apartado se nos pide que utilizando la aplicación que hemos creado anteriormente, la firmemos digitalmente y que solo pueda leer los datos del directorio “c:/datos”.

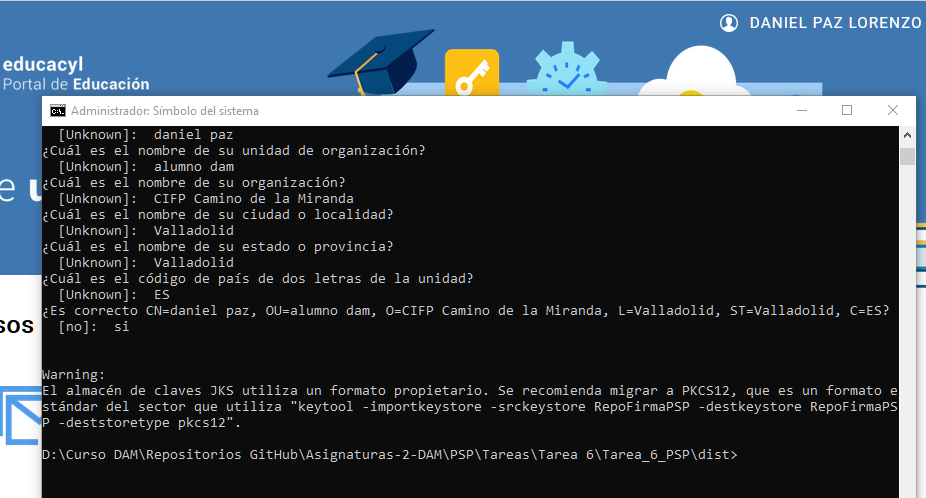
Comenzamos compilando la aplicación en NetBeans:



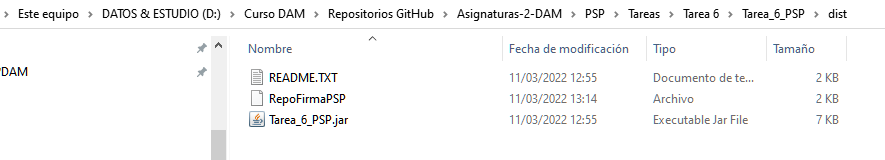
*Podemos ver en el navegador de la izquierda como se nos ha generado el paquete .jar*

A continuación, abrimos la consola de comandos de Windows en modo administrador, nos dirigimos al directorio del proyecto y generamos un par de claves (privada y pública) para firmar el fichero con el comando “keytool”:



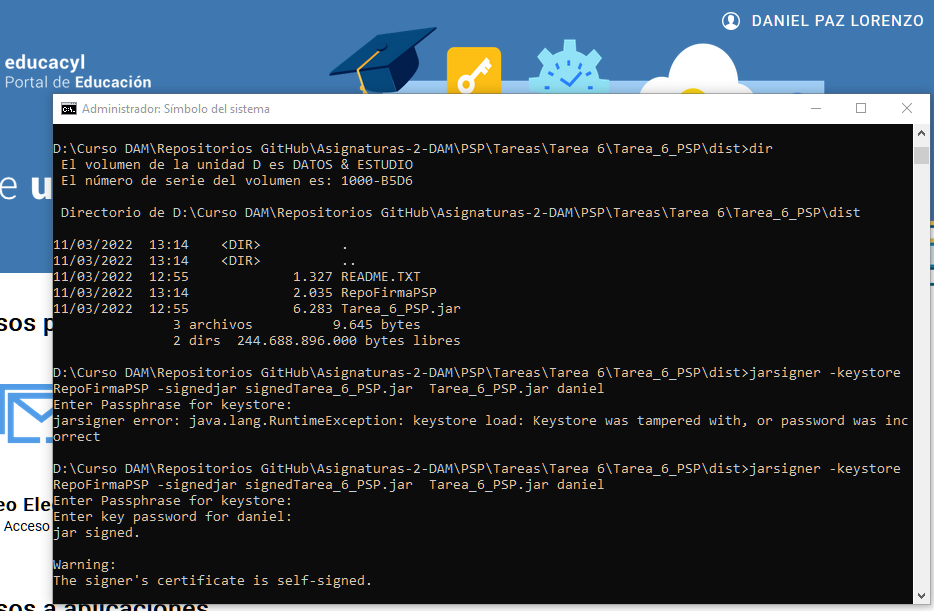


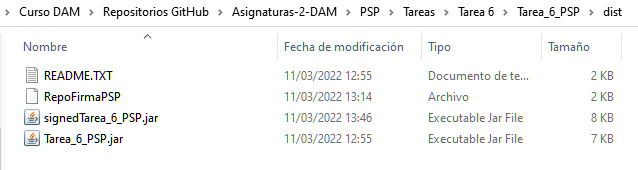
*Rellenamos los datos que nos van solicitando*



*Si entramos en el directorio ya vemos que se nos ha creado el almacenamiento de claves*

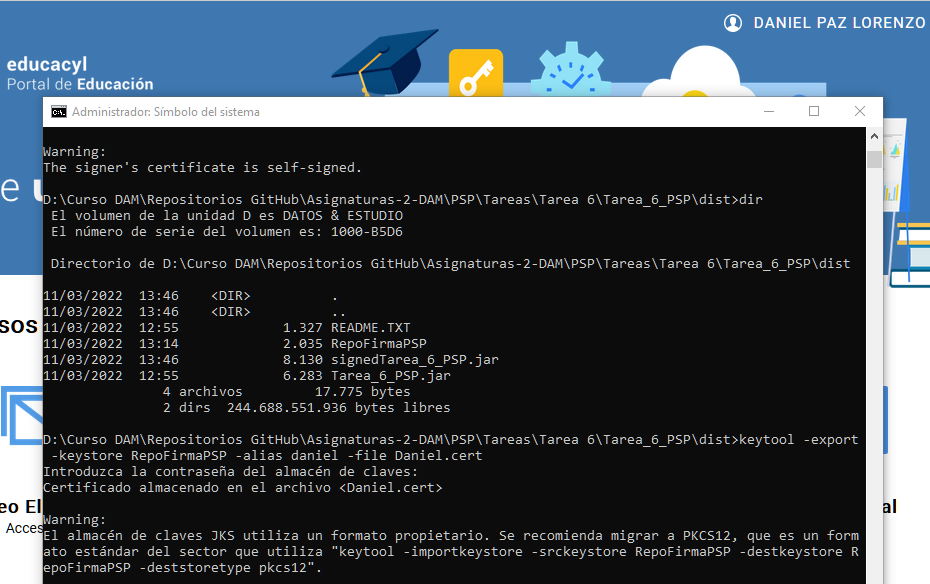
Por último, vamos a firmar la aplicación con el certificado que hemos creado con el comando “jarsigner”:



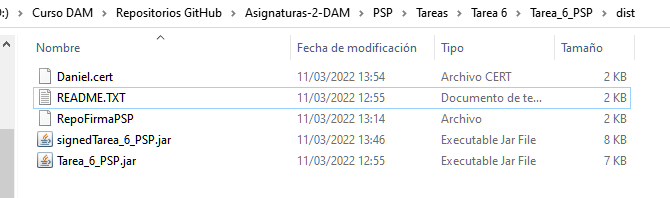


*Comprobamos que dentro del directorio se nos ha creado un nuevo paquete .jar ya firmado digitalmente*

Ya solo nos queda exportar la llave pública de nuestro certificado para que un usuario externo pueda utilizar la aplicación validando mi firma digital. Para ello utilizamos nuevamente el comando “keytool” con el atributo “-export” de la siguiente manera:

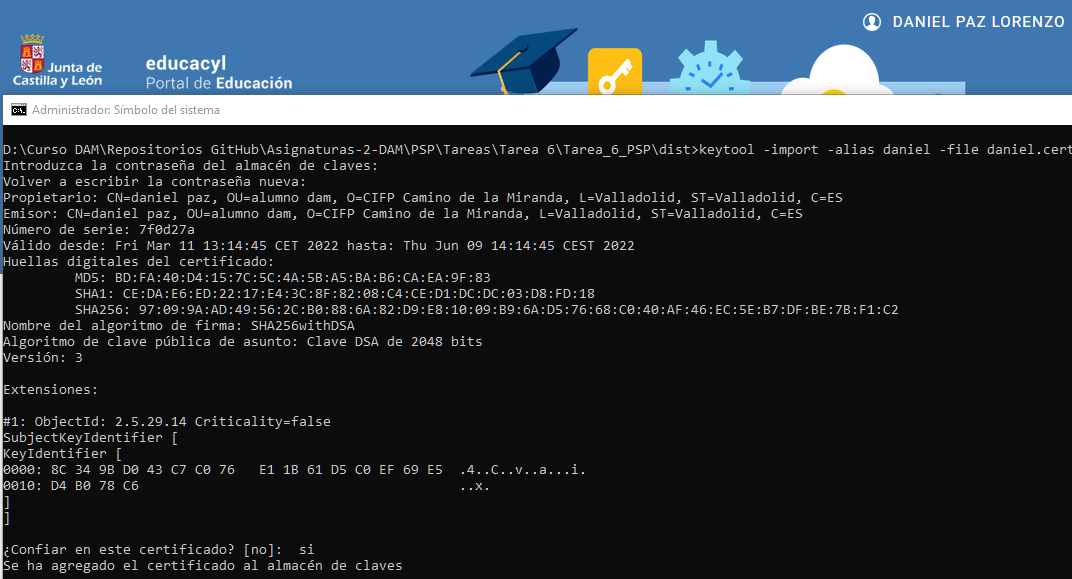


Volvemos al directorio para comprobar que se nos ha generado el certificado:



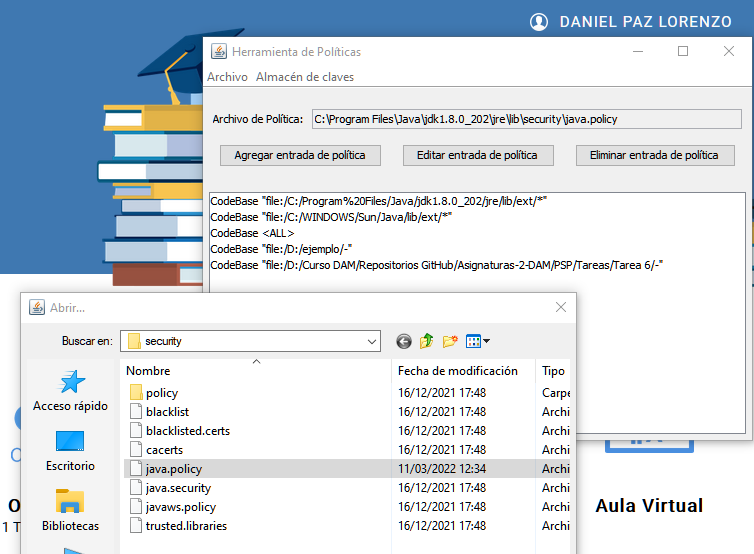
El siguiente apartado nos pide que la aplicación solo pueda leer los datos del directorio “c:/datos”, para ello tendremos que configurar la política de seguridad de nuestra aplicación firmada.

Lo primero que haremos será importar el certificado para validar la firma del fichero utilizando el comando “keytool -import”:

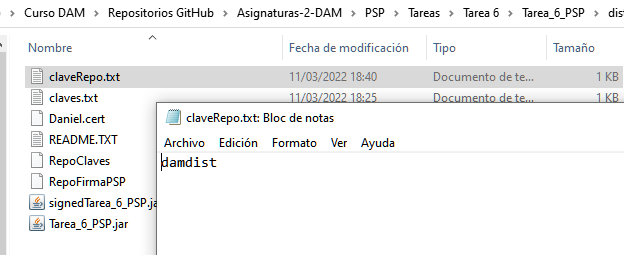


*Al ejecutar nos solicita contraseña para el nuevo almacén de claves creado*

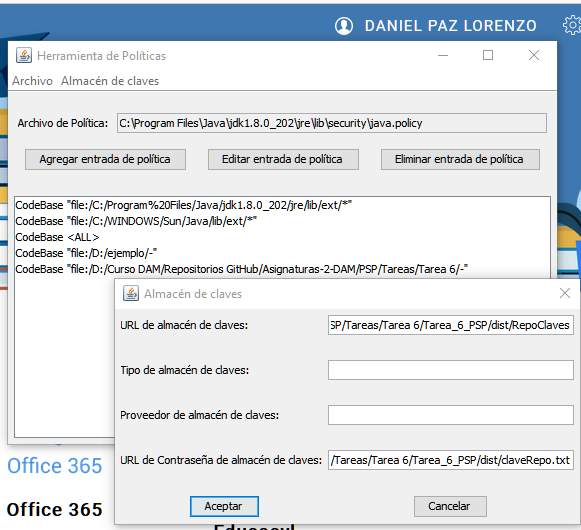
Pasamos a configurar la política de seguridad para que permita ejecutar el fichero firmado:



*Abrimos la herramienta policitytool, pulsamos Archivo->Abrir, seleccionamos java.policy y lo abrimos*

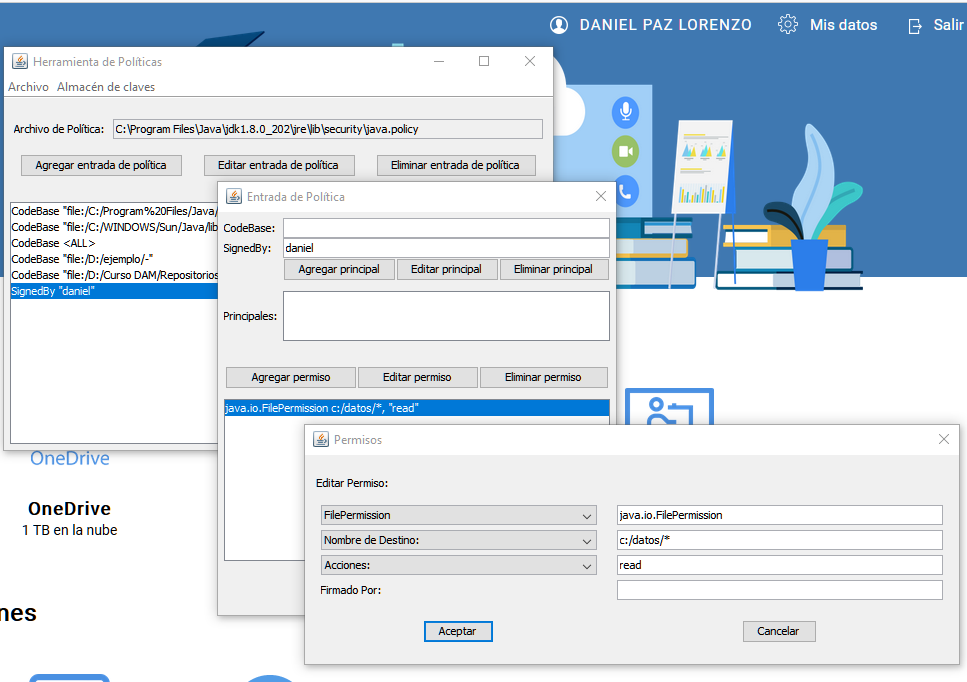


*Creamos un .txt dentro del mismo directorio que contenga la clave del repositorio de claves*



*Abrimos el almacén de claves y metemos las 2 url del repositorio de las claves y del fichero con la contraseña del repositorio*

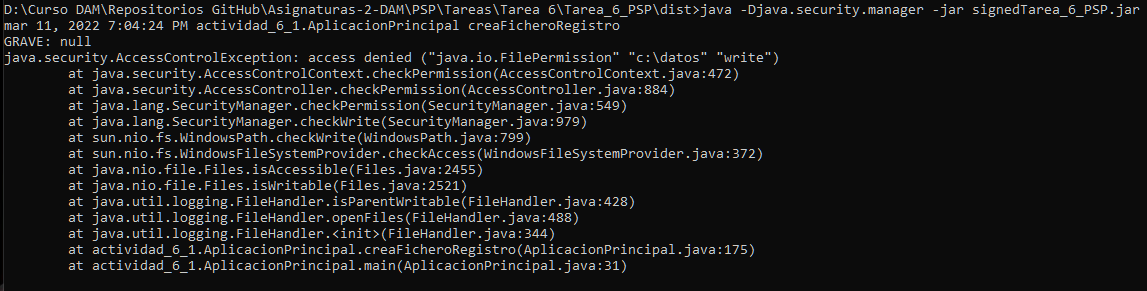
Una vez tenemos importado el almacén de claves vamos a agregar una entrada de política para que la aplicación pueda acceder a la carpeta C:/datos:



*Establecemos los parámetros necesarios y guardamos*

Ya solo nos queda comprobar que hemos configurado correctamente la política de seguridad ejecutando la aplicación.

1. Este primer pantallazo corresponde a una ejecución anterior a configurar las políticas de seguridad donde podemos ver que tenemos denegado el acceso a c:/datos:



1. Después de configurar y guardar la nueva política de seguridad ejecutamos la aplicación y vemos como ahora si no nos muestra ningún mensaje de error y podemos ejecutar la aplicación sin restricciones:

