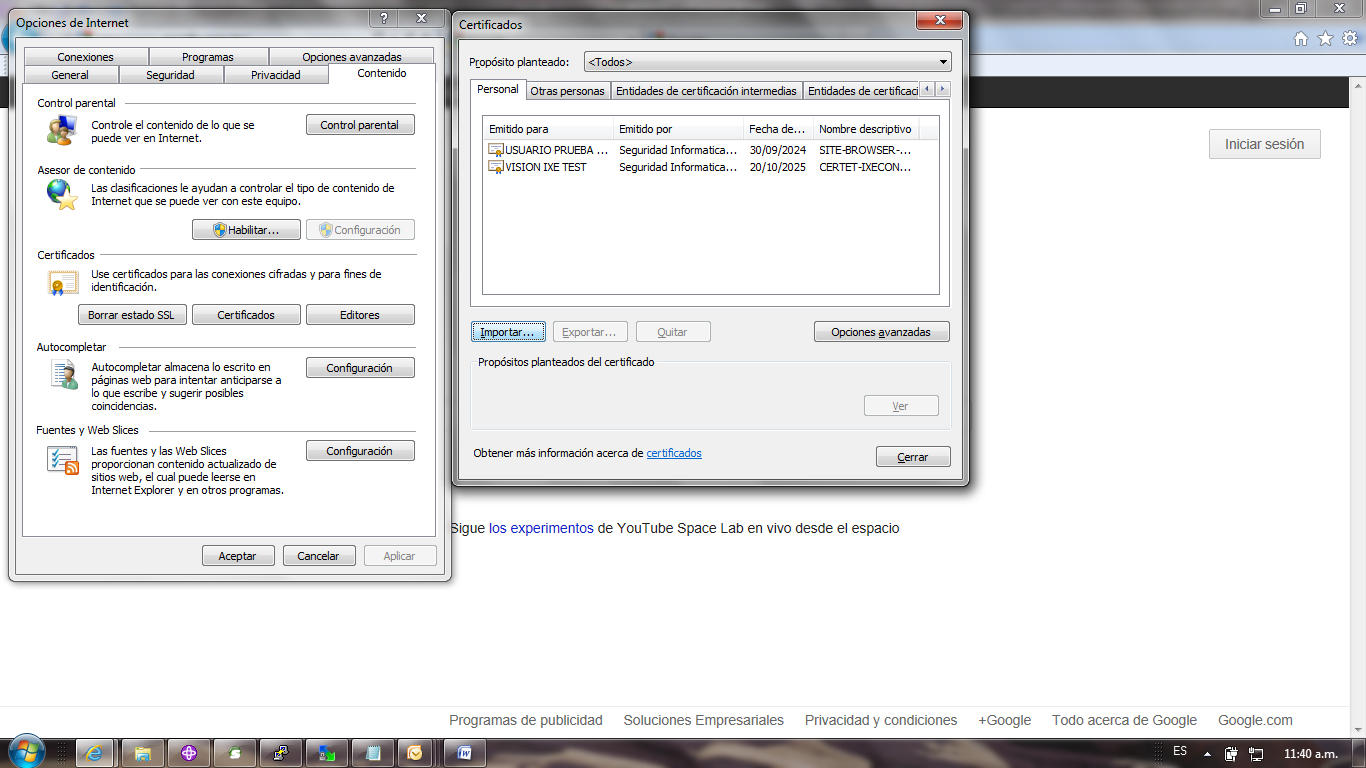
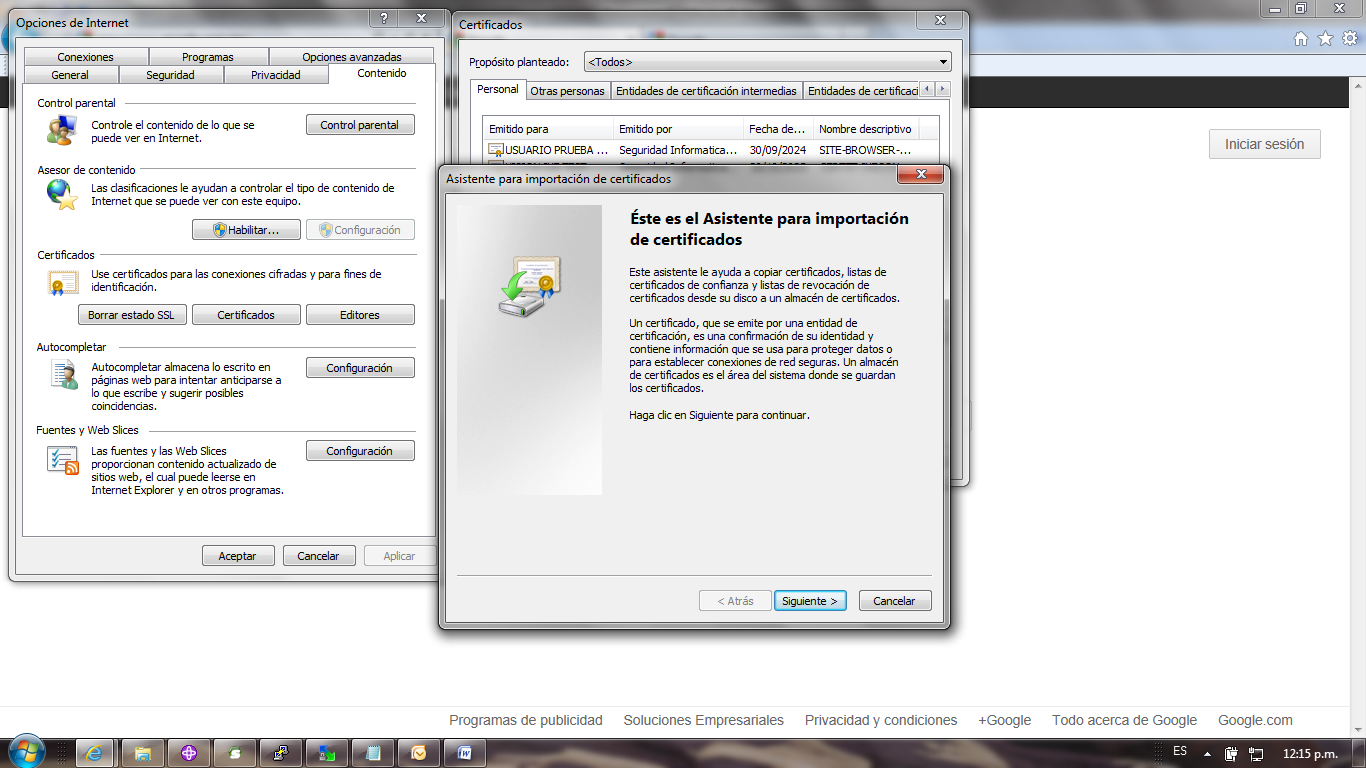
**Configuración del Certificado para la comunicación Altamira - ESB.**

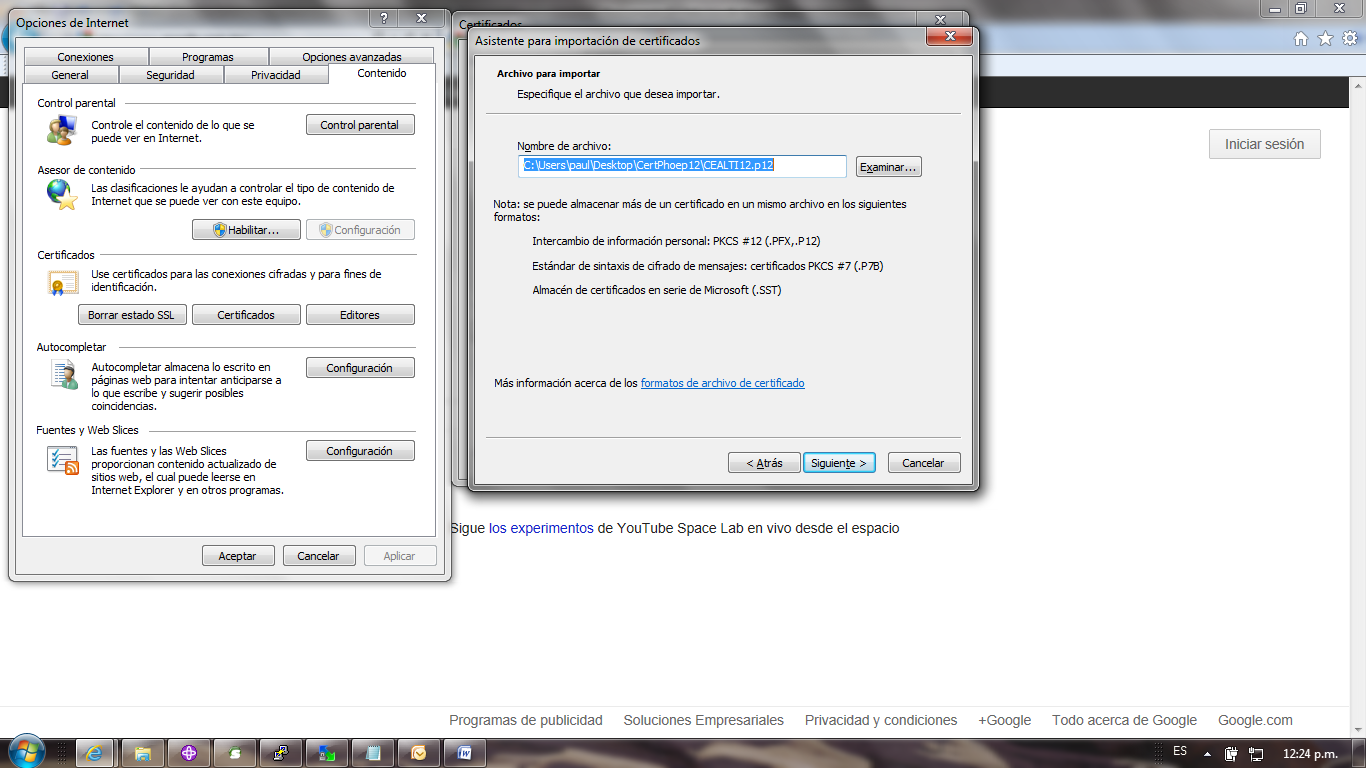
1. Realizar la solicitud para la creación del certificado a SIO ([bsio@banorte.com](mailto:bsio@banorte.com)).
2. El formato del certificado deberá ser PKCS12.
3. Una vez que el SIO envía el certificado, se deberá obtener de este mismo la CA. Nosotros lo obtuvimos de la siguiente forma:

* Abrir el navegador Internet Explorer e ingresar a la siguiente ruta:
* Herramientas/Opciones de Internet/Contenido/Certificados.
* Una vez ubicados en certificados en la pestaña Personal. Dar Click en importar



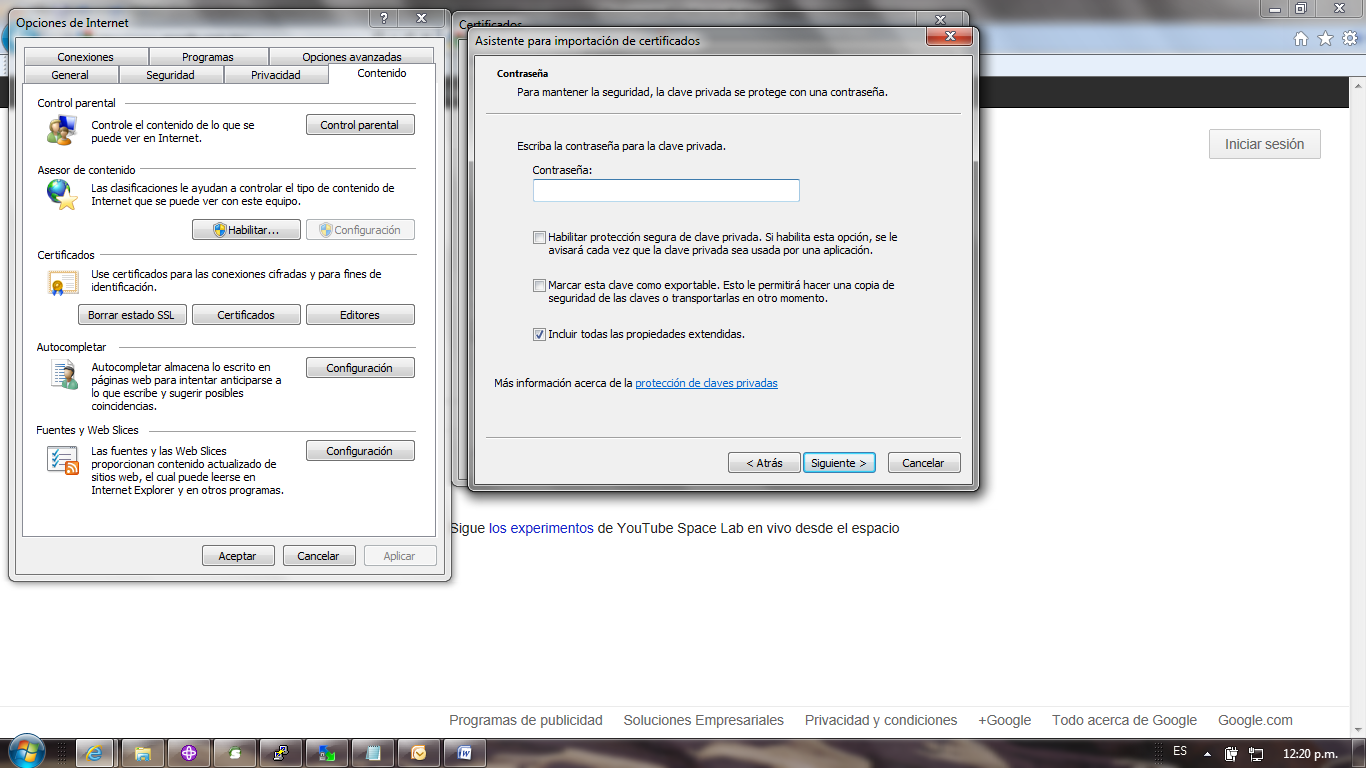


* Importar el certificado PKCS12 enviado por SIO.

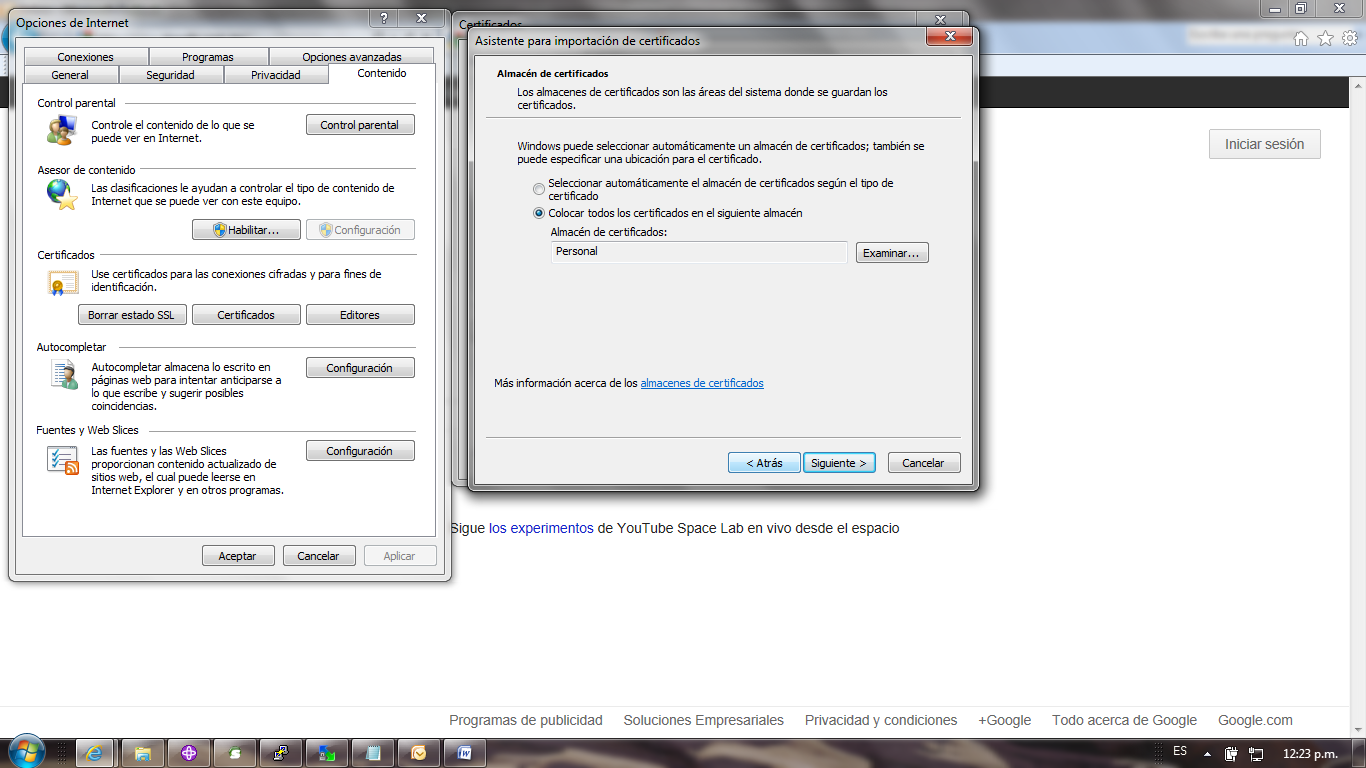


* Ingresar el password del Certificado proporcionado por el área de SIO. Cabe mencionar que el área de SIO deberá enviar también el nombre de la etiqueta que posteriormente se utilizara para la instalación de los certificados en el ambiente.

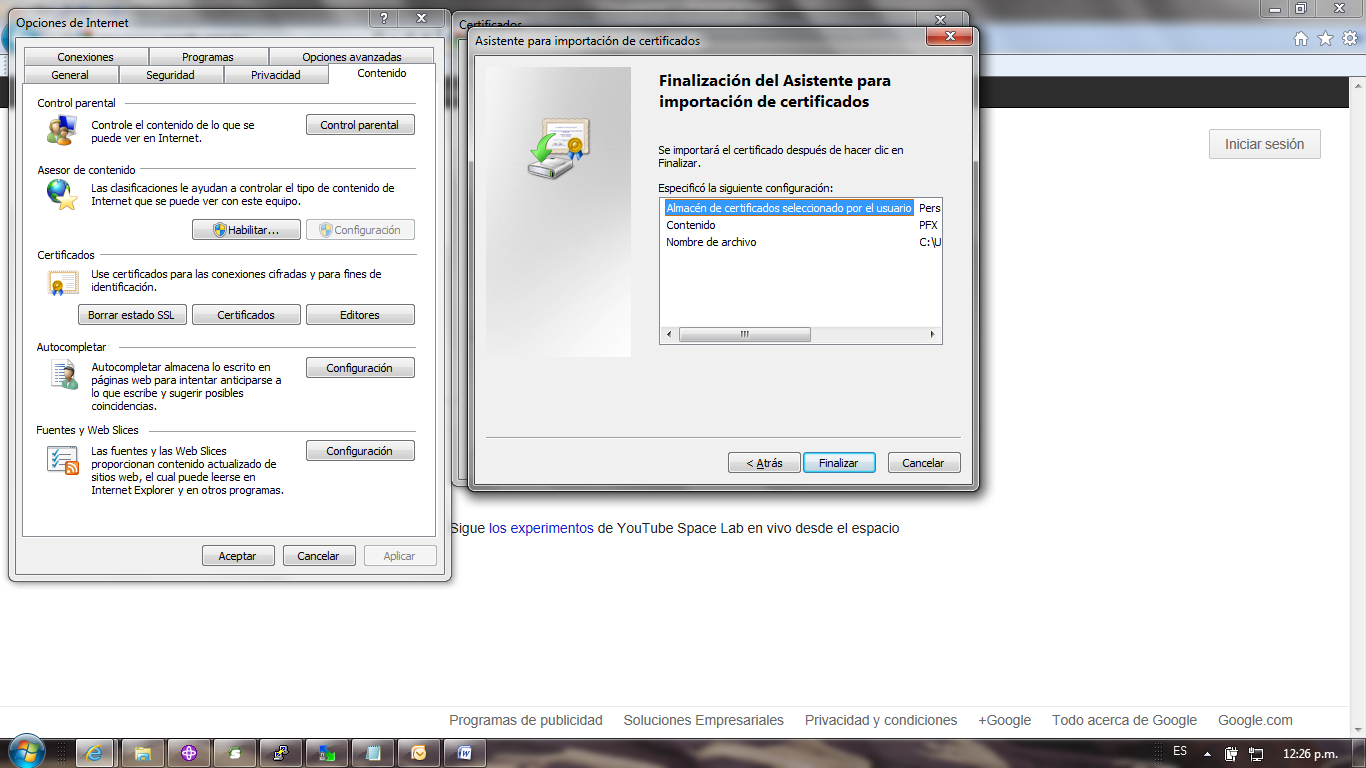
PWD: **CEALIXTE** ETIQUETA: **CERTET-IXECONECT-D120829**



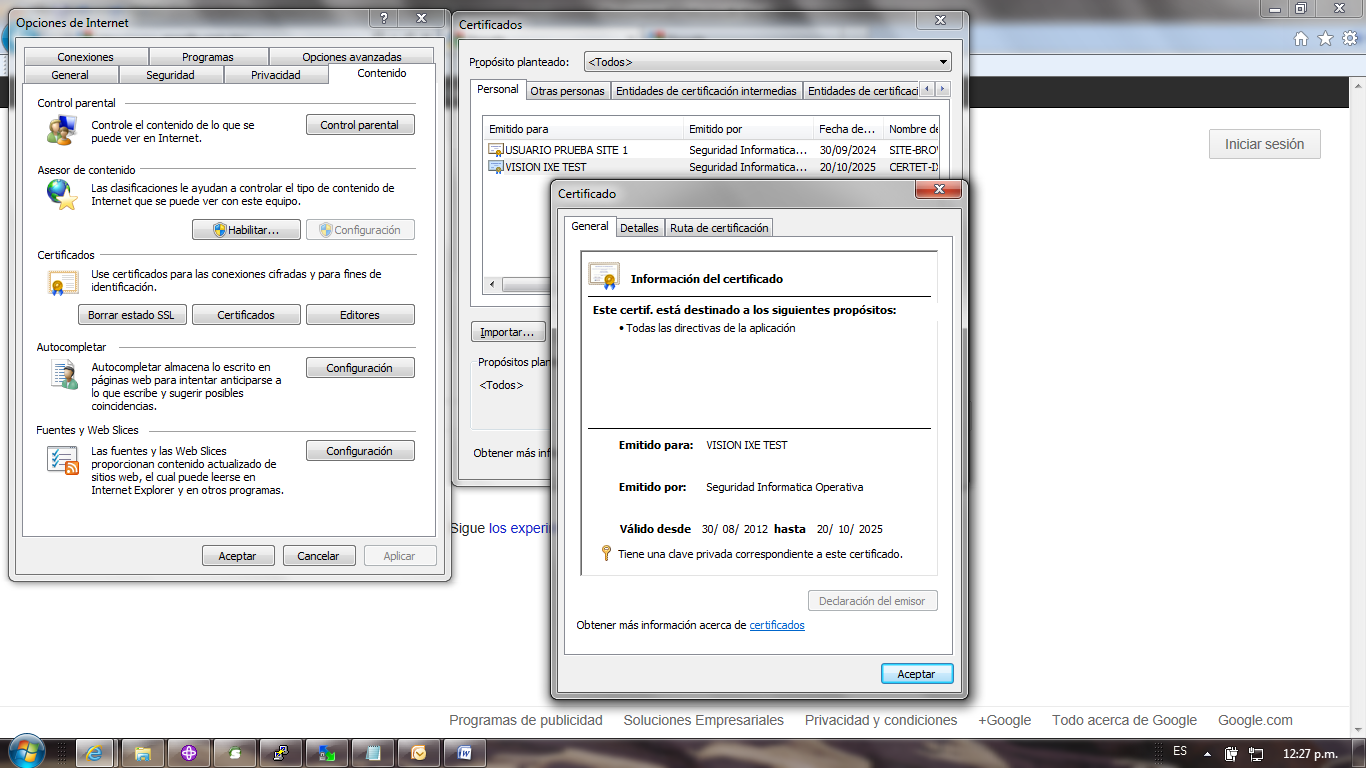
* Dejar el almacén de Personal para la instalación del certificado



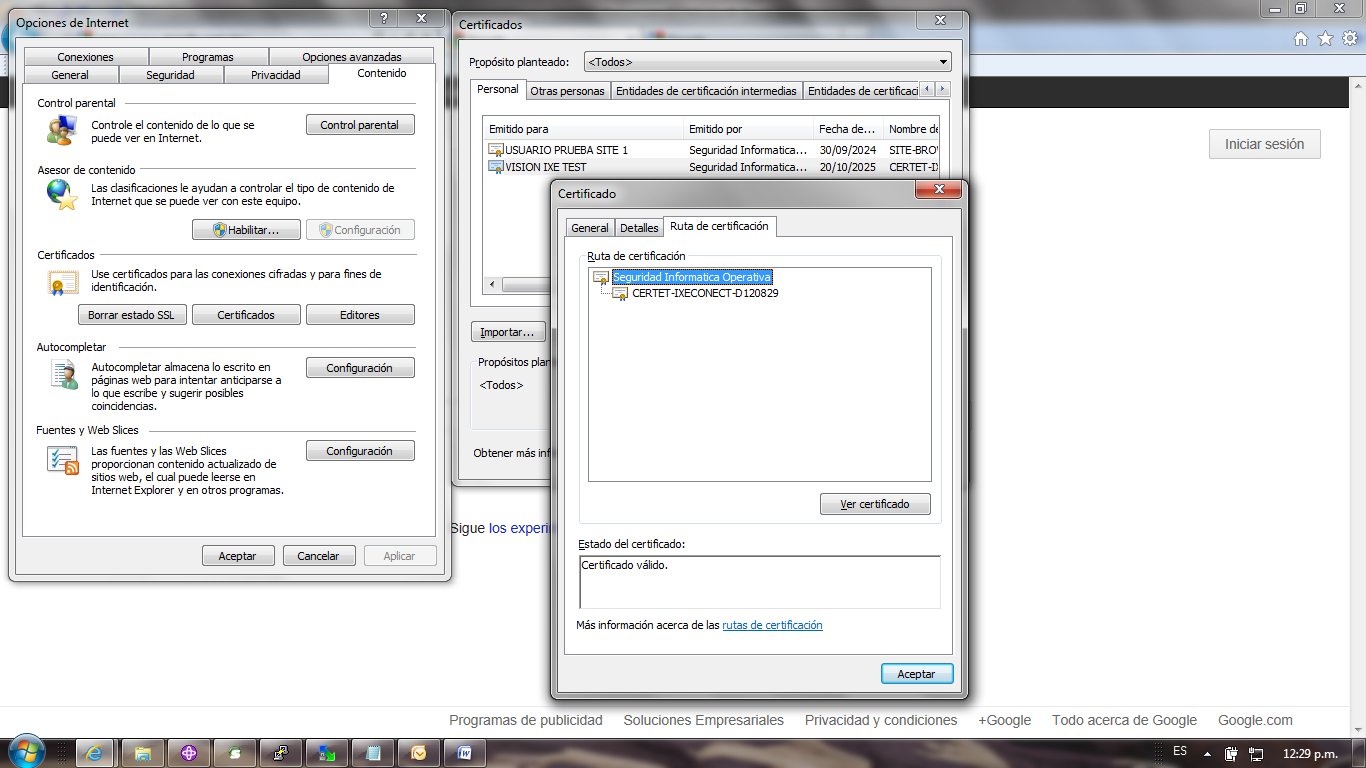
* Dar click en Finalizar.



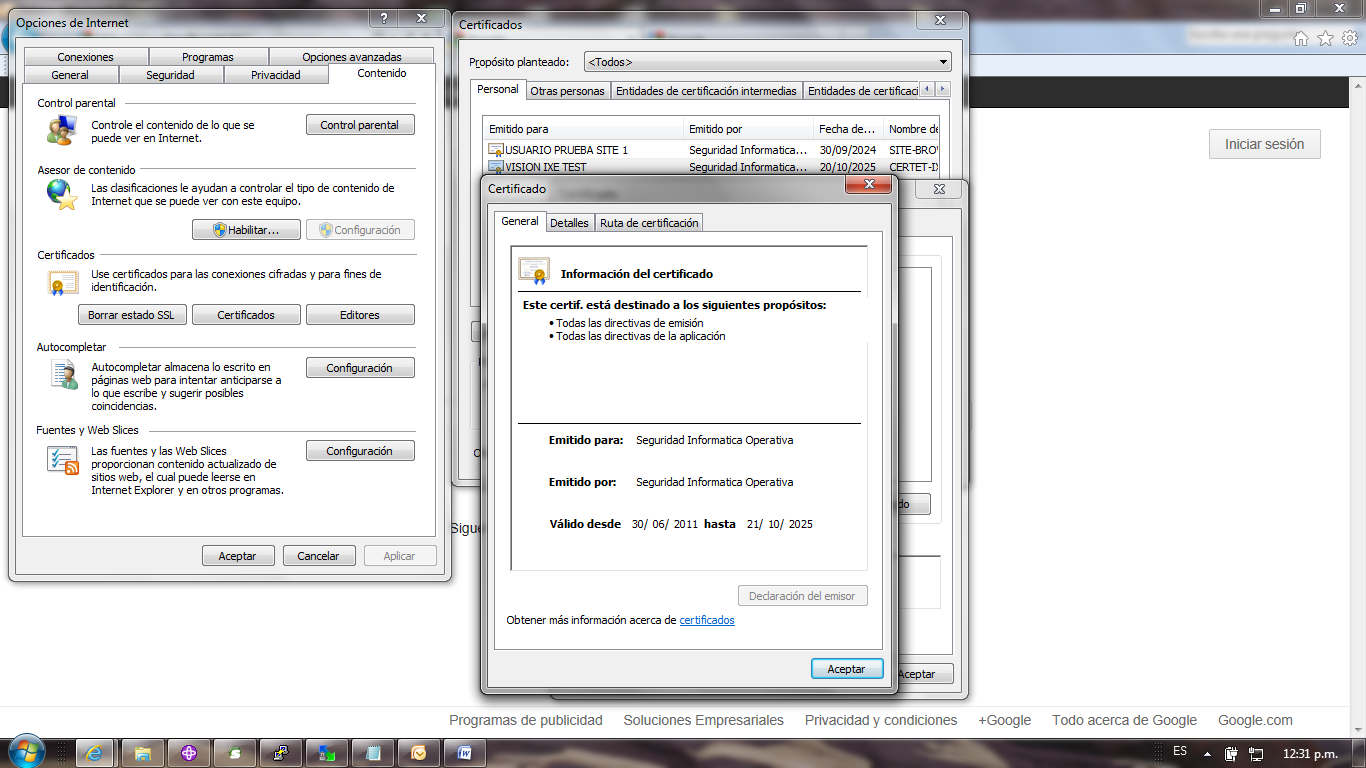
* Una vez instalado el certificado dar doble click sobre él. Nos mostrara la siguiente ventana.



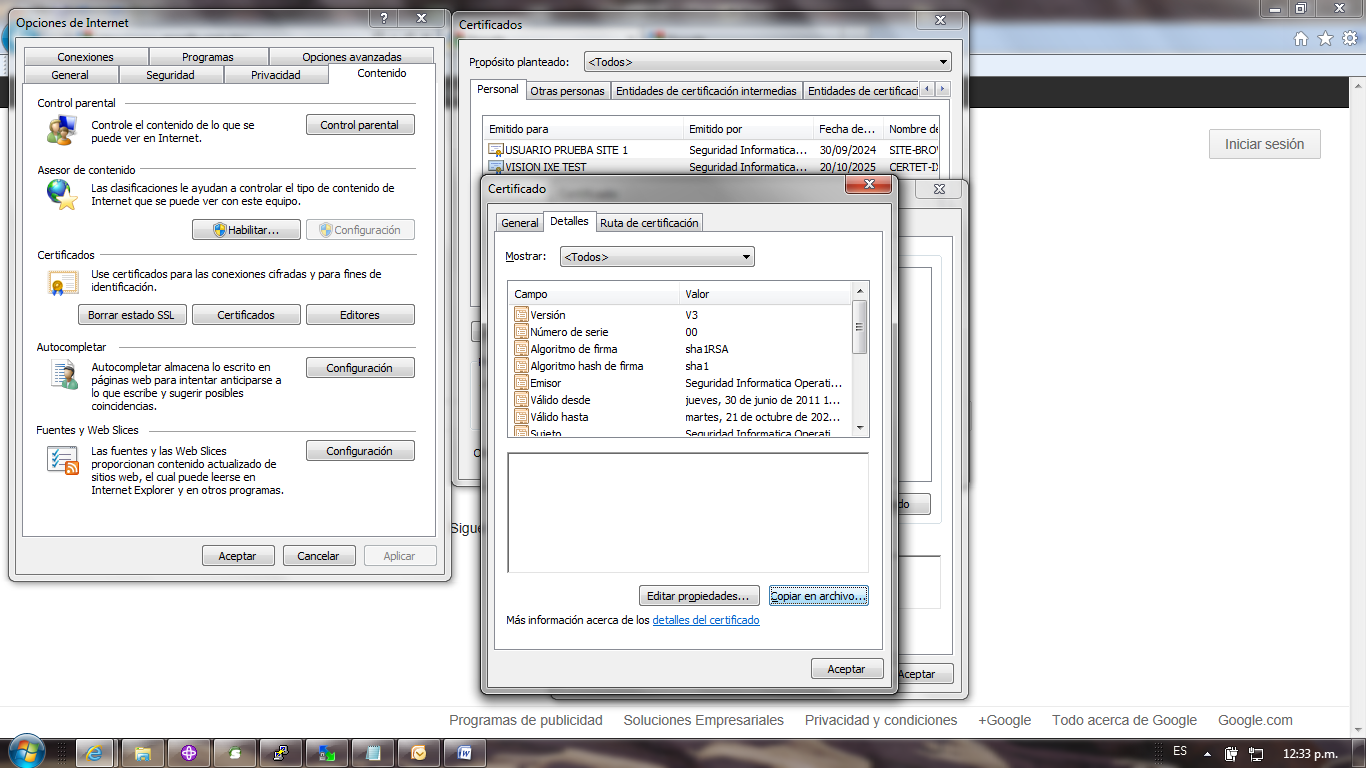
* Ir a la pestaña Ruta de Certificación. Y dar click en Seguridad Informática Operativa.



* Una vez que seleccionamos Seguridad Informática Operativa se habilitara la opción Ver Certificado al cual le daremos click.



* Ir a la pestaña Detalles y dar click en Copiar Archivo.



* Guardar el certificado en formato DER\_binario codificado X.509 (.CER), una vez guardo el certificado este sería nuestra CA.

1. Una vez configurado nuestro keystore y truststore. Instalar los certificados de la siguiente forma.

* En el archivo truststore se almacenara el certificado CA, este certificado una vez instalado deberá quedar configurado en los personales. Ejemplo:

gsk7cmd -cert -add -db /desa\_WMBFILES/jks/desa\_ALTAMIRA\_BRK/desa\_ALTAMIRA\_BRK\_TRUSTSTORE.jks -pw arqusr -label CERTET-IXECONECT-D120829 -file CA-Interfaces.cer -format ascii

* En el archivo keystore se almacenara el certificado PKCS12, este certificado una vez instalado deberá quedar configurado en los de confianza. Ejemplo:

gsk7cmd -cert -import -db CEALTI12.p12 -pw CEALIXTE -label CERTET-IXECONECT-D120829 -type pkcs12 -target /desa\_WMBFILES/jks/desa\_ALTAMIRA\_BRK/desa\_ALTAMIRA\_BRK\_KEY.jks -target\_pw arqusr

5.- Si se desea instalar el certificado en la JVM se hace de la siguiente forma después de exportarlo (Paso 3), en este caso se exportó con el nombre **CERT-SIO.cer**

Teclear el comando: ()

C:\bea\jdk142\_05\bin>keytool -import -alias IXE -file c:\certificados\**CERT-SIO.cer** -keystore c:\bea\jdk142\_05\jre\lib\security\cacerts

Escriba la contrase±a del almacÚn de claves: **changeit**

**--El sistema confirmará la acción.**

Propietario: CN=Seguridad Informatica Operativa, T=Servicios Web BANORTE, OU="SI

O PROD CA PRINC,Seguridad Informatica", O=BANORTE, L=Mexico, ST=DF, C=MX

Emisor: CN=Seguridad Informatica Operativa, T=Servicios Web BANORTE, OU="SIO PRO

D CA PRINC,Seguridad Informatica", O=BANORTE, L=Mexico, ST=DF, C=MX

N·mero de serie: 0

Vßlido desde: Thu Jun 30 05:00:00 GMT 2011 hasta: Wed Oct 22 04:59:59 GMT 2025

Huellas digitales del certificado:

MD5: AF:1D:0B:66:A6:BB:50:94:24:84:89:8F:8B:89:DA:39

SHA1: F1:6F:2A:66:32:72:03:CB:2D:D9:27:0A:1D:6E:35:E5:AC:1A:AB:96

┐Confiar en este certificado? [no]: si

Se ha a±adido el certificado al almacÚn de claves

C:\bea\jdk142\_05\bin>