Guía de ayuda para el procedimiento de delegación, voto e información electrónicos

Contenido

- Introducción.
- Especificaciones técnicas.
- Voto o Delegación Electrónica.
- Mis Comprobantes.
- Obtener tarjetas para voto o delegación a distancia, vía entrega o correo postal.
- Derecho de Información.
- Formas de Acceso.
- ¿Qué es la firma electrónica?
- Autoridades de certificación.
- Certificados Digitales.
- Time Stamping.
- Proceso Firma Digital.
- Verificación Firma Digital.
- Cómo utilizar el DNI electrónico.
- Prestadores de Servicios de Certificación de Confianza.

Introducción

Este documento le guiará en los procesos de Voto o Delegación a distancia, así como en el acceso al Derecho de información.

Antes de continuar, por favor lea las condiciones asociadas a cada proceso. En la página de bienvenida, o en el menú lateral, podrá encontrar un acceso al documento con las condiciones a cumplir, para el voto o delegación a distancia, y para el derecho de información.

A continuación se describen las funcionalidades que usted puede realizar:

- Votar o Delegar de forma electrónica.
- Mis comprobantes.Acceso cuentas.
- Obtener duplicados de tarjetas para votar o delegar a distancia por entrega o correo postal.
- Derecho de Información.

Para todas ellas, es necesario identificarse previamente en la aplicación. Ver ***Formas de acceso***.

Especificaciones técnicas

Para acceder por Internet al sistema de Voto Electrónico y ejecutar todas las opciones incluidas en dicho sistema, necesita contar en su equipo con la siguiente la configuración:

Navegadores:

Microsoft Explorer 5 o superior, Nestcape Browser v.6.0 o 7.0, Mozilla 1.X o superior o bien, FireFox 1.0 o superior hasta la versión 3.0. Se recomienda una resolución de pantalla mínima de 800*600 píxeles.

Si el navegador no es Microsoft Internet Explorer, deberá soportar JAVA. Para ello, si no tiene instalada la máquina virtual de Java debe proceder a su instalación. Recomendamos la versión 1.4.2. Sun Microsystem: ***http://java.com/es/download/manual.jsp***

Visor de PDF:

Adobe Acrobat Reader v.5.1 o superior

Comprimir / descomprimir ficheros:

Winzip 7.0 o superior

Software de firma digital.

El software necesario para realizar la firma digital (certificado electrónico) se descargará e instalará de forma automática. Para ello usted debe ser administrador de su máquina.

Requisitos mínimos de hardware y conexión a Internet:

Windows 98 o posterior, 128 MB RAM o 256 si se usa un navegador diferente a Internet Explorer, Módem de 56k o superior, Tarjeta de sonido de 16 bits.

Si va a votar con Documento Nacional de Identidad electrónico (DNIe) necesitará además:

- Un ordenador personal (Intel -a partir de Pentium III- o tecnología similar).
- Un lector de tarjetas inteligentes que cumpla el estándar ISO 7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.
- Unos módulos criptográficos y drivers específicos que, normalmente, se distribuyen con el propio lector.

Voto o Delegación Electrónica

Para acceder a esta funcionalidad deberá seleccionarla en la página de bienvenida, o desde el menú lateral, dentro del grupo Voto a Distancia, en la opción de votar. Además es necesario que usted se identifique en la aplicación. Ver ***Formas de acceso***.

Si usted quiere votar o delegar su voto de forma electrónica, necesita obligatoriamente disponer de un certificado electrónico emitido por algún Prestador de Servicios de Certificación de confianza; para ello, si no dispone de un certificado válido, podrá obtener información y solicitarlo accediendo a los enlaces de la sección ***Prestadores de servicios de certificación***.

Una vez identificado el accionista, deberá seleccionar las cuentas de valores con que desea participar, en el caso de tener varias, podrá seleccionar una, varias o todas las cuentas y pulsar el botón con la opción correspondiente.

Para ver todas las opciones disponibles, deberá consultar las condiciones para participar en la junta.

A continuación le aparecerá una nueva página, con los datos de la/s cuenta/s seleccionadas y los puntos del orden del día con las opciones de voto disponibles.

También en la parte superior derecha le aparecerá un identificador de la votación a realizar, que posteriormente se reflejará en el justificante o recibo de su votación.

Si usted ha seleccionado la opción de delegar, deberá seleccionar el titular que le representa, bien un miembro del consejo de administración, bien otra persona física. Además se podrá instruir al representante para que extienda o no la delegación, a las propuestas sobre los nuevos puntos no previstos del Orden del Día.

Una vez informados los campos solicitados, usted deberá pulsar el botón de firmar. En este momento se validará que los datos introducidos son correctos. En caso afirmativo se le mostrará una nueva página, con el justificante de la operación realizada, indicando la fecha completa de la votación realizada y el identificador de la misma. Si por contra algún dato no es correcto, se mostrará en la página actual un mensaje con el error producido.

Una vez verificados que todos los datos son correctos, le aparecerá una nueva página, donde usted podrá descargarse un recibo PDF justificante de la acción realizada. Para visualizar y guardar el comprobante deberá tener instalado el programa ***Acrobat Reader***. Si no lo tiene puede descargarlo dentro de la opción de especificaciones técnicas del menú lateral, o desde el link adjunto.

Los recibos justificantes de la acción realizada emitidos en formato PDF están firmados electrónicamente.

Mis Comprobantes

Para acceder a esta funcionalidad deberá seleccionarlo desde el menú lateral, dentro del grupo Voto a Distancia, en la opción de Mis Comprobantes. Además es necesario que usted se identifique en la aplicación. Ver ***Formas de acceso***.

Si usted quiere obtener los recibos comprobantes de sus votaciones realizadas, necesita obligatoriamente disponer de un certificado electrónico emitido por algún Prestador de Servicios de Certificación de confianza; para ello, si no dispone de un certificado válido, podrá obtener información y solicitarlo accediendo a los enlaces de la sección ***Prestadores de servicios de certificación***.

Una vez identificado el accionista, se le mostrará una página con acceso a todos los comprobantes o justificantes de las acciones realizadas por usted, ordenadas por fecha de forma descendente, de tal forma que le aparecerá en primer lugar la última acción realizada.

Para ver todas las opciones disponibles, deberá consultar las condiciones para participar en la junta.

Pinchando en cada fecha de la lista de comprobantes, podrá descargarse un recibo PDF justificante asociado a la acción realizada. Para visualizar y guardar el comprobante deberá tener instalado el programa ***Acrobat Reader***. Si no lo tiene puede descargarlo desde el menú lateral dentro de la opción de especificaciones técnicas o desde el link adjunto.

Los recibos justificantes de la acción realizada emitidos en formato PDF están firmados electrónicamente.

Obtener tarjetas para voto o delegación a distancia, vía entrega o correo postal

Para acceder a esta funcionalidad deberá seleccionarla en la página de bienvenida, o desde el menú lateral, dentro del grupo Voto a Distancia, en la opción de obtener tarjetas. Además es necesario que usted se identifique en la aplicación. Ver ***Formas de acceso***.

Si usted quiere obtener tarjetas para votar o delegar por entrega o correo postal, necesita obligatoriamente disponer de un certificado electrónico emitido por algún Prestador de Servicios de Certificación de confianza; para ello, si no dispone de un certificado válido, podrá obtener información y solicitarlo accediendo al enlace de Prestadores de servicios de certificación

Una vez identificado el accionista, deberá seleccionar las cuentas de valores que desea obtener duplicados de tarjetas, en el caso de tener varias, podrá seleccionar una, varias o todas las cuentas y pulsar el botón con la opción correspondiente.

Para ver todas las opciones disponibles, deberá consultar las condiciones para participar en la junta.

A continuación se descargará un archivo comprimido con documentos PDF, correspondientes a las cuentas seleccionadas.

Para obtener las tarjetas y poder guardarlas o imprimirlas, necesita tener instalado un programa descompresor de archivos, por ejemplo ***Winzip***. Si usted no lo tiene, en el menú lateral, dentro de la opción especificaciones técnicas, encontrará un acceso para poder descargarlo.

Derecho de Información

El derecho de información tiene como finalidad atender las consultas, quejas o sugerencias por parte del accionariado de la junta.

Existirá un periodo válido para que un usuario identificado como accionista de la junta, pueda solicitar información.

En la página de Derecho de Información aparecerá informado el Nombre, Apellidos y NIF del accionista.

Si usted desea enviar su consulta por correo postal, podrá descargarse el formulario del link ***Formulario Derecho de información.***

Si por contra, usted desea enviar su consulta de forma electrónica, deberá informar los siguientes apartados:

Datos para solicitar Información:

Indicar obligatoriamente el texto que expresará la consulta, queja o sugerencia.

Datos para el envío de la Información:

Si elige el envío por **Correo Electrónico**, deberá informar obligatoriamente el campo e-mail y opcionalmente el campo teléfono. En breve recibirá una respuesta personalizada por correo electrónico.

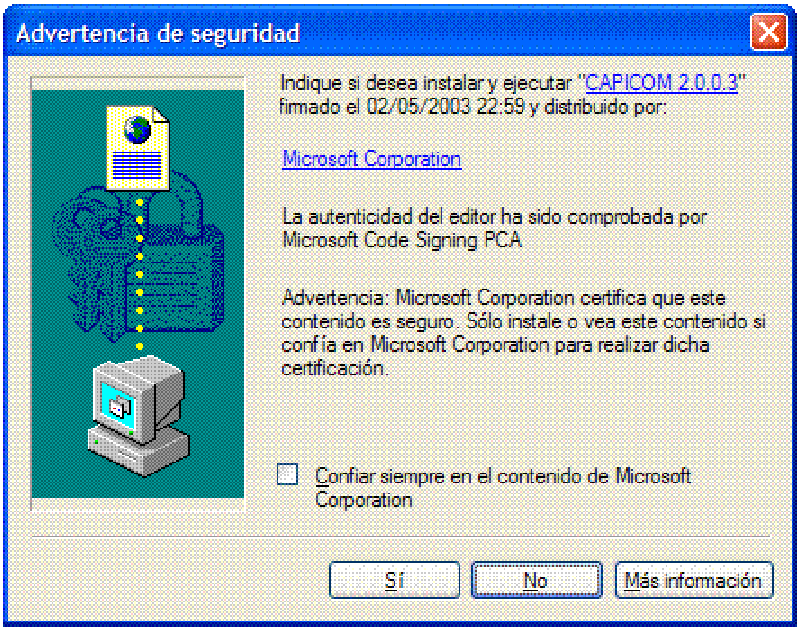
Formas de Acceso

Para acceder a la aplicación y participar en la junta, para emitir instrucciones de voto de forma electrónica, o para obtener tarjetas para votar o delegar a distancia por entrega o correo postal, o para acceder al servicio de derecho de información; es necesario que usted se identifique para verificar que es un accionista válido y puede participar en la junta. Para ello, necesitará disponer de un certificado electrónico.

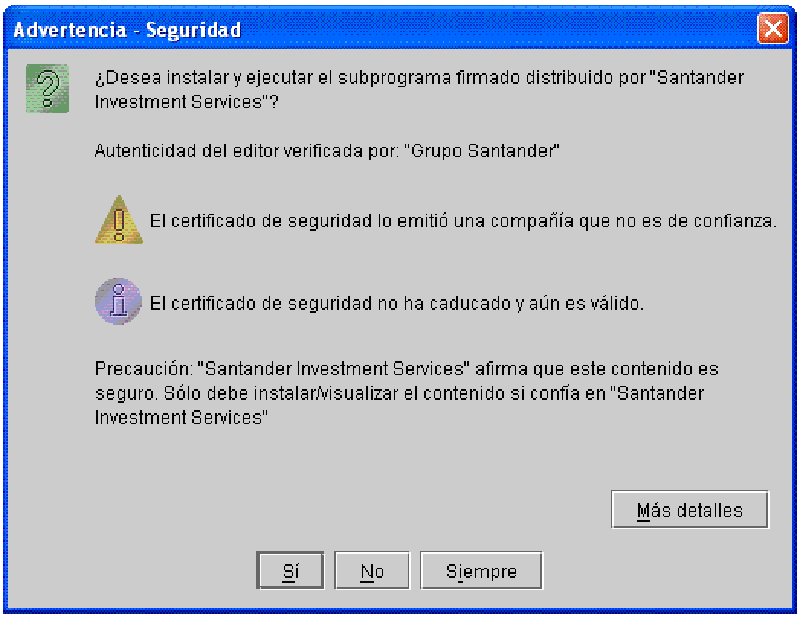
En el caso de no disponer de un certificado electrónico válido para participar en la junta, emitido por algún Prestador de Servicios de Certificación de confianza; podrá obtener información y solicitarlo accediendo a los enlaces de la sección ***Prestadores de servicios de certificación***.

Además en el caso de que su ordenador no disponga de un software de firma electrónica, la aplicación lo descargará automáticamente. Este software de firma es necesario para usar certificados electrónicos, y si usted no se lo descarga no podrá acceder a las funcionalidades de la aplicación que los requieran. Para su descarga, en función del navegador utilizado, le aparecerán las siguientes pantallas.

Explorer



Otros navegadores



Una vez comprobado que usted es un accionista válido para participar en la junta, se le mostrará su posición, informando todas sus cuentas de valores en la que es titular de las mismas. En caso de duda o aclaración en la información presentada, deberá ponerse en contacto con la Oficina de Atención al Accionista, para ello tiene un acceso en el menú lateral, dentro del grupo Enlaces.

En la lista se refleja los títulos de las distintas cuentas de valores, así como su situación actual. De tal forma que si la votación aún no se ha realizado, aparecerá el literal *Sin procesar*, por contra si ya hemos participado con una determinada cuenta, aparecerá un literal indicando quién ha realizado la votación, y en el caso de delegar el voto, se mostrará sobre quién se ha delegado.

Finalmente le aparecerán en un recuadro las operaciones que puede realizar. Estas opciones serán diferentes si lo que pretende es obtener tarjetas, o si es participar en la junta. Para ver todas las opciones disponibles deberá consultar las condiciones asociadas a cada proceso. En la página de bienvenida, o en el menú lateral, podrá encontrar un acceso al documento con las condiciones a cumplir.

Nota: Si usted se ha identificado en la aplicación, a través de un certificado electrónico, podrá acceder a cualquier servicio que requiera dicho dispositivo. Para ver las formas de acceso que requieren cada proceso, por favor consulte las condiciones de participación en la junta.

¿Qué es la firma electrónica?

La firma digital es un mecanismo que permite firmar un documento electrónico de forma que se garanticen las siguientes condiciones:

- Identificación de la persona que firma el documento (Autenticidad).
- Imposibilidad de manipulación del documento por alguien distinto del firmante (Integridad).
- Imposibilidad de repudio de la firma (No repudio).

Siguiendo las pautas de la Directiva 1999/93/CE, la Ley define la Firma Electrónica Reconocida como aquella basada en un Certificado Reconocido y generada mediante un dispositivo seguro de creación de firma. La Ley otorga equivalencia funcional y legal con la firma manuscrita.

Temas relacionados:

- Autoridades de certificación.
- Certificados digitales.
- Time stamping.
- Proceso de firma digital.
- Verificación de la firma digital.

Autoridades de certificación

La Ley 59/2003 de Firma Electrónica define a los Prestadores de Servicios de Certificación o Autoridades de Certificación (AC) como los sujetos que hacen posible el empleo de la firma electrónica mediante la expedición de certificados electrónicos.

Están obligados a efectuar una tutela y gestión permanente de los certificados que emiten estando obligados para ello a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados.

La AC al hacerse responsable de los certificados que emite, dando fe de la relación existente entre los datos que figuran en el certificado y la persona o entidad que lo solicita, deberá hacer un control estricto sobre la exactitud y veracidad de los datos del certificado.

Para solicitar un certificado a una AC la persona o entidad interesada debe cumplir unos procedimientos previos, confeccionando un documento, denominado **Requerimiento de Certificación** en el que figuran los datos representativos del solicitante y su clave pública.

Estos datos se presentan normalmente a entidades intermedias, **Autoridades de Registro** autorizadas por las AC, y cuya misión es comprobar la validez de los datos presentados en el Requerimiento de Certificación.

Certificados Digitales

Un Certificado Electrónico de Usuario es un conjunto de datos que engloba al menos la siguiente información:

- Identificación del Titular del Certificado.
- Datos propios del certificado: Número de Serie, Autoridad de Certificación que lo emitió, Fechas de emisión y caducidad, etc.
- Una pareja de claves: Clave Pública y Clave Privada. Esta pareja de claves tiene la propiedad de que lo que se cifra con la clave pública sólo se puede descifrar con la clave privada y viceversa.
- Firma electrónica de la Autoridad de Certificación que garantiza su autenticidad.

La utilidad fundamental de un Certificado es garantizar la relación entre una persona, física o jurídica, y su clave pública de forma que otros puedan utilizar con garantía dicha clave pública en las comunicaciones cifradas entre ellos.

Existen dos tipos de certificados en función de dónde quedan guardados los datos:

- El certificado de tipo software queda almacenado en el disco duro del PC.
- El certificado de tipo hardware queda almacenado en una tarjeta externa de la que no salen las claves.

La Ley define una clase particular de certificados electrónicos denominados Certificados Reconocidos, que son los que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los Certificados Reconocidos son una pieza fundamental de la Firma Electrónica Reconocida.

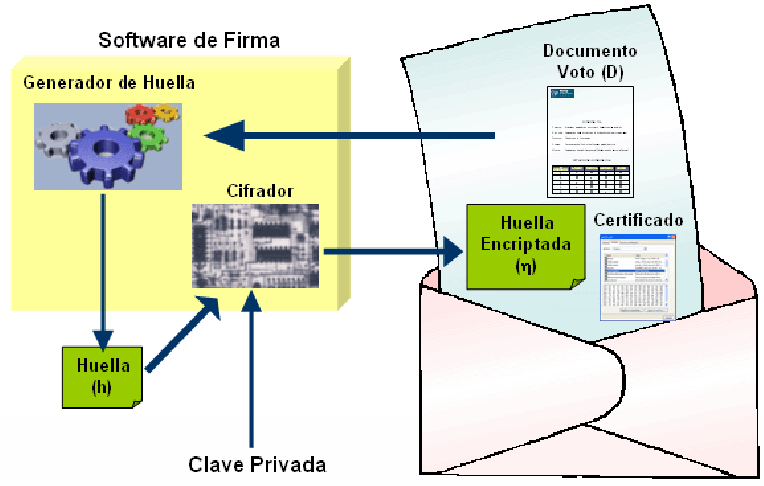
Time Stamping

El servicio de Sello de Tiempo o Time Stamping permite incluir en la firma de un documento una marca segura de fecha y hora.

Este servicio se puede utilizar para certificar el instante en que se hace la comprobación de la validez de un certificado.

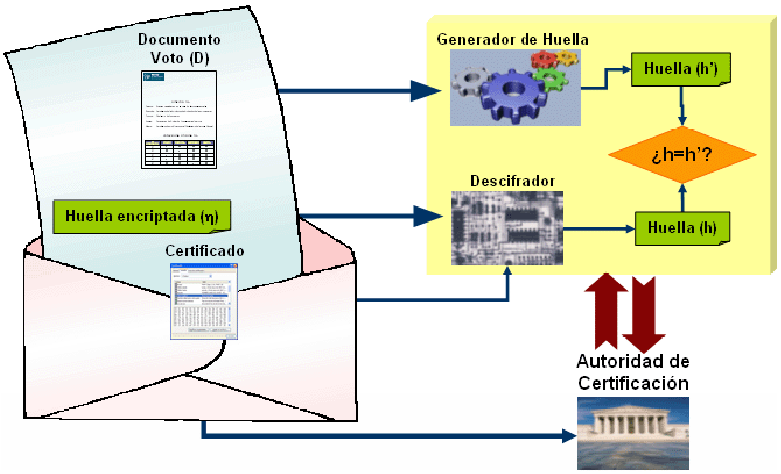
En general las Autoridades de Certificación (ACs) son las que ofrecen este servicio y en este time stamping se las conoce como TS.

Proceso Firma Digital



- El emisor genera el documento que desea enviar al receptor (por ejemplo, el documento con las votaciones generadas).
- Al documento se le aplica una función hash, mediante la cual obtiene un resumen del documento o huella.
- Se cifra la huella utilizando la clave privada del emisor
- Se envía al receptor los siguientes elementos:
    - El cuerpo del documento, que es el documento en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública del receptor.
    - La firma del documento, que a su vez se compone de dos elementos:
        - La huella cifrada con la clave privada del emisor.
        - El certificado digital del emisor, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada de la Autoridad de Certificación.

Verificación Firma Digital



- El receptor recibe los siguientes elementos:
    - El cuerpo del documento, que es el documento en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública del receptor.
    - La firma del documento, que a su vez se compone de dos elementos:
        - La huella cifrada con la clave privada del emisor.
        - El certificado digital del emisor, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada de la Autoridad de Certificación.
- Descifra el Certificado Digital del emisor, utilizando para ello la clave pública de la Autoridad de Certificación que ha expedido dicho certificado. Esa clave pública se tomará, por ejemplo, de la página Web de la AC en la que existirá depositada dicha clave pública a disposición de todos los interesados.

- Una vez descifrado el Certificado, se podrá acceder a la clave pública del emisor, que era uno de los elementos contenidos en dicho certificado. Además podrá saber a quién corresponde dicha clave pública, dado que los datos personales del titular de la clave constan también en el certificado.
- El receptor utilizará la clave pública del emisor obtenida del certificado digital para descifrar la huella.
- El receptor aplicará al cuerpo del documento, que aparece en claro o no cifrado, la misma función hash que utilizó el emisor con anterioridad, obteniendo igualmente el receptor un mensaje-resumen o huella. Si el cuerpo del documento también ha sido cifrado para garantizar la confidencialidad del mismo, previamente el receptor deberá descifrarlo utilizando para ello su propia clave privada (recordemos que el cuerpo del documento había sido cifrado con la clave pública del receptor)
- El receptor comparará la huella recibida del emisor con la huella obtenida por el mismo. Si ambas huellas coinciden totalmente significa lo siguiente:
    - El documento no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.
    - La huella descifrada por el receptor con la clave pública del emisor ha sido necesariamente cifrada con la clave privada del emisor y, por tanto, proviene necesariamente del emisor.
    - Como el certificado digital nos dice quién es el emisor, podemos concluir que el documento ha sido firmado digitalmente por el emisor, siendo el emisor una persona con identidad determinada y conocida.

Por el contrario, si las huellas no coinciden, quiere decir que el documento ha sido alterado por un tercero durante el proceso de transmisión, y si la huella descifrada por el receptor es ininteligible quiere decir que no ha sido cifrado con la clave privada del emisor. En resumen, que el documento no es auténtico o que el documento no ha sido firmado por el emisor sino por otra persona.

Cómo utilizar el DNI electrónico

Si usted ya dispone de un DNI electrónico:

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que nos permitirán el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en el DNI electrónico. A continuación le informamos los pasos a seguir, para utilizar su DNI electrónico, en la aplicación:

- Verifique que ha conectado el lector de tarjetas del DNI electrónico a su ordenador
- Verifique que previamente ha instalado el software del driver de acceso del lector de tarjetas. Este software normalmente se distribuye con el propio lector
- Para acceder al certificado electrónico, existente en su tarjeta DNI electrónico, deberá tener instalado el software del módulo criptográfico. Este módulo criptográfico en entornos Microsoft Windows se denomina CSP (Cryptographic Service Provider); en entornos UNIX/Linux o MAC se denominado PKCS#11. A continuación le presentamos un enlace donde podrá descargarse estos componentes. Descargas

Esta información la puede ampliar en la Web del DNI electrónico del Ministerio del Interior, a través del siguiente enlace, Web DNI electrónico

Si usted aún no dispone de un DNI electrónico:

Para obtener su DNI electrónico deberá acudir a una Oficina de expedición, a través del siguiente enlace podrá consultar los pasos a realizar. ***http://www.dnielectronico.es/como_utilizar_el_dnie/***

Prestadores de Servicios de Certificación de Confianza

Si usted accede a la aplicación de voto electrónico mediante un Certificado Digital, deberá disponer bien de un certificado electrónico emitido por alguno de los siguientes Prestadores de Servicios de Certificación, o bien poseer el Documento Nacional de Identidad electrónico (DNIe).

Si no dispone de un certificado válido o del Documento Nacional de Identidad electrónico (DNIe), podrá obtener información y solicitarlo accediendo al enlace asociado a cada uno de los Prestadores de Servicios de Certificación.

Prestadores de Servicios de Certificación

DNI ELECTRONICO	**http://www.dnielectronico.es/**
FABRICA NACIONAL DE MONEDA Y TIMBRE	**http://www.cert.fnmt.es/**