RECOMENDACIONES PARA LAS ÁREAS DE INFORMÁTICA PARA UTILIZAR LA FIRMA ELECTRÓNICA DE CORREOS EN LOS SERVICIOS UNIVERSITARIOS:

Introducción:

En el marco de una nueva propuesta para la Gestión Presupuestal y Financiera para los adelantos de fondos, vía transferencia bancaria y firma electrónica para los Centros del Interior se elaboró un conjunto de recomendaciones para las estaciones de trabajo y cuentas de correo involucrados en el nuevo procedimiento.

Este documento pretende ser una guía de trabajo que le permita al Informático responsable del servicio universitario verificar si las condiciones de las estaciones de trabajo y de las cuentas de correo pueden dar las garantías que este proceso requiere.

Introducción de la firma electrónica en la UdelaR

La *firma electrónica* consiste en el uso de tecnologías de la información para asegurar, sobre documentos electrónicos, funciones similares a la de la *firma autógrafa* y *el sello s*obre documentos en papel.

El uso de la firma electrónica hoy está amparada por la ley[1], y la Universidad de la República ha decidido adoptarla en el marco de ciertos procesos administrativos y financieros[2].

Para esto, se utiliza el mecanismo más habitual y reconocido para la implementación de firma electrónica: la constitución de una **infraestructura de clave pública** (**PKI,** según su sigla en inglés). Ésta permite el uso de técnicas de criptografía para garantizar la integridad de un documento electrónico, así como su atribución o imputación a una persona, en el instante en que procedió a firmarlo electrónicamente.

El Servicio Central de Informática de la Universidad (SeCIU) es responsable del desarrollo, de las operaciones y del mantenimiento de la Autoridad de Certificación para este proceso, así como de sugerir las políticas de seguridad de la información aplicables.

El presente documento agrupa el conjunto de reglas, recomendaciones y procedimientos necesarios para el buen desarrollo de los procesos de firma electrónica en la UdelaR. Podrá evolucionar en función de la experiencia y de los cambios tecnológicos, en cual caso será comunicado a los interesados por los canales habituales.

1 Ley 18.600 y reglamentación aferente, la cual da en particular lugar a la creación de la Unidad de Certificación Electrónica (UCE – www.uce.gub.uy).

2 El primer proceso para el que se utiliza la firma electrónica es la gestión presupuestal y financiera de los adelantos de fondos para los Centros Universitarios del Interior, por transferencia bancaria. Ver resolución del CDC del 1ro de Octubre de 2013.

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

Definiciones y actores

SeCIU opera una **Autoridad de Registro** y una **Autoridad de Certificación** que otorgan a las personas que los requieren los dispositivos físicos y lógicos necesarios a la firma electrónica.

A la entrega de éstos, los **titulares de dispositivos de firma electrónica** recibirán una copia y firmarán[3] un formulario, un instructivo y un compendio de reglas y recomendaciones, que deberán respetar.

Las Unidades Informáticas de los servicios universitarios asesorarán y asistirán a los titulares en los procesos de firma electrónica, y serán responsables de asegurar el respeto de la normas y recomendaciones de seguridad de la información necesaria para las estaciones de trabajo en las que se procede a la firma electrónica de documentos.

La Autoridad de Certificación dispone de una **clave pública raíz**, a la que corresponde un certificado http://www.seciu.edu.uy/ca

Dispositivos de firma electrónica

Concretamente, cada persona que debe proceder a firmar documentos electrónicos recibe de SeCIU una tarjeta con microchip, o **tarjeta inteligente** – la cual es estrictamente ***personal*** **–** y eventualmente un lector de tarjetas que será conectado a la computadora en la que se firman los documentos. El acceso a esa tarjeta está protegido por un Número Personal de Identificación (o **código PIN**, por su sigla en inglés) que sólo debe conocer el titular de la tarjeta.

Esta tarjeta contiene una **clave privada**, específicamente asociada a la persona que firma, una **clave pública** y un **certificado** de ésta, emitido por la **Autoridad de Certificación**.

Acerca de la seguridad de la información

La seguridad de la información requiere exigencias y disposiciones en términos de *disponibilidad*, *integridad*, *confidencialidad* e *imputabilidad* (o *trazabilidad*). En cada caso, debería estar sustentada en un análisis de riesgos según cada uno de estos cuatro ejes, y respaldada por los responsables de la información.

Es conveniente que los Centros Universitarios de la UdelaR trabajen en lo que respecta a la seguridad de la información, y que las más altas autoridades lo patrocinen y lo promuevan.

Sin perjuicio de otras recomendaciones al respecto, es oportuno basarse sobre metodologías y estándares reconocidos al respecto. Se podrá en particular tomar como guía la RFC 2196 – *Site Security Handbook*[4].

Destacamos que la seguridad no es algo perteneciente únicamente al área Informática sino que depende de varios niveles de servicio por ejemplo: vigilancia física de los accesos a los servicios universitarios y en particular a las áreas donde se encuentran las estaciones de trabajo vinculadas con este procedimiento, mantenimiento de la higiene de los espacios físicos donde se encuentran las

3 Con su firma autógrafa, respaldada por un documento de identidad.
4 Ver: http://tools.ietf.org/html/rfc2196 (en inglés)

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

estaciones de trabajo, acondicionamiento térmico, etc.

Respecto a los dispositivos y datos de firma

Para cumplir su función como garante de la *integridad* e *imputabilidad* de un documento o un mensaje, los dispositivos de firma electrónica tienen una exigencia muy fuerte de:

- *confidencialidad* de la **clave privada** de quién firma, la cual sólo deberá ser accesible a su titular, de manera a que no se pueda usurpar dicha firma,
- *integridad* de las **claves públicas**, de manera de poder autenticar al firmante de un documento del cual se verifica la integridad y que se imputa a esa persona.

Para lo primero, las claves privadas están almacenadas *únicamente* en el micro-chip de la tarjeta personal, y el acceso a éstas está protegido por el PIN, mediante medidas técnicas y mecanismos estandarizados[5].

Para poder firmar, el titular debe estar *en posesión* de su tarjeta y tener *conocimiento* de su código PIN. Este doble requerimiento – tener una cosa y conocer otra – es típica de un mecanismo de **acceso con seguridad fuerte**. Evita la usurpación de la firma si se pierde la tarjeta ***o*** si el código PIN se ve comprometido.

Respecto a las claves públicas, si bien – como la denominación indica – no existe exigencia de *confidencialidad*, conviene insistir sobre la importancia y criticidad de la *integridad*: el engaño sobre una clave pública, por ejemplo haciendo pasar una clave arbitraria por la de una persona, sería similar a la falsificación de un documento de identidad.

Para garantizar esta integridad y atribución, en las tarjetas personales de firma, se distribuye la clave pública del titular conjuntamente con un *certificado*, es decir una versión "firmada" (o más bien "sellada") por la autoridad de certificación de la PKI.

De esta manera, alcanza con disponer del **certificado raíz de la autoridad de certificación** de la Autoridad de Certificación. A partir de éste se podrá verificar la validez de todas las firmas realizadas con una clave asociada a un certificado emitido por esta Autoridad.

El **certificado raíz** de la autoridad de certificación de SeCIU **siempre** deberá ser obtenido a partir de una fuente segura. Se lo puede obtener de SeCIU o descargar de la dirección: http://www.seciu.edu.uy/ca

El documento se divide en:

Directivas generales: directivas generales sobre seguridad, y sobre el mantenimiento de las estaciones de trabajo.

Seguridad en nivel de Sistema: Comentaremos aquí diversos aspectos de configuracion de los equipos, centrándonos sobre todo en aquellos equipos multiusuario (equipos de correo, servidores de archivos, etc).

5 Dispositivos PCKS#12.

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

RECOMENDACIONES GENERALES

Estas recomendaciones se basan en que para cada servicio universitario existirá personal responsable del mantenimiento del equipamiento informático en el mismo. Deberá quedar claro quién es el responsable del área Informática de cada servicio y deberá comunicarse a SeCIU nombre del mismo y forma de contactarlo.

Los equipos utilizados para el mencionado proyecto deberán ser de uso exclusivo de las áreas administrativo/contables involucradas (pudiendo ser PC o portátiles individuales) y requerirán un nivel de mantenimiento, seguridad lógica y física y de resguardo de información que otorgue garantías al proceso de firmado en el cual dichas estaciones participan.

Por otro lado las cuentas de correo que cada servicio universitario utilizará en el marco de esta gestión presupuestal y financiera para los adelantos de fondos, vía transferencia bancaria y firma electrónica deberán mantener una política de tratamiento y respaldo diferencial permitiendo conservar toda la historia de envíos y recepciones de correos desde y hacia la misma en forma diaria.
Todo envío de correo se realizará con copia a una cuenta de respaldo creada en el servidor de correo de SeCIU.

Será tarea del responsable de informática del servicio mantener informados y actualizados a los funcionarios administrativo/contables intervinientes en este proceso sobre los cambios en las prácticas de operación de la estación de trabajo como de las cuentas de correo que intervienen en el proceso.

Las recomendaciones son generales y son independientes del sistema operativo que las mismas tienen (Windows, Ubuntu, Linux, etc.)

CONTACTOS:

Ante cualquier duda de carácter técnico y más específico, el responsable informático del servicio podrá contactarse con SeCIU a través de su Mesa de Ayuda al teléfono 2 4083901/02 int. 110 de 8 a 18 hs o por correo electrónico a mesadeayuda@seciu.edu.uy

GUÍA DE BUENAS PRÁCTICAS:

- **Recomendaciones para las estaciones de trabajo**

- Sin perjuicio del conjunto de la política de seguridad de la información, la estación de trabajo en la que se conecta un dispositivo de lectura de tarjetas con microchip deberá ser

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

objeto previamente y permanentemente de una vigilancia particular en términos de instalación, mantenimiento y respetos de las normas y las buenas prácticas de seguridad de la información. En particular:

- Que sean libres o privativos, el sistema operativo y todos los aplicativos que corren en esa computadora deberán ser legítimos. Deberán haber sido obtenidos de fuentes de distribución de software confiables, y la integridad de los medios de instalación (CD, pendrive, por red, etc) deberá haber sido verificada.
- Sólo se deberán utilizar sistemas operativos y paquetes de software durante su ciclo de vida útil, es decir mientras exista mantenimiento y soporte por parte de los canales de distribución.
- Se deberán efectuar periódicamente las actualizaciones de seguridad en el sistema y de todos los aplicativos que corren en la aplicación.
- En los sistemas operativos susceptibles a virus (como Microsoft Windows) se deberá disponer de un anti-virus, y ser particularmente vigilante en la actualización permanente de éste.
- Más generalmente, en todos los sistemas, se deberán tomar todas las medidas oportunas para evitar todo tipo de *malware*.
- En estas estaciones de trabajo al menos, no se debería correr ningún software de tipo servidor, que comparta recursos, aunque sea con controles de acceso. Para compartir datos o recursos con otros usuarios, se lo deberá hacer a través de servidores específicamente dedicados a esta función, o a lo sumo a través de estaciones de trabajo de menor criticidad.
- Conviene configurar en la estación de trabajo un cortafuegos local, que bloquee todas las solicitudes entrantes excepto, eventualmente, las que se requieran para la administración y monitoreo del parque informático, validadas en el marco de la política de servicios del Centro Universitario.

  - **Recomendaciones para los usuarios**

- Sin perjuicio de poder tener derechos específicos, en su trabajo cotidiano, el usuario deberá utilizar una cuenta personal, con acceso protegido por contraseña, y con los derechos mínimos necesarios.
- Sin perjuicio de que el titular tenga derechos de administración, las cuentas con permisos de administrador sólo deben utilizarse para tareas puntuales de mantenimiento y por personas con formación para realizarlas.
- Siempre se deben utilizar contraseñas robustas, deben ser cambiadas periódicamente (según la robustez exigida),
- Configurar el navegador para que esté protegido durante la navegación (Java, Javascript, Cookies).

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

- Los usuarios deberán recibir una capacitación adecuada al uso correcto de los programas y sistemas que utilizan, en particular para el buen uso de los dispositivos de firma electrónica.

RECOMENDACIONES PARA LA CONFIGURACIÓN DE LAS CUENTAS DE CORREO QUE SE UTILIZARÁN EN EL PROCESO:

- Configurar el cliente de correo Thunderbird de manera de que al bajar los correos mantenga una copia en el servidor de correo. Para esto se debería configurar el cliente de correo con la opción Imap.
- Sin perjuicio de la política general de respaldo de datos, es necesario tomar en cuenta los requerimientos específicos de los documentos firmados.
- En función del tipo de documentos y de la exigencia de preservación, al igual que se resguarda copia de la correspondencia enviada, no se deberá borrar el contenido de las casillas que contienen documentos firmados.
- Para garantizar su preservación, se deberá realizar al menos un respaldo periódico, de la estación de trabajo o del servidor en que se mantiene el contenido de la cuenta.

Procedimiento para instalación de la configuración para envío de correos firmados por la CA de la Universidad:

Provisión de una tarjeta personal

Para obtener una tarjeta personal con microchip, que permita al titular firmar electrónicamente correos electrónicos y documentos, la persona deberá llenar y firmar el formulario "Formulario_solicitud_de_CertificadoDigital v2.0" y el documento "Final_TarjInt_Responsabilidad_Uso_CertificadosDigitales v1.0".

Provisión de un lector de tarjetas

A menos que la tarjeta personal sea destinada a ser utilizada únicamente en una computadora compartida que ya está dotada de un lector de tarjetas con microchip, SeCIU también proveerá al solicitante de una tarjeta un lector de tarjetas

Los procedimientos descriptos a continuación, fueron realizados para utilizar el cliente de correo Thunderbird.

Instalación del módulo para utilizar la lectora de tarjetas inteligentes

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

Se tomaron como referencia para este punto dos de los Sistemas Operativos más utilizados en las estaciones de trabajo de la UdelaR, que son Windows y Ubuntu.

Para realizar la instalación en Windows, se debe seguir el manual **"Manual Instalacion Tarjeta Inteligente – Windows.pdf"**.

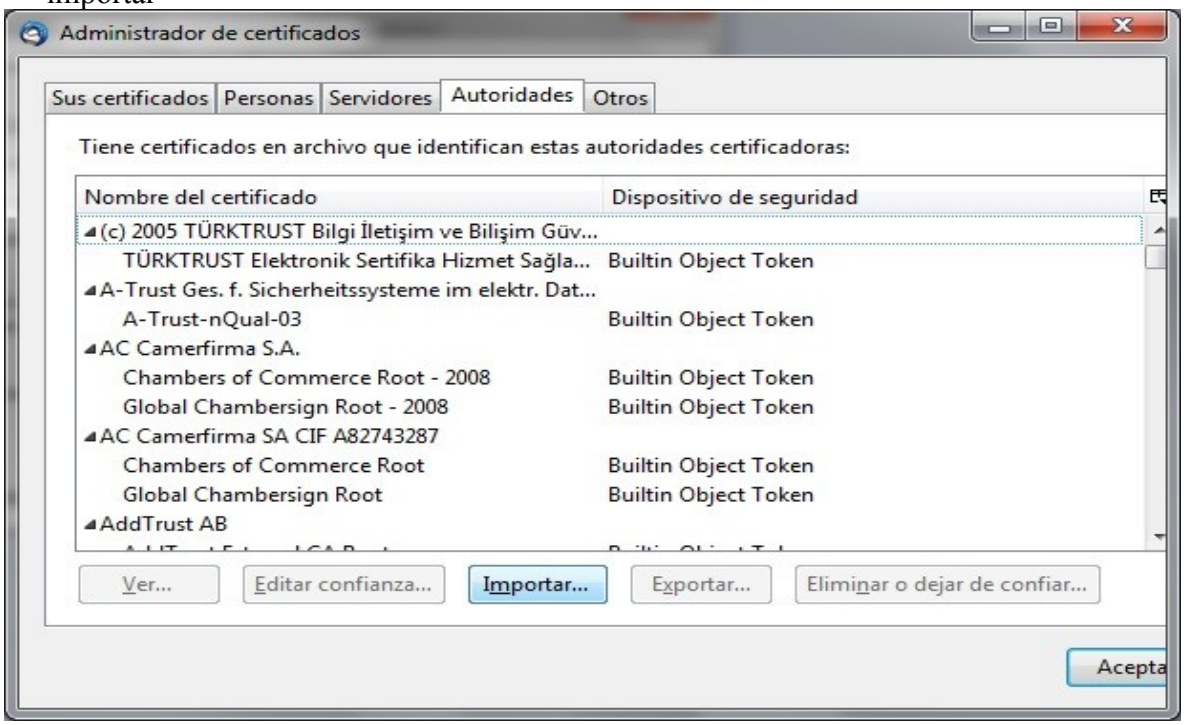
Para realizar la instalación en Ubuntu, se debe seguir el manual **"Manual Instalacion Tarjeta Inteligente – Ubuntu.pdf"**.

Estos manuales indicarán los pasos a seguir para la instalación de todos los dispositivos necesarios para el uso de las tarjetas inteligentes.

Importar certificado de la autoridad certificadora (CA)

Teniendo abierto el Thunderbird del usuario que va a usar firma:

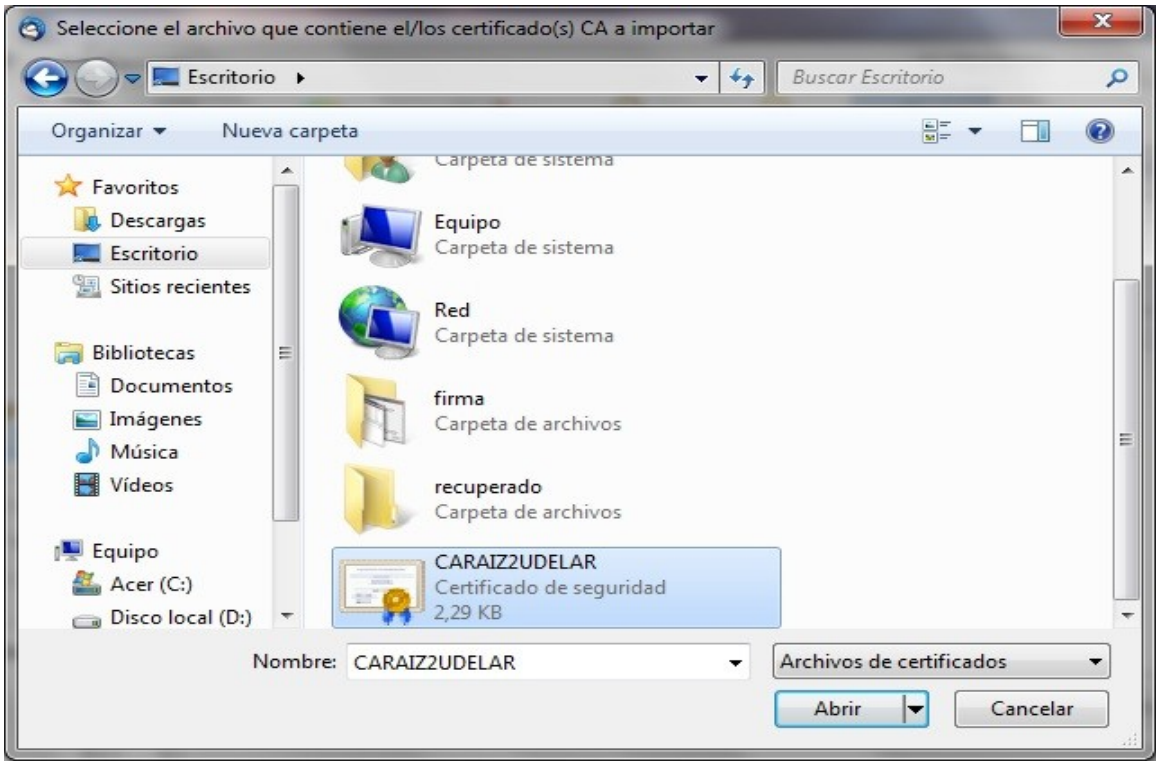
- Bajar el certificado de la siguiente url: http://www.seciu.edu.uy/ca y guardarlo por ejemplo en el escritorio del PC
- En el Thunderbird, ir a Herramientas/Opciones/Avanzado/Certificados
- En la pantalla de administración de certificados ir a la pestaña Autoridades y luego pulsar importar



- Ir a la ruta donde se tenga guardado el certificado de la autoridad certificadora (CA) y

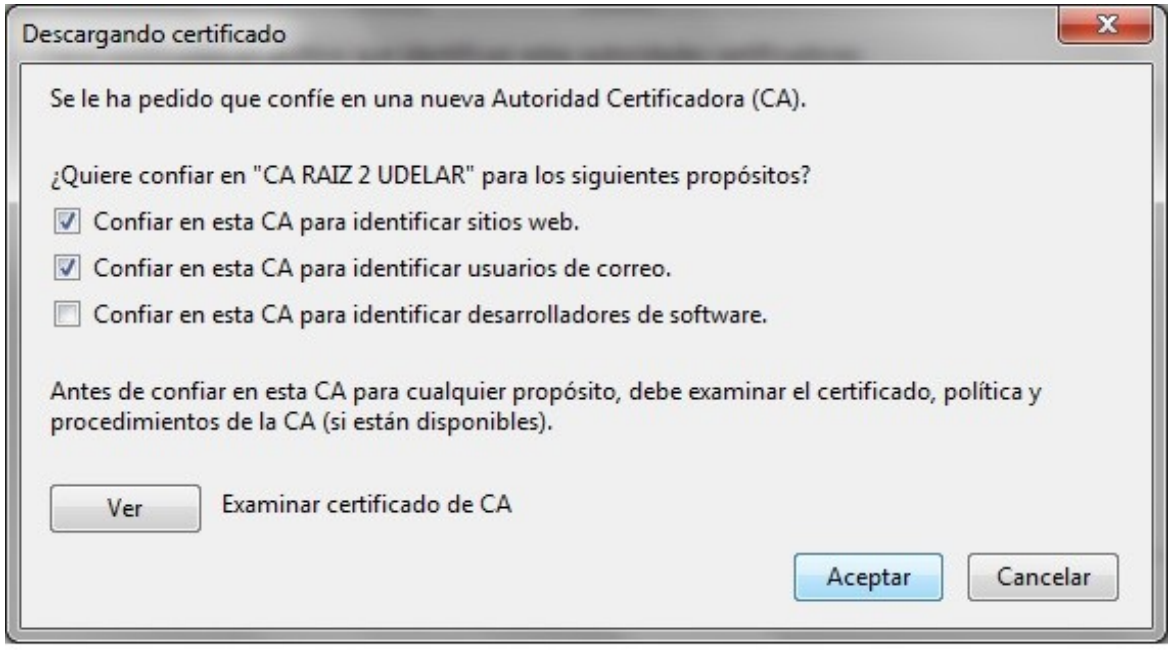
Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY

seleccionarlo para importarlo
A continuación se muestra un ejemplo de como sería esto en una estación de trabajo con Windows, asumiendo que se guardó el certificado de la autoridad certificadora en el Escritorio de Windows.



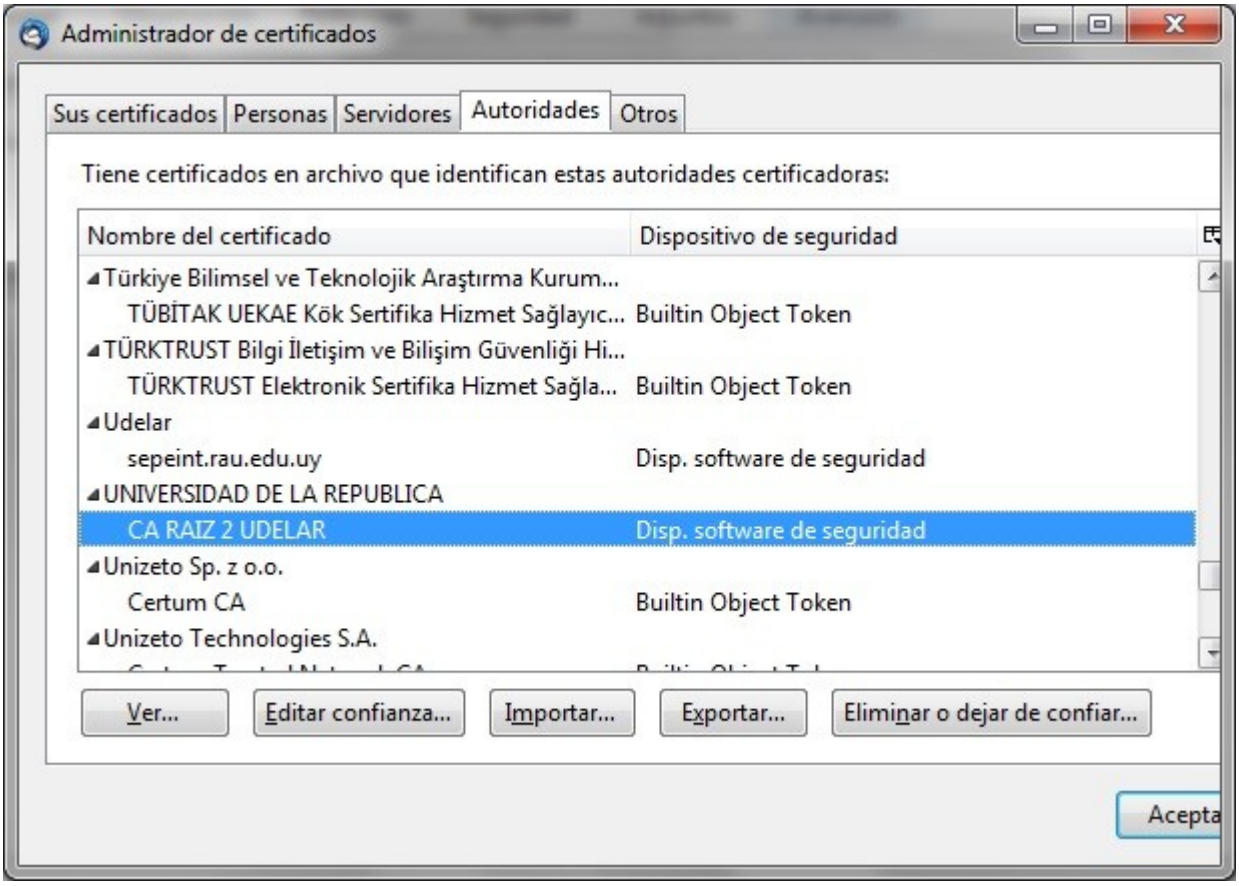
- Aparecerá otra ventana donde se seleccionarán las opciones que se muestran a continuación. Presionar aceptar

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY



- Para verificar que quedo guardado correctamente, ir a la ventana de administración de certificados y a la pestaña Autoridades. Allí aparecerá listado el certificado de la autoridad certificadora (CA) de la UdelaR.

Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY



Colonia 2066 - CP 11200 - Teléfono: [598 2] 408 3901 - Fax: [598 2] 4015843 - Correo electrónico: secretar@seciu.edu.uy - Montevideo - URUGUAY