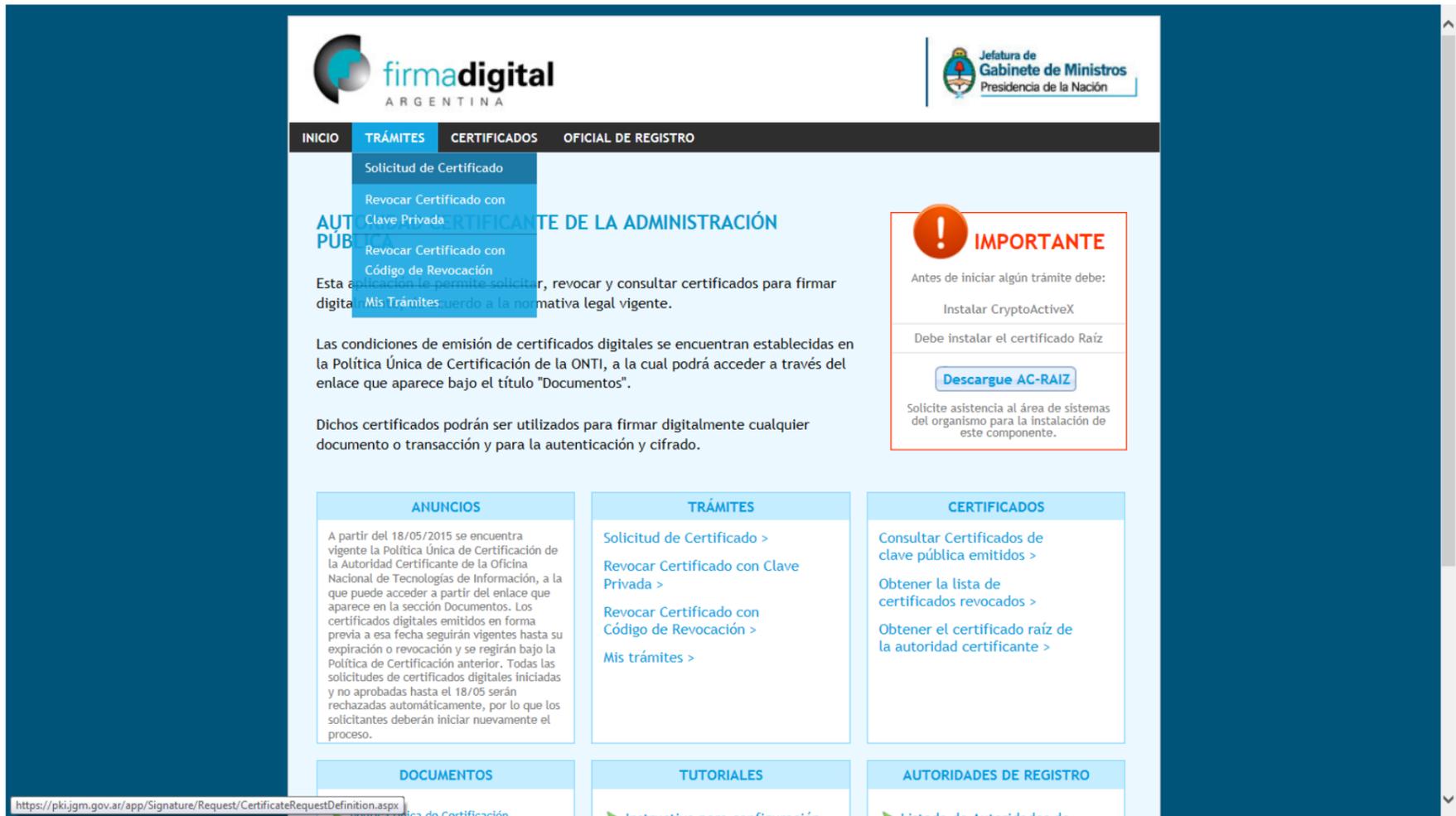


Tutorial de solicitud de certificado de Firma Digital por SOFTWARE

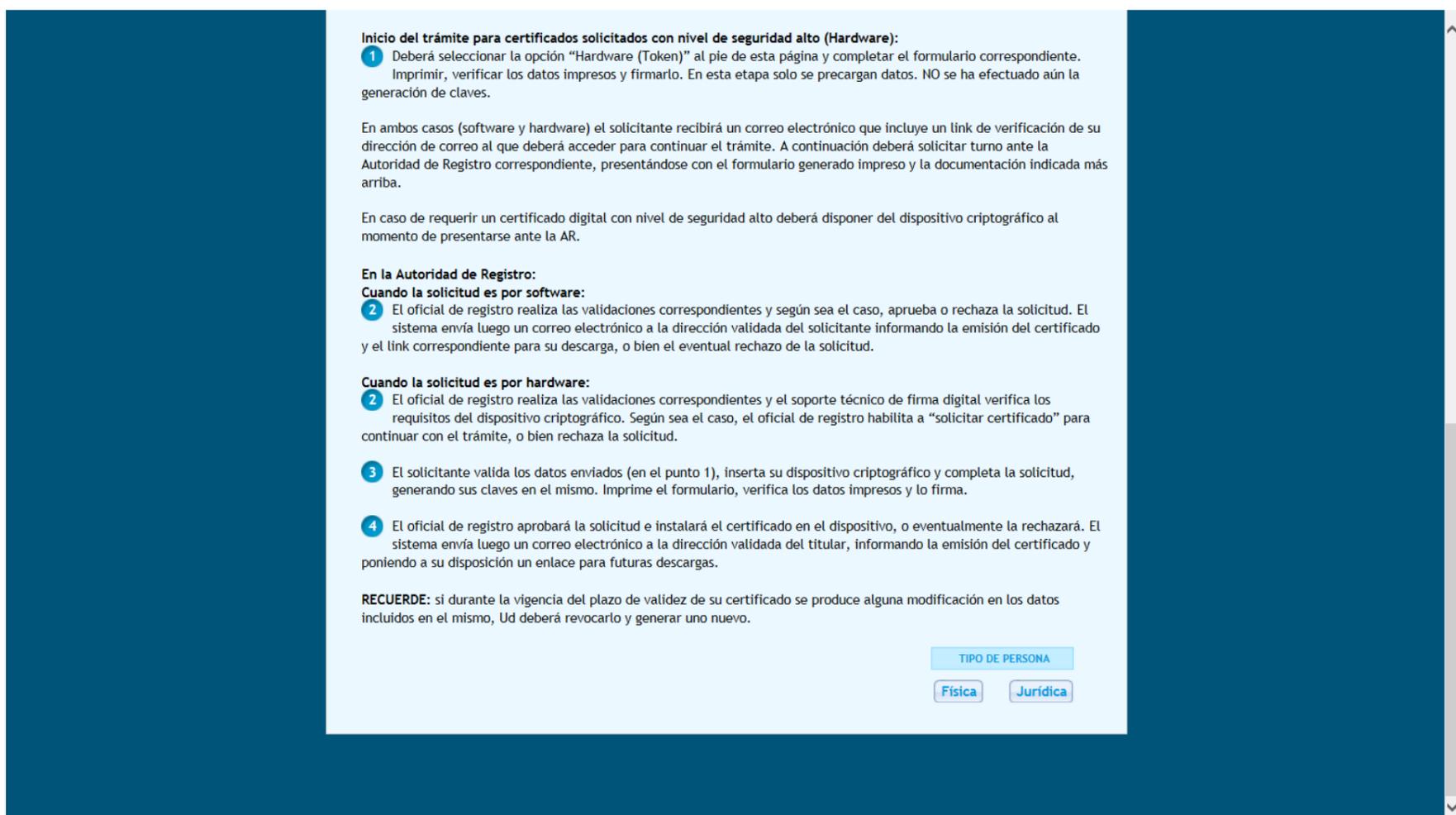
Importante: la solicitud debe ser realizada en la PC y con el usuario que usara la Firma Digital.

- 1) En <https://pki.jgm.gov.ar/app/> acceder a la pestaña **Tramites** opción **Solicitud de Certificado**.



The screenshot shows the 'Solicitud de Certificado' page on the firmadigital website. The page features a navigation menu at the top with options: INICIO, TRÁMITES, CERTIFICADOS, and OFICIAL DE REGISTRO. The main content area includes a header with the firmadigital logo and the text 'AUTORIDAD CERTIFICANTE DE LA ADMINISTRACIÓN PÚBLICA'. Below this, there is a section titled 'Esta aplicación le permite solicitar, revocar y consultar certificados para firmar digitalmente. Mis Trámites: acuerdo a la normativa legal vigente.' followed by a paragraph explaining the conditions of issuance of digital certificates according to the ONTI policy. A prominent orange box with a warning icon and the word 'IMPORTANTE' contains instructions: 'Antes de iniciar algún trámite debe: Instalar CryptoActiveX' and 'Debe instalar el certificado Raíz', with a 'Descargue AC-RAIZ' button. At the bottom, there are several category buttons: ANUNCIOS, TRÁMITES, CERTIFICADOS, DOCUMENTOS, TUTORIALES, and AUTORIDADES DE REGISTRO. The URL at the bottom of the browser window is 'https://pki.jgm.gov.ar/app/Signature/Request/CertificateRequestDefinition.aspx'.

- 2) En la página Solicitud de Certificado se encuentran los requerimientos y la guía paso a paso para solicitar certificados digitales. Luego de leer lo detallado seleccionar al final de la página el tipo de persona, **Física o Jurídica** según corresponda.



The screenshot shows the 'Inicio del trámite para certificados solicitados con nivel de seguridad alto (Hardware)' section. It contains a numbered list of steps:

- 1) Deberá seleccionar la opción "Hardware (Token)" al pie de esta página y completar el formulario correspondiente. Imprimir, verificar los datos impresos y firmarlo. En esta etapa solo se precargan datos. NO se ha efectuado aún la generación de claves.
- 2) El oficial de registro realiza las validaciones correspondientes y según sea el caso, aprueba o rechaza la solicitud. El sistema envía luego un correo electrónico a la dirección validada del solicitante informando la emisión del certificado y el link correspondiente para su descarga, o bien el eventual rechazo de la solicitud.
- 3) El solicitante valida los datos enviados (en el punto 1), inserta su dispositivo criptográfico y completa la solicitud, generando sus claves en el mismo. Imprime el formulario, verifica los datos impresos y lo firma.
- 4) El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada del titular, informando la emisión del certificado y poniendo a su disposición un enlace para futuras descargas.

 Below the steps, there is a 'RECUERDE:' section stating that if any modification occurs during the validity of the certificate, the user must revoke it and generate a new one. At the bottom right, there is a 'TIPO DE PERSONA' section with two buttons: 'Física' and 'Jurídica'.

3) En la página siguiente seleccionar **Software**.

generación de claves.

En ambos casos (software y hardware) el solicitante recibirá un correo electrónico que incluye un link de verificación de su dirección de correo al que deberá acceder para continuar el trámite. A continuación deberá solicitar turno ante la Autoridad de Registro correspondiente, presentándose con el formulario generado impreso y la documentación indicada más arriba.

En caso de requerir un certificado digital con nivel de seguridad alto deberá disponer del dispositivo criptográfico al momento de presentarse ante la AR.

En la Autoridad de Registro:

Cuando la solicitud es por software:

- El oficial de registro realiza las validaciones correspondientes y según sea el caso, aprueba o rechaza la solicitud. El sistema envía luego un correo electrónico a la dirección validada del solicitante informando la emisión del certificado y el link correspondiente para su descarga, o bien el eventual rechazo de la solicitud.

Cuando la solicitud es por hardware:

- El oficial de registro realiza las validaciones correspondientes y el soporte técnico de firma digital verifica los requisitos del dispositivo criptográfico. Según sea el caso, el oficial de registro habilita a "solicitar certificado" para continuar con el trámite, o bien rechaza la solicitud.
- El solicitante valida los datos enviados (en el punto 1), inserta su dispositivo criptográfico y completa la solicitud, generando sus claves en el mismo. Imprime el formulario, verifica los datos impresos y lo firma.
- El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada del titular, informando la emisión del certificado y poniendo a su disposición un enlace para futuras descargas.

RECUERDE: si durante la vigencia del plazo de validez de su certificado se produce alguna modificación en los datos incluidos en el mismo, Ud deberá revocarlo y generar uno nuevo.

TIPO DE DISPOSITIVO CRIPTOGRÁFICO

4) En la nueva página se encuentra el formulario de solicitud donde se completan los datos correspondientes.

firmadigital ARGENTINA

Jefatura de Gabinete de Ministros Presidencia de la Nación

INICIO TRÁMITES CERTIFICADOS OFICIAL DE REGISTRO

SOLICITUD DE CERTIFICADO

Datos del Solicitante

DATOS PERSONALES

Nombres *

Apellidos *

Tipo de Documento *

Número de documento *

País emisor *

Cuit/Cuil *

DATOS DE LA ORGANIZACIÓN

Organización *

Área de la que depende *

Cargo/Función *

Correo electrónico *

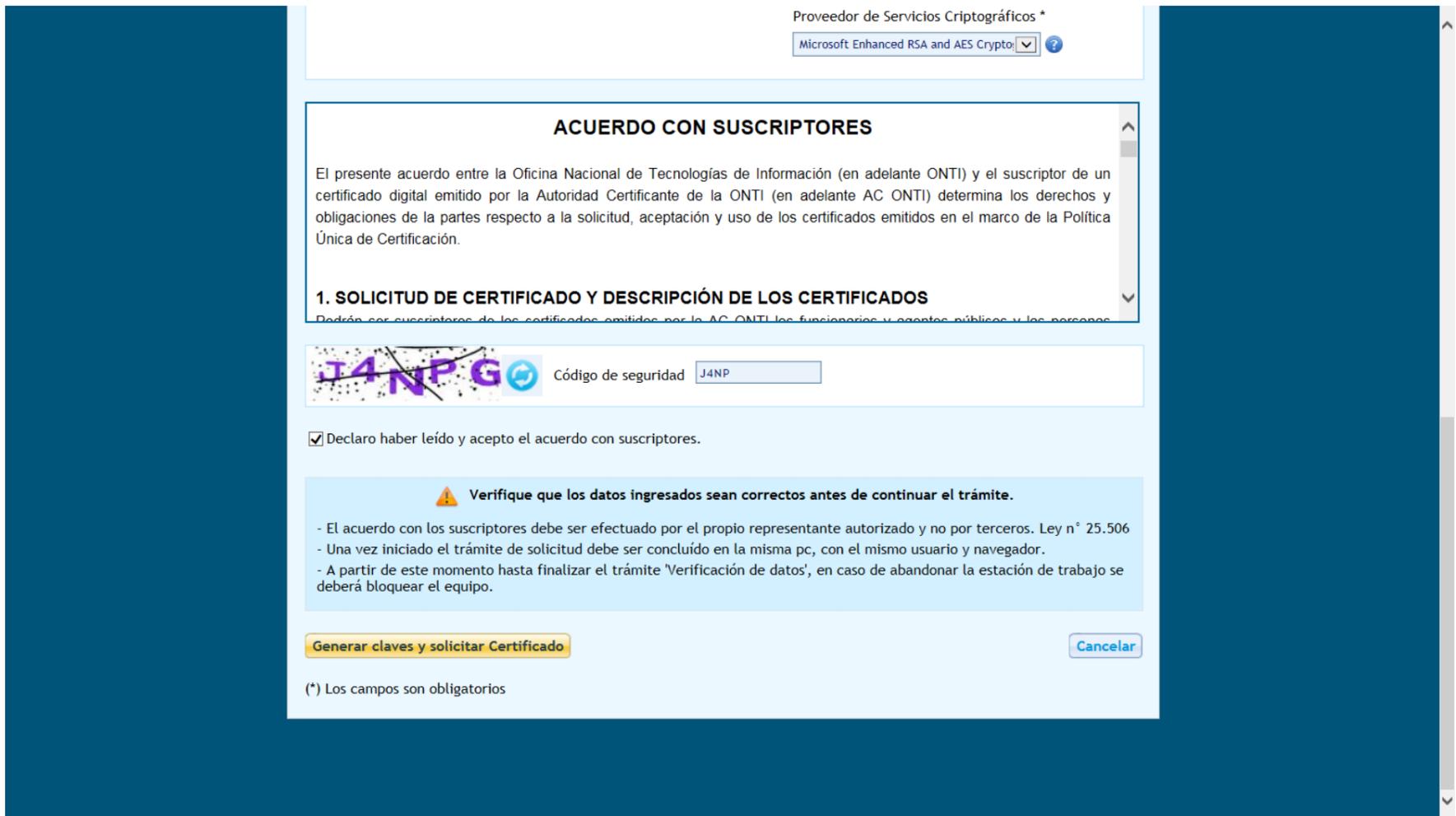
Provincia *

Localidad *

Aplicación

Autoridad de Registro *

5) Una vez completado en la misma página al final ir a **Generar claves y solicitar certificado**.



Proveedor de Servicios Criptográficos *

Microsoft Enhanced RSA and AES Crypto

ACUERDO CON SUSCRIPTORES

El presente acuerdo entre la Oficina Nacional de Tecnologías de Información (en adelante ONTI) y el suscriptor de un certificado digital emitido por la Autoridad Certificante de la ONTI (en adelante AC ONTI) determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política Única de Certificación.

1. SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS

Podrán ser suscriptores de los certificados emitidos por la AC ONTI los funcionarios y agentes públicos y las personas...

J4NP GO Código de seguridad J4NP

Declaro haber leído y acepto el acuerdo con suscriptores.

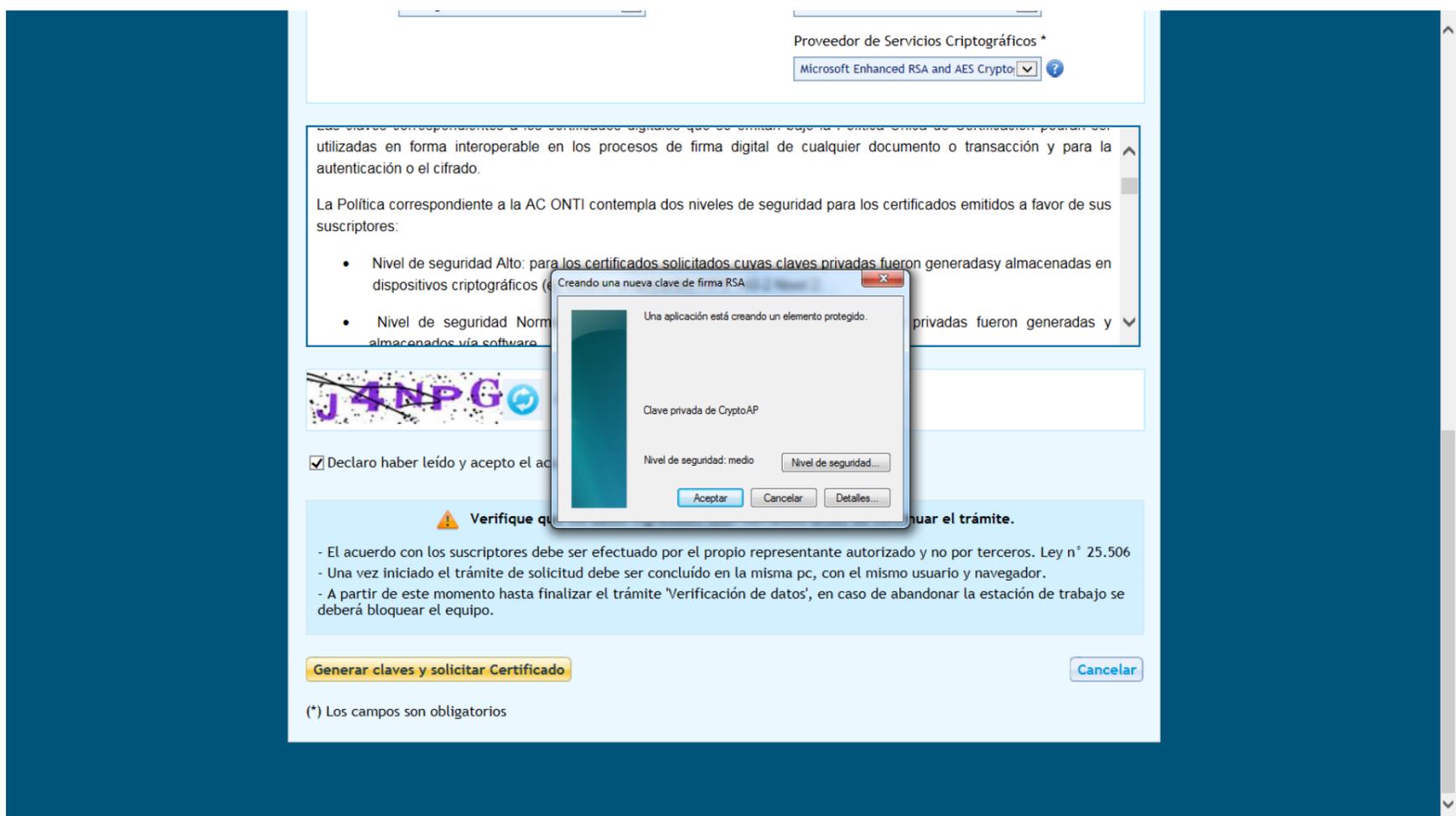
⚠ Verifique que los datos ingresados sean correctos antes de continuar el trámite.

- El acuerdo con los suscriptores debe ser efectuado por el propio representante autorizado y no por terceros. Ley n° 25.506
- Una vez iniciado el trámite de solicitud debe ser concluido en la misma pc, con el mismo usuario y navegador.
- A partir de este momento hasta finalizar el trámite 'Verificación de datos', en caso de abandonar la estación de trabajo se deberá bloquear el equipo.

Generar claves y solicitar Certificado Cancelar

(*) Los campos son obligatorios

6) Se le preguntara que nivel de seguridad quiere para su firma. Haga click en **Nivel de seguridad**.



Proveedor de Servicios Criptográficos *

Microsoft Enhanced RSA and AES Crypto

Las claves correspondientes a los certificados digitales que se emiten bajo la Política Única de Certificación pueden ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

La Política correspondiente a la AC ONTI contempla dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores:

- Nivel de seguridad Alto: para los certificados solicitados cuyas claves privadas fueron generadas y almacenadas en dispositivos criptográficos (e...
- Nivel de seguridad Normal: para los certificados solicitados cuyas claves privadas fueron generadas y almacenadas vía software.

J4NP GO

Declaro haber leído y acepto el acuerdo con suscriptores.

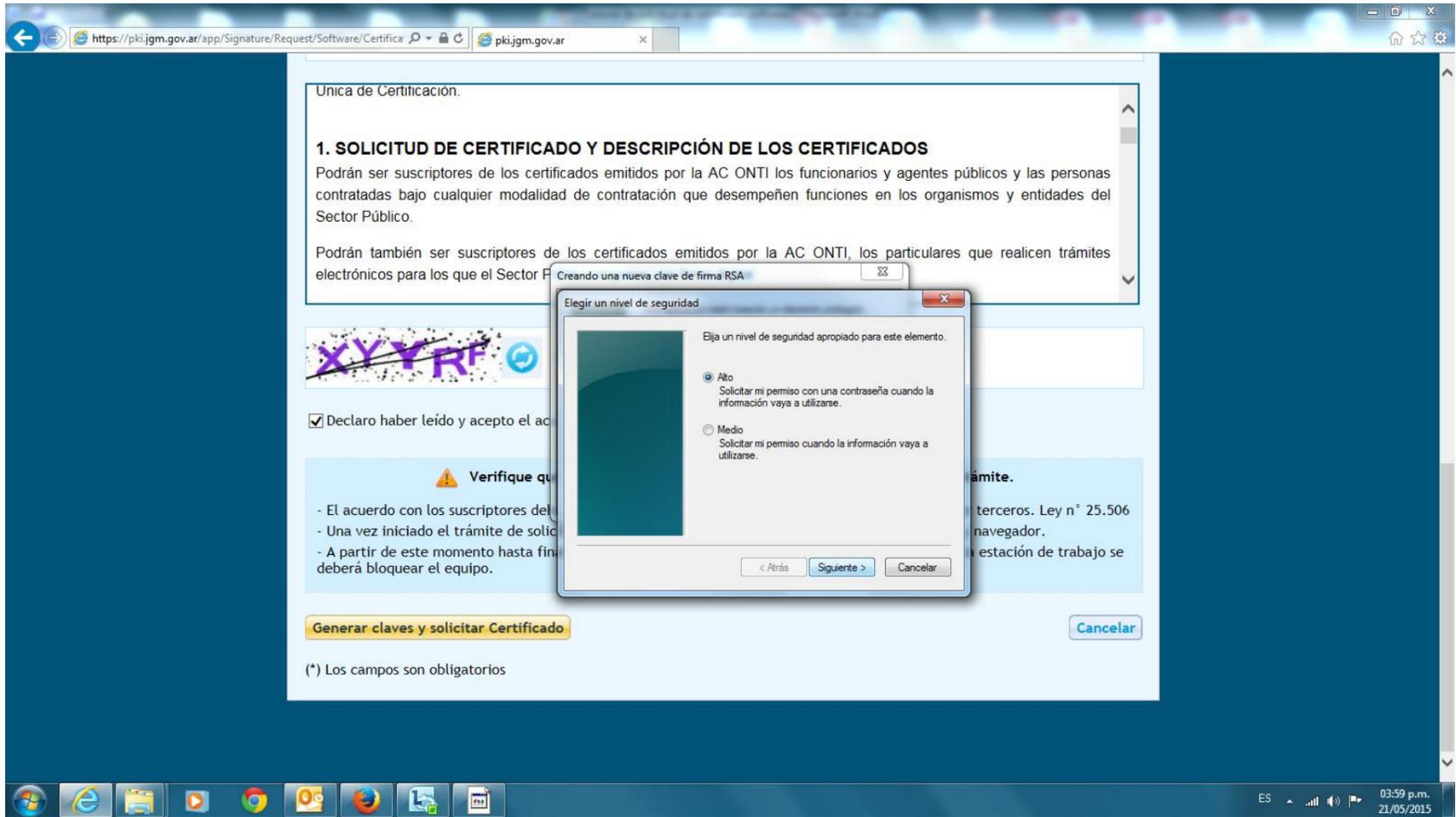
⚠ Verifique que los datos ingresados sean correctos antes de continuar el trámite.

- El acuerdo con los suscriptores debe ser efectuado por el propio representante autorizado y no por terceros. Ley n° 25.506
- Una vez iniciado el trámite de solicitud debe ser concluido en la misma pc, con el mismo usuario y navegador.
- A partir de este momento hasta finalizar el trámite 'Verificación de datos', en caso de abandonar la estación de trabajo se deberá bloquear el equipo.

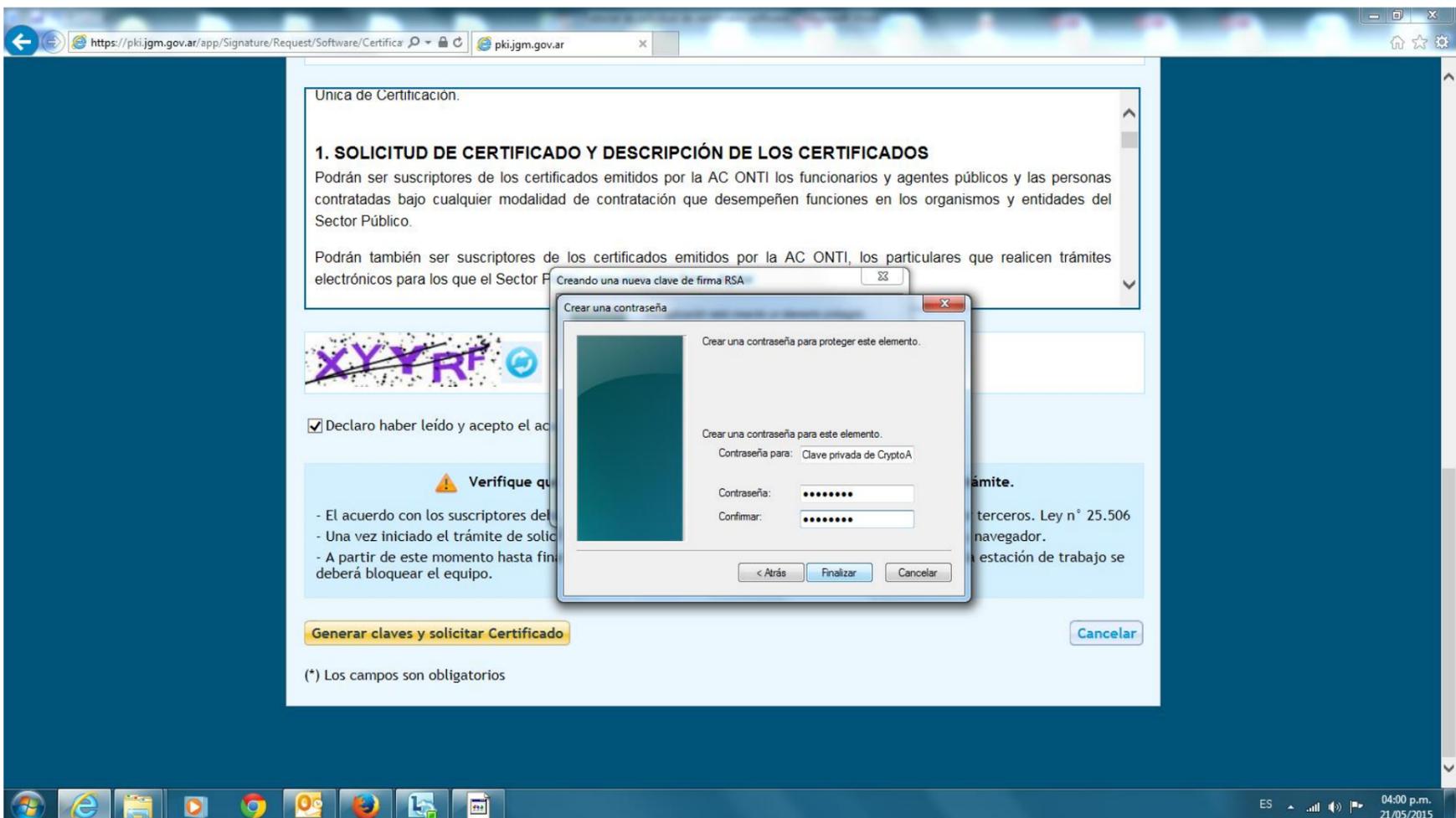
Generar claves y solicitar Certificado Cancelar

(*) Los campos son obligatorios

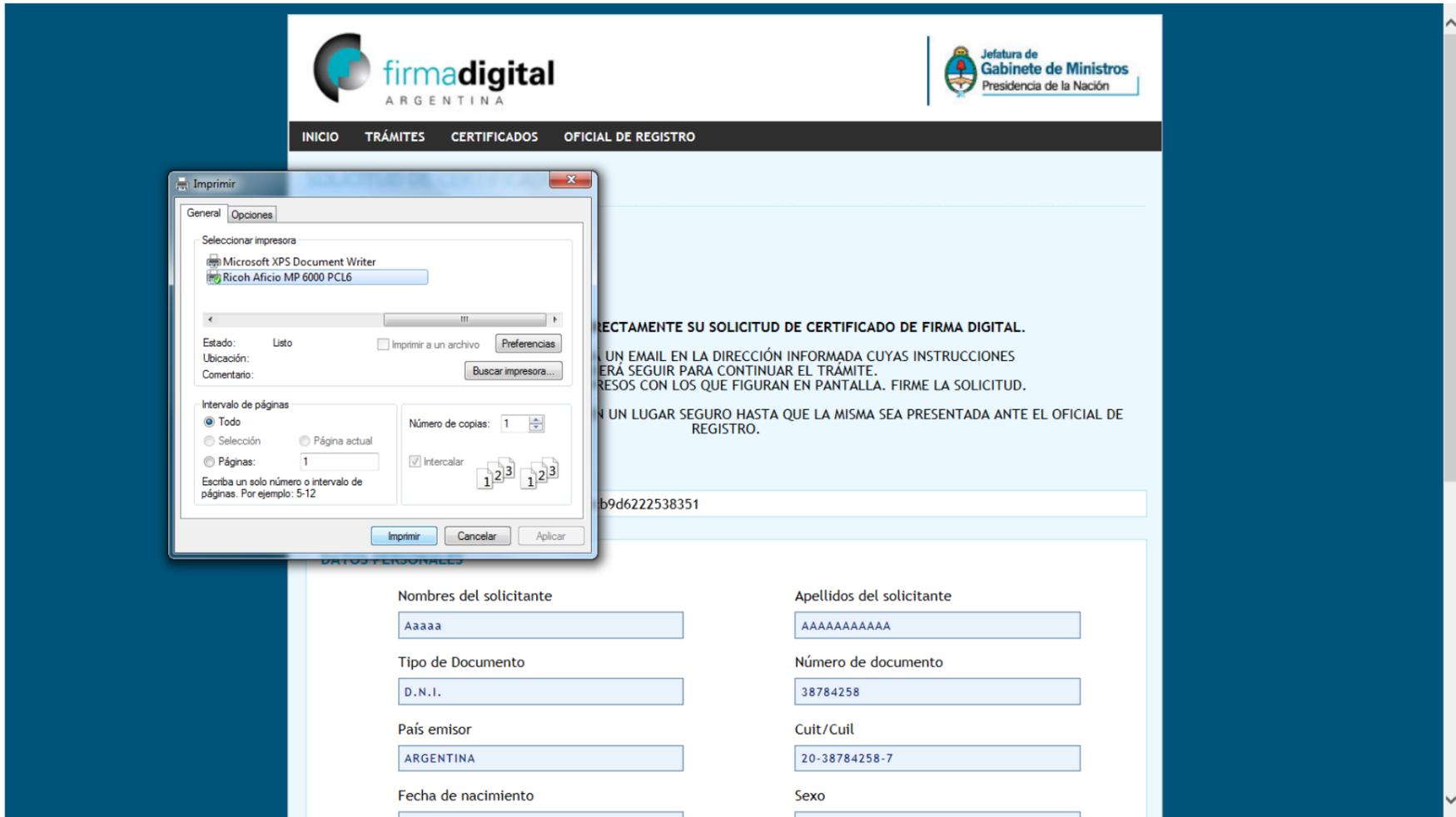
7) Seleccione nivel de seguridad ALTO y pulse en siguiente.



8) Se le pedirá establecer una contraseña. Cree una y haga click en **Aceptar**.



9) Aparecerá una ventana preguntándole si desea imprimir la solicitud. **IMPRIMA LA SOLICITUD Y FIRMELA EN EL CAMPO "FIRMA Y ACLARACION DEL SOLICITANTE"**



10) Le llegará un correo electrónico a la dirección utilizada para realizar el trámite. Debe seguir el hipervínculo incluido en el correo para confirmar la solicitud. Luego debe ponerse en contacto con un **Oficial de Registro** correspondiente a la Autoridad de Registro en la cual comenzó el trámite.