CESAR ROBERTO ROSALES MAQUERA
Sub Director de Servicios de Certificación Digital
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROSALES MAQUERA Cesar Roberto FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 03/05/2023 12:00:40-0500

HÉCTOR EDUARDO SARAVIA MARTÍNEZ
Director de Certificación y Servicios Digitales
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: SARAVIA MARTINEZ Hector Eduardo FAU 20295613620 hard
Motivo: En señal de conformidad
Fecha: 03/05/2023 13:36:39-0500

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DOCUMENTO TÉCNICO

VERSIÓN: 1.0	CÓDIGO: DT-DCSD/SDSCD-010

DIRECCIÓN: CERTIFICACIÓN Y SERVICIOS DIGITALES

SUB DIRECCIÓN: SERVICIOS DE CERTIFICACIÓN DIGITAL

GUÍA DE USUARIO: SOFTWARE DE FIRMA DIGITAL REFIRMA PCX

CLASIFICACIÓN:	PÚBLICA

RUBRO	NOMBRE	CARGO
ELABORADO POR:	Alejandro Javier Ramírez Salazar	Administrador de Plataforma EREP
REVISADO POR:	Cesar Roberto Rosales Maquera	Sub Director de Servicios de Certificación Digital
APROBADO POR:	Héctor Eduardo Saravia Martínez	Director de Certificación y Servicios Digitales

FIRMA DIGITAL

Firmado digitalmente por: RAMIREZ SALAZAR Alejandro Javier FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 25/04/2023 15:11:57-0500

Firmado digitalmente por: ORDOÑEZ PISCOYA Jose Alexander FAU 20295613620 hard
Motivo: En señal de conformidad
Fecha: 25/04/2023 17:12:02-0500

GUÍA DE USUARIO: SOFTWARE DE FIRMA DIGITAL REFIRMA PCX

1. OBJETIVO

Establecer las acciones, funciones y opciones que el usuario debe seguir para la operación del Software de Firma Digital ReFirma PCX, a fin de que les permita firmar y validar documentos digitales.

2. ALCANCE

Este documento es administrado por la Sub Dirección de Servicios de Certificación Digital - SDSCD de la Dirección de Certificación y Servicios Digitales - DCSD y es fuente de aplicación para el usuario, quien no requiere de preparación ni entrenamiento previo, sólo debe seguir las instrucciones dadas en el presente manual.
El contenido de este manual puede ser modificado o actualizado, según las competencias y exigencias requeridas.

3. CLASIFICACIÓN DE INFORMACIÓN

De acuerdo al listado de clasificación y acceso a la información, este documento es clasificado como **PÚBLICA**.

4. ROLES

Usuario: Es la persona que hace uso del Software de Firma Digital.

5. GLOSARIO DE TÉRMINOS

Autoridad Administrativa Competente (AAC)	Es el organismo público responsable de acreditar a las Entidades de Certificación (EC), a las Entidades de Registro o Verificación (ER) y a los Prestadores de Servicios de Valor Añadido (PSVA) públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el Reglamento de la Ley de Firmas y Certificados Digitales o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, quien la ejerce a través de la Dirección de la Gestión de la Infraestructura Oficial de la Firma Electrónica del Indecopi (DGI).
Certificado Digital	Es un documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación (EC) que vincula

	un par de llaves (una pública y otra privada) con una persona natural o jurídica confirmando su identidad digital.
Infraestructura Oficial de Firma Electrónica (IOFE):	Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (AAC), provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a la integridad de los documentos electrónicos; y a la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en la que participan Entidades de Certificación y Entidades de Registro o Verificación acreditadas ante la Autoridad Administrativa Competente (AAC), incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidad de Certificación para el Estado Peruano (ECEP), las Entidades de Registro o Verificación para el Estado Peruano (EREP) y los Prestadores de Servicios de Valor Añadido para el Estado Peruano (PSVA).
Lista de Certificados Digitales Revocados (CRL o LCR)	Lista en la que se deberán incorporar todos los certificados cancelados o revocados (cancelados de oficio) por la Entidad de Certificación, de acuerdo con lo establecido en el Reglamento de la Ley de firmas y certificados digitales.
Firma digital	La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
Planta PKI	El concepto PKI se refiere al acrónimo en inglés: Public Key Infrastructure y en la práctica corresponde a un centro de datos altamente especializado que contiene los equipos (hardware), programas computacionales (software) y el personal técnico idóneo, necesarios para cumplir con todos los procesos de certificación digital dentro de un marco regulado por la Infraestructura Oficial de Firma Electrónica (IOFE), cumpliendo, así con los estándares internacionales y procedimientos respectivos.
ReFirma-PCX	Aplicativo de escritorio que se instala desde una página web. Posterior a su instalación se puede ejecutar directamente desde los íconos de acceso directo creados en el escritorio y menú inicio de la computadora del usuario o desde la misma página web. Permite firmar digitalmente documentos en formato PAdES, CAdES y XAdES, realizando las validaciones requeridas para la generación de firmas digitales con valor legal.

TSL (Lista de Servicios de Confianza)	La Lista de Servicios de Confianza (Trust-service Status List - TSL) contiene los nombres y los certificados digitales de las Entidades Prestadoras de Servicios de Certificación consideradas confiables. Es decir, las que INDECOPI (la Autoridad Administrativa Competente y encargada de la TSL) ha acreditado conforme a la Ley de Firmas y Certificados Digitales, aprobada por Decreto Supremo 052-2008-PCM.
OCSP (Protocolo online de validación de certificados digitales)	Es el acrónimo de Online Certificate Status Protocol. OCSP es un protocolo utilizado para determinar el estado de vigencia de un certificado digital sin requerir el uso de una CRL. A diferencia de una verificación basada en CRL, la verificación con OCSP provee información en tiempo real.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

Una vez que se haya instalado el REFIRMA PCX el usuario puede realizar las siguientes opciones (Figura 1):

1. Firmar documentos PDF
2. Firmar cualquier documento
3. Firmar documentos XML
4. Validar PDF
5. Validar cualquier documento
6. Validar XML
7. Lista de Certificados de **Confianza**

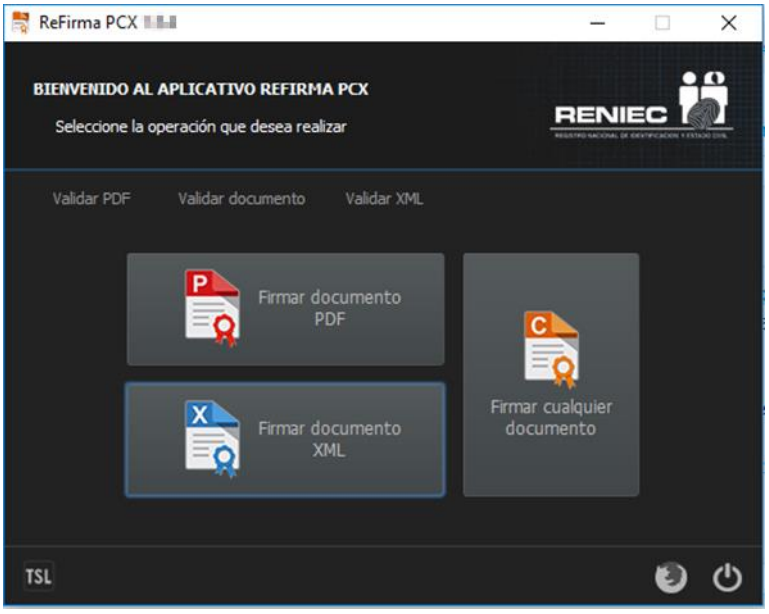

Figura 1 – Opciones del REFIRMA PCX

6.1. Firmar Documentos PDF

Esta opción permitirá firmar documentos PDF.

Realice los siguientes pasos para firmar los documentos:

1. Haga clic en la opción “Firmar documentos PDF”. (Figura 2)

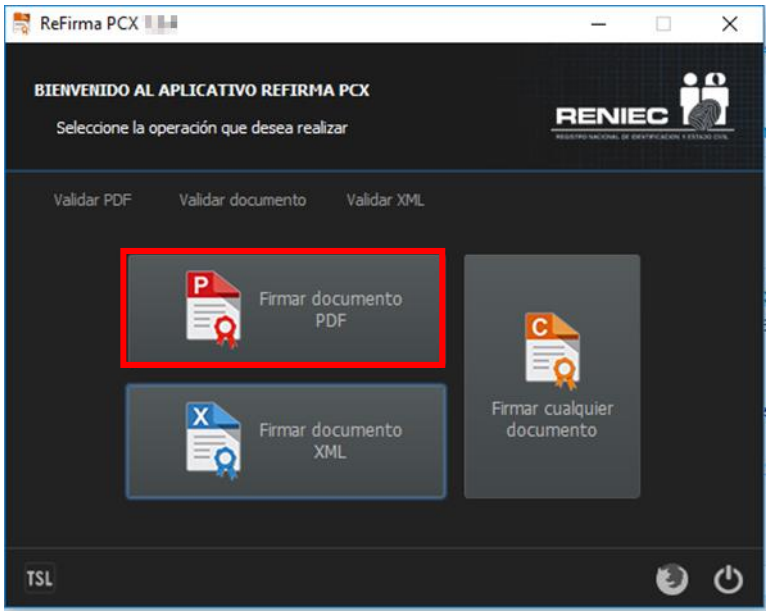

Figura 2 – Opcion firmar documentos PDF

2. Automáticamente le mostrará la siguiente pantalla para poder seleccionar el documento que desea firmar. Haga clic en la opción “Seleccionar PDF”. (Figura 3)

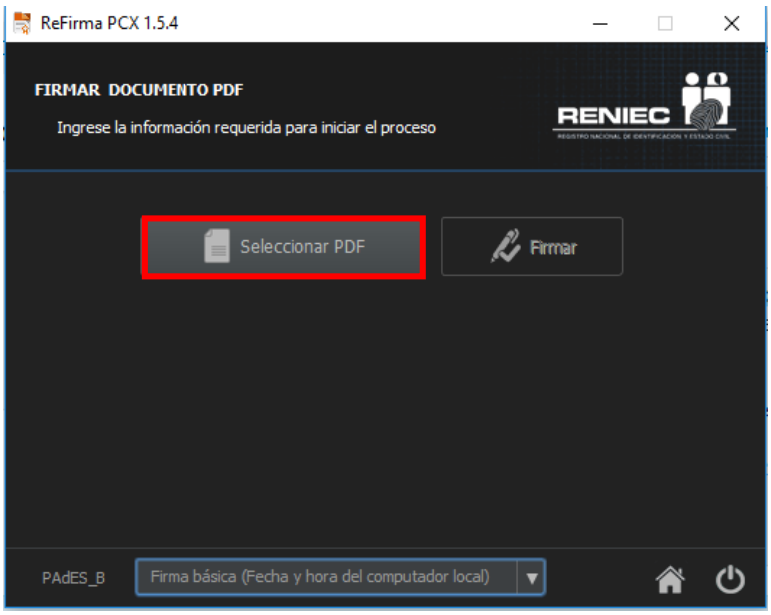

Figura 3 – Seleccionar archivo

3. Automáticamente se mostrará un cuadro de diálogo, elegir el documento que desea seleccionar y haga clic en el botón “Abrir”. (Figura 4)

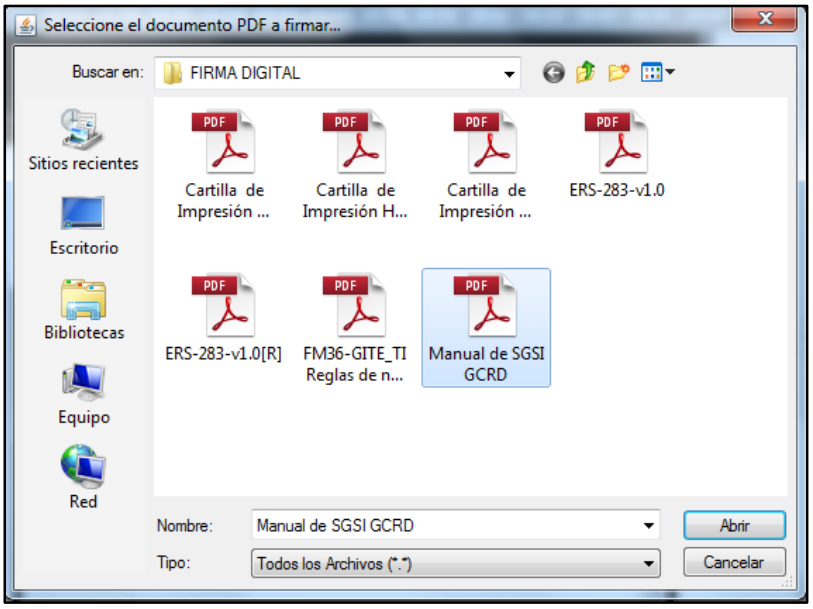

Figura 4 – Abrir archivo

4. Automáticamente se cargará el documento seleccionado, para poder firmar. (Figura 5)

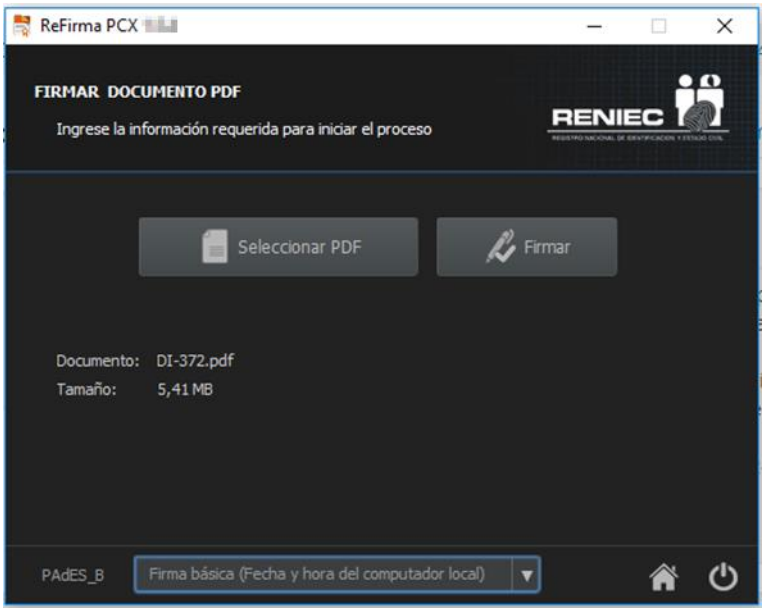

Figura 5 – Cargar documento.

5. Inserte el DNIe en la lectora para poder realizar la firma del documento.

6. Para firmar el documento debe de desplegar el combo de firma PAdES y seleccionar la firma que desea utilizar, teniendo en cuenta la descripción de firmas que se describe en la NOTA 01.

Figura 6 – Elegir firma.

7. Una vez seleccionada el tipo de firma que desea utilizar. Haga clic en el botón “Firmar”. (Figura 7)

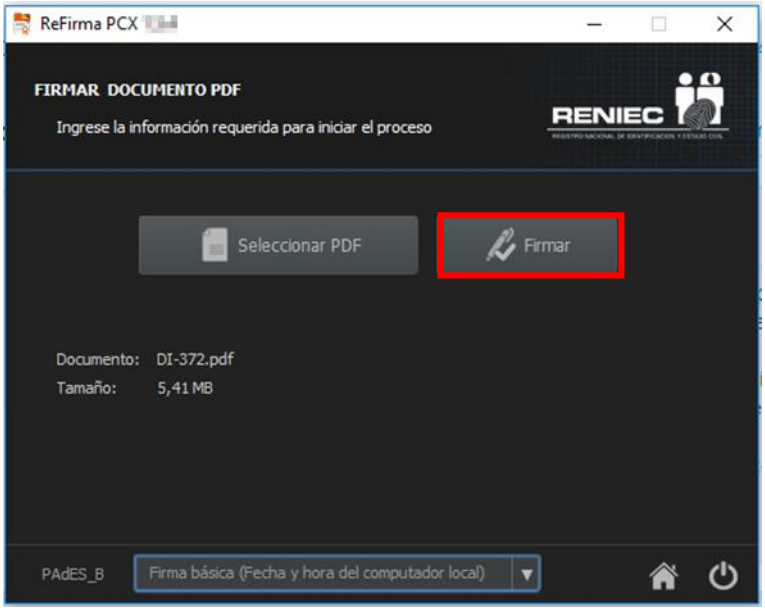

Figura 7 – Firmar documento.

8. Automáticamente aparecerá una pantalla con la lista de certificados digitales, seleccione el certificado digital y haga clic en el botón “Aceptar”. (Figura 8)

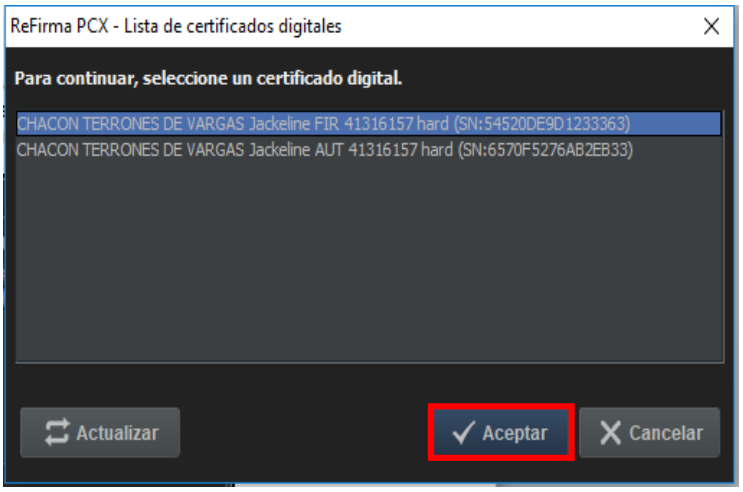

Figura 8 – Seleccionar Certificado Digital.

9. Para poder firmar el documento debe de ingresar el pin del DNIe del destinatario. una vez que ingresado haga clic en el botón “Aceptar” (Figura 9). El aplicativo verifica el PIN ingresado según lo descrito en la NOTA 02.

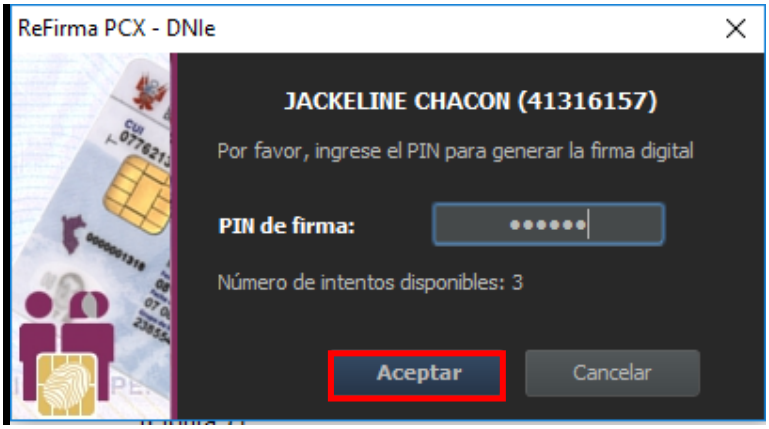

Figura 9 – Ingresar PIN.

10. Una vez que se terminó de firmar el documento se mostrará un mensaje que el archivo fue firmado correctamente y se encuentra en la misma ruta de donde seleccionó el documento, haga clic en el botón “Inicio” para volver a la pantalla inicial. (Figura 10)

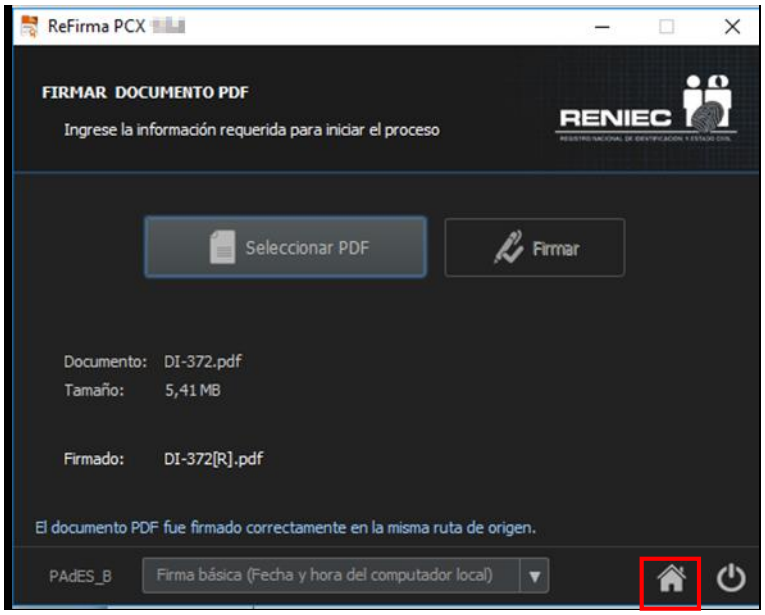

Figura 10 – Firmado correcto

6.2. Firmar Cualquier Documento

Esta opción permitirá firmar cualquier documento.

Realice los siguientes pasos para firmar cualquier tipo de documento:

1. Haga clic en la opción “Firmar cualquier documento”. (Figura 11)

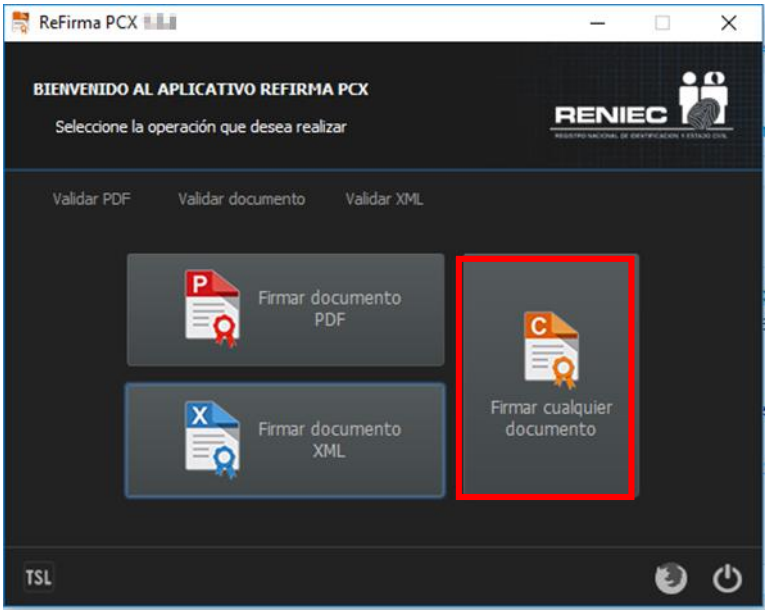

Figura 11 – Opcion firmar cualquier documento

2. Automáticamente le mostrará la siguiente pantalla para poder seleccionar el documento que desea firmar. Haga clic en la opción “Seleccionar Documento”. (Figura 12)

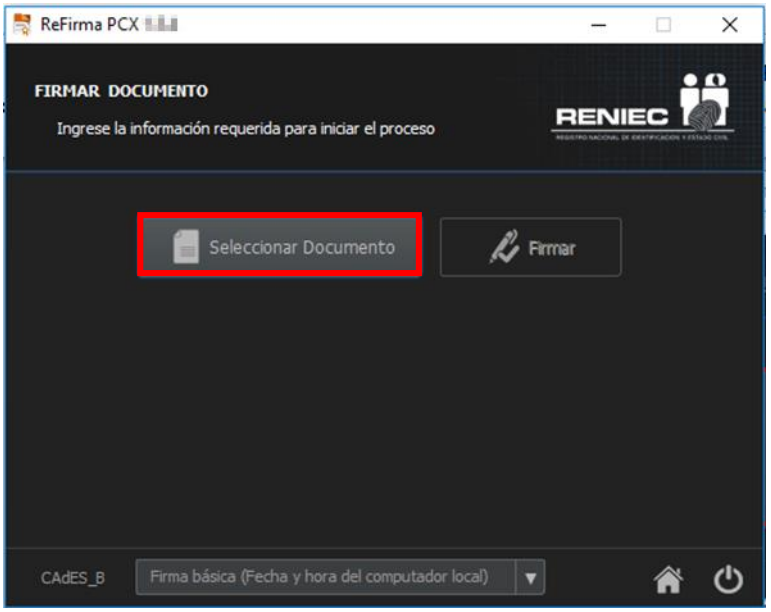

Figura 12 – Seleccionar documento

3. Automáticamente se mostrará un cuadro de diálogo, elegir el documento que desea seleccionar y haga clic en el botón “Abrir”. (Figura 13)

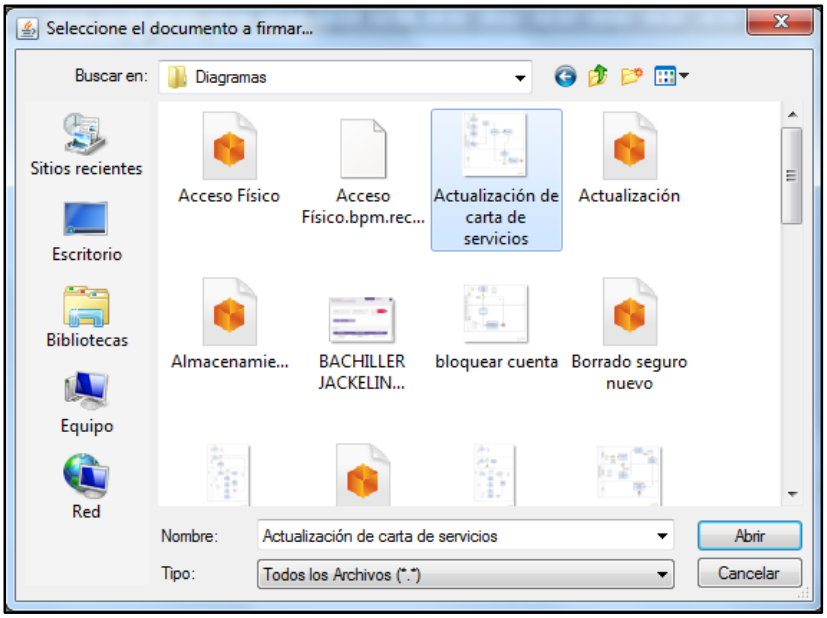

Figura 13 – Abrir archivo

4. Automáticamente se cargará el documento seleccionado, para poder firmar. (Figura 14)

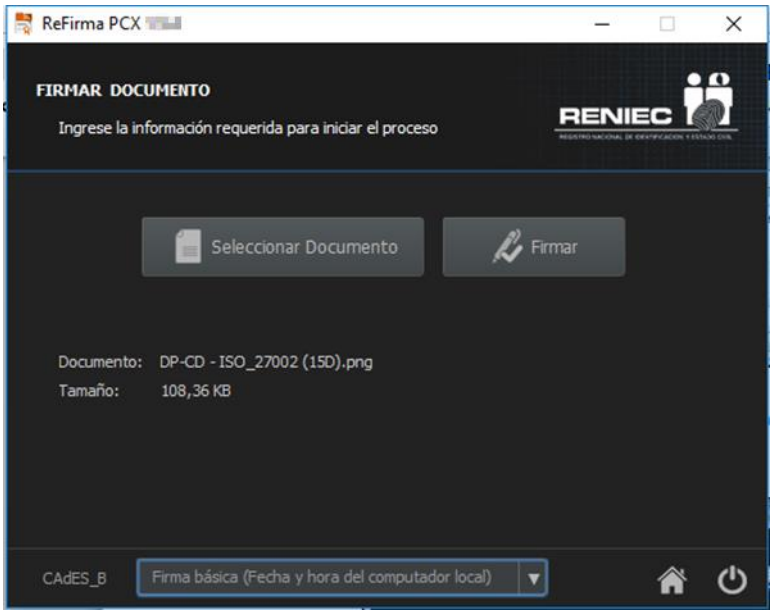

Figura 14 – Cargar documento.

5. Inserte el DNIe en la lectora para poder realizar la firma del documento.

6. Para firmar el documento debe de desplegar el combo de firma CAdES y seleccionar la firma que desea utilizar, teniendo en cuenta la descripción de firmas que se describe en la NOTA 01.

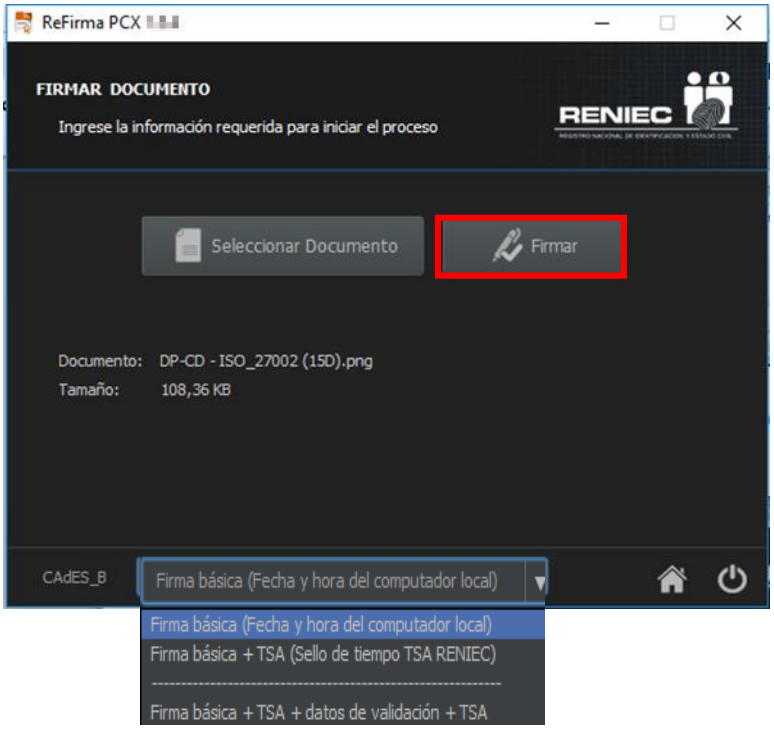

Figura 15 – Elegir firma.

7. Automáticamente aparecerá una pantalla con la lista de certificados digitales, seleccione el certificado digital y haga clic en el botón “Aceptar”. (Figura 16)

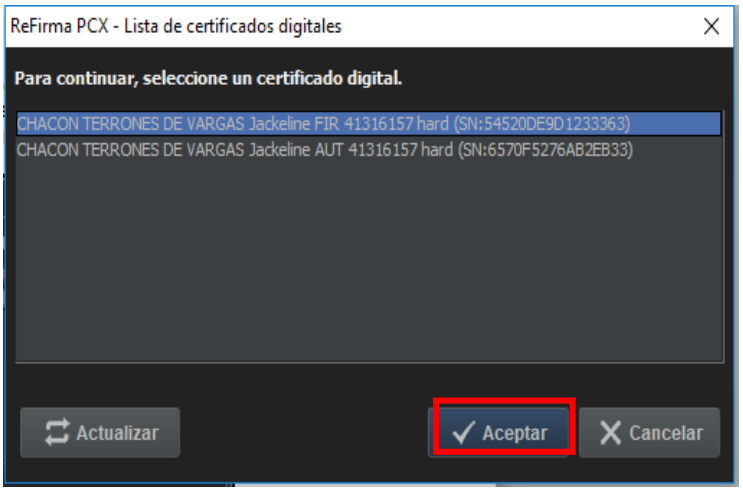

Figura 16 Seleccionar Certificado Digital.

8. Para poder firmar el documento debe de ingresar el pin del DNIe del destinatario. una vez que ingresado haga clic en el botón “Aceptar”. (Figura 17)

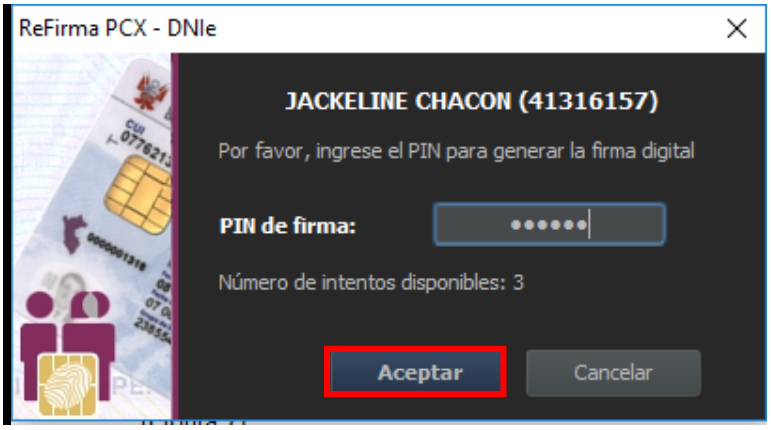

Figura 17 – Ingresar PIN.

9. Una vez que se terminó de firmar el documento se mostrará un mensaje que el archivo fue firmado correctamente y se encuentra en la misma ruta de donde seleccionó el documento, haga clic en el botón “Inicio” para volver a la pantalla inicial. (Figura 18)

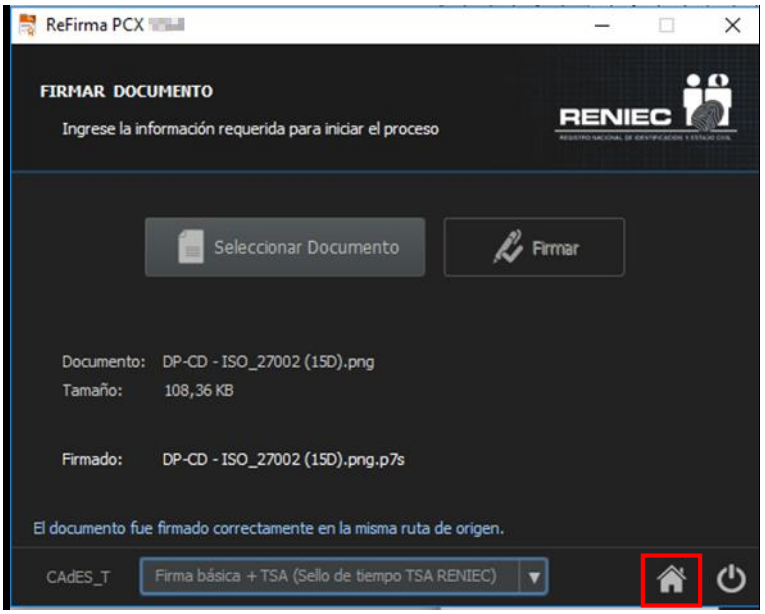

Figura 18 – Firmado correcto

6.3. Firmar Documento XML

Esta opción permitirá firmar documentos XML.

Realice los siguientes pasos para firmar documentos XML:

1. Haga clic en la opción “Firmar documento XML”. (Figura 19)

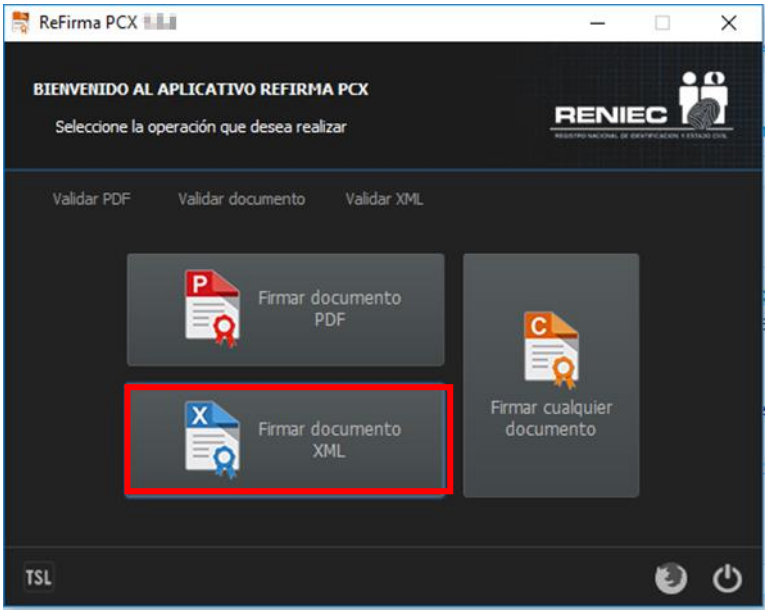

Figura 19 – Opcion firmar documento XML

2. Automáticamente le mostrará la siguiente pantalla para poder seleccionar el documento que desea firmar. Haga clic en la opción “Seleccionar XML”. (Figura 20)

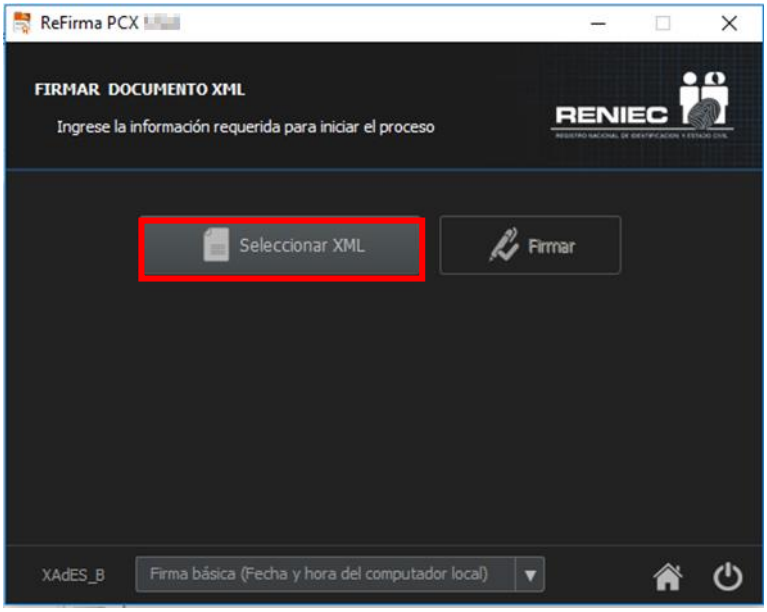

Figura 20 – Seleccionar archivo

3. Automáticamente se mostrará un cuadro de diálogo, elegir el documento que desea seleccionar y haga clic en el botón “Abrir”. (Figura 21)

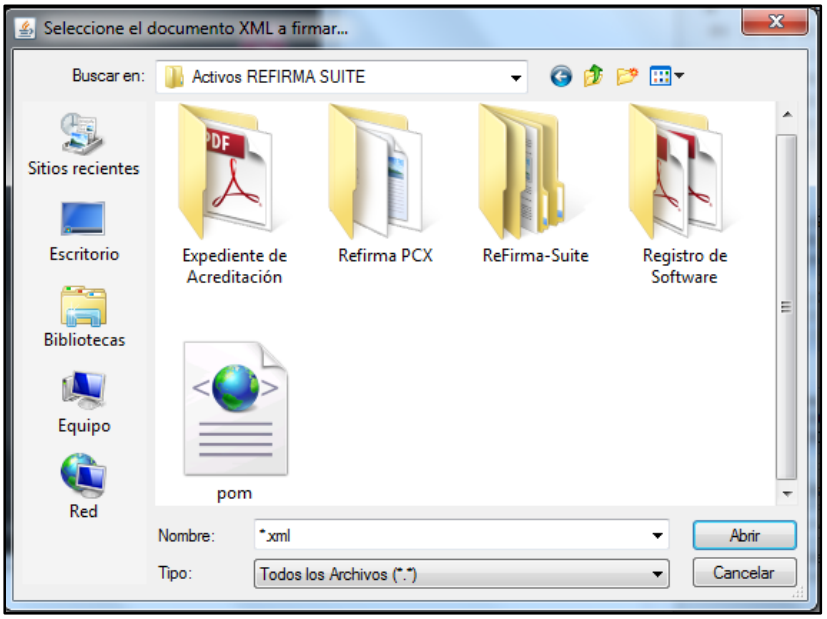

Figura 21 – Abrir archivo

4. Automáticamente se cargará el documento seleccionado, para poder firmar. (Figura 22)

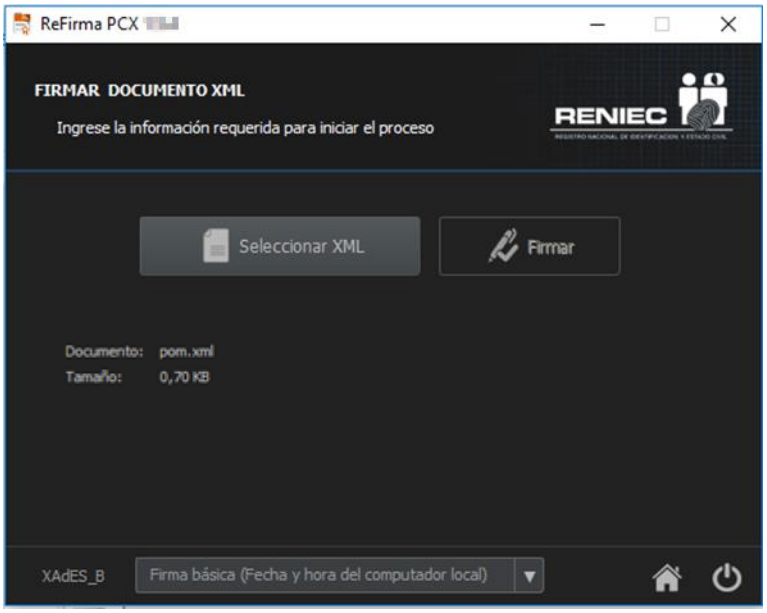

Figura 22 – Cargar doumento.

5. Inserte el DNIe en la lectora para poder realizar la firma del documento.

6. Para firmar el documento debe de desplegar el combo de firma XAdES y seleccionar la firma que desea utilizar, teniendo en cuenta la descripción de firmas que se describe en la NOTA 01.

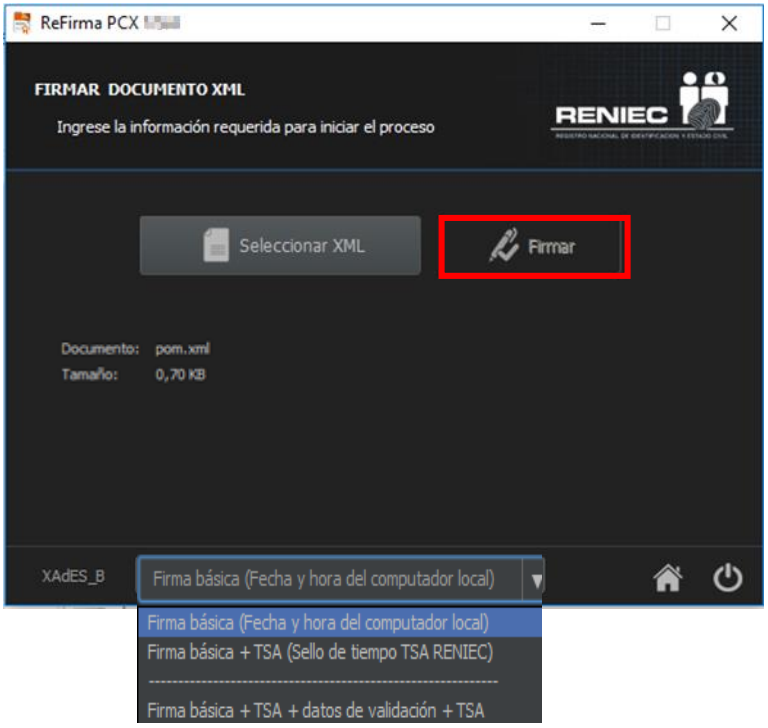

Figura 23 – Elegir firma.

7. Automáticamente aparecerá una pantalla con la lista de certificados digitales, seleccione el certificado digital y haga clic en el botón “Aceptar”. (Figura 24)

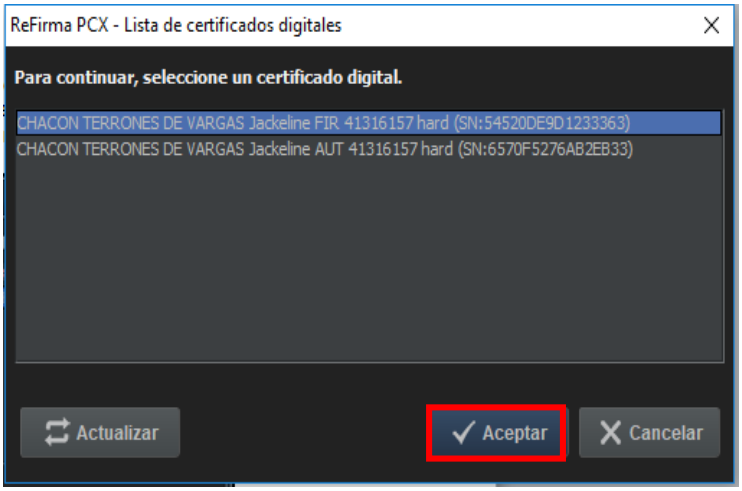

Figura 24 – Seleccionar Certificado Digital.

8. Para poder firmar el documento debe de ingresar el pin del DNIe del destinatario. una vez que ingresado haga clic en el botón “Aceptar” (Figura 25) . El aplicativo verifica el PIN ingresado según lo descrito en la NOTA 02.

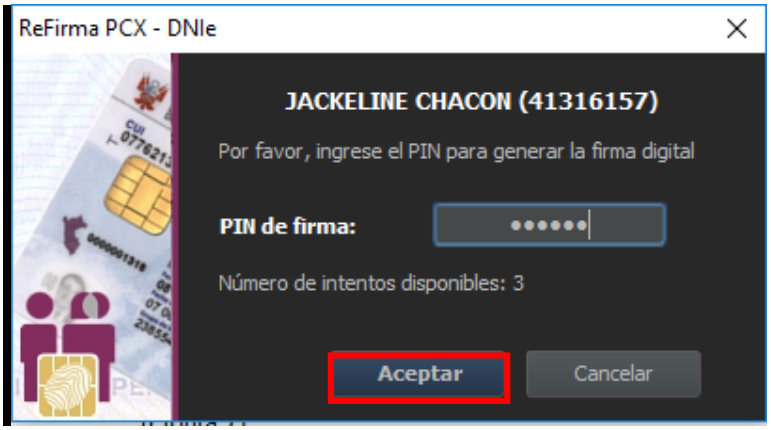

Figura 25 – Ingresar PIN.

9. Una vez que se terminó de firmar el documento se mostrará un mensaje que el archivo fue firmado correctamente y se encuentra en la misma ruta de donde seleccionó el documento, haga clic en el botón “Inicio” para volver a la pantalla inicial. (Figura 26)

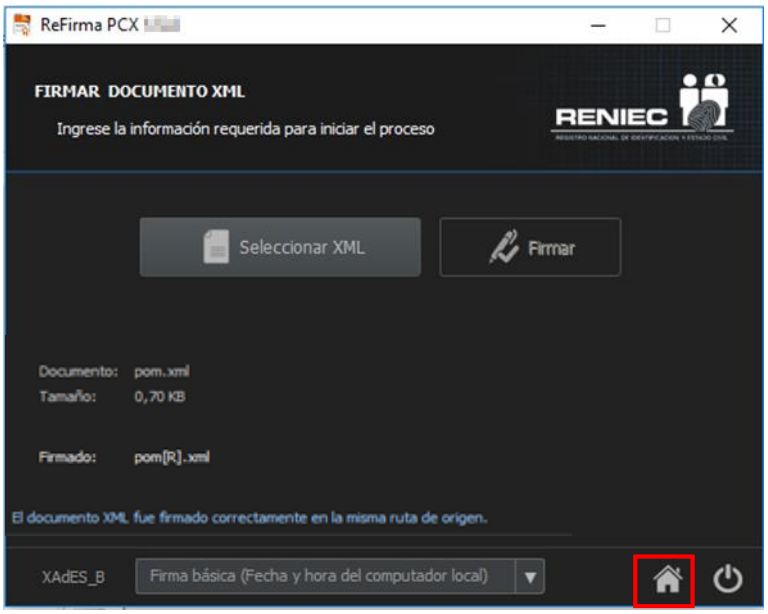

Figura 26 – Firmado correcto

NOTA 01:
Descripción de Firmas

a. Firma básica (Fecha y hora del computador local): Define un perfil para firmas electrónicas a corto plazo. Debe incluir una firma electrónica y el certificado de firma. (Nivel B)
b. Firma básica + TSA (Sello de tiempo TSA RENIEC): Como nivel B, pero agrega una marca de tiempo, que demuestra que la firma existía en una fecha y hora determinadas. (Nivel T) (*)
c. Firma básica + TSA + datos de validación + TSA: como nivel LT, pero agrega una marca de tiempo de documento y datos VRI para la TSA (Time Stamping Authority). Un formulario de LTA puede ayudar a validar la firma más allá de cualquier evento que pueda limitar su validez. Esto es lo que recomendamos para las firmas electrónicas calificadas. (Nivel LTA) (*)

(*) Los niveles de firma T y LTA están disponibles para entidades públicas que suscriban un Convenio TSA con el RENIEC.

NOTA 02:
1. Si el usuario se equivocó al ingresar su PIN del DNIe, el sistema mostrará el siguiente mensaje de alerta. (Figura 27)

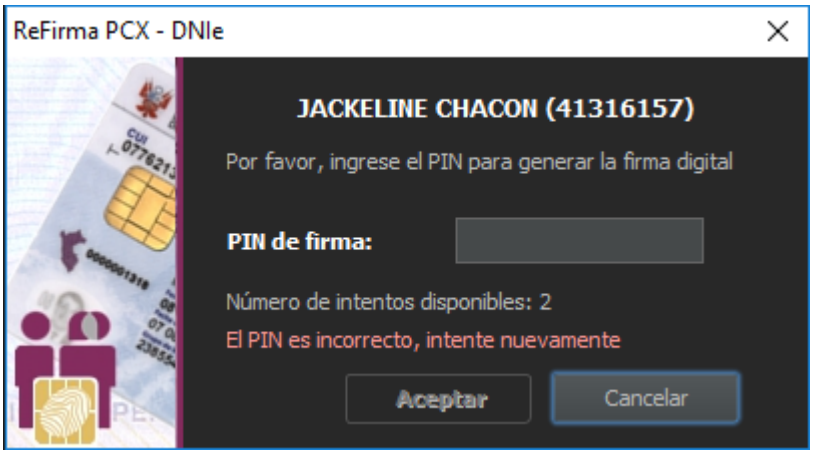

Figura 27 – PIN incorrecto

Cuando sea el caso del DNI Electrónico, el sistema le permitirá ingresar 3 veces su PIN (en su Versión 1) y 5 veces su PIN (en su Versión 2), y si se equivocó las veces permitidas se bloqueará el acceso al DNI Electrónico.

2. Si utiliza un token criptográfico para realizar la firma del documento, el sistema mostrará la siguiente pantalla. (Figura 28)

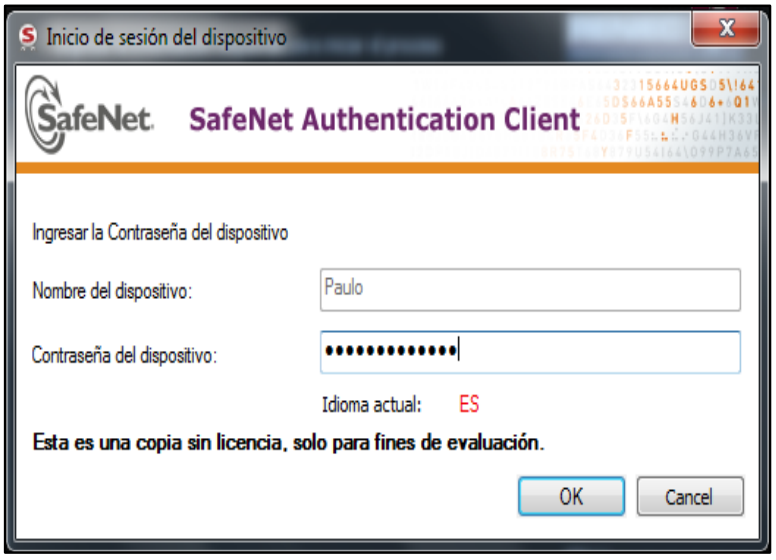

Figura 28 – Contraseña de dispositivo

3. Si el usuario se equivocó al ingresar su contraseña del token criptográfico, el sistema mostrará el siguiente mensaje de alerta. (Figura 29)

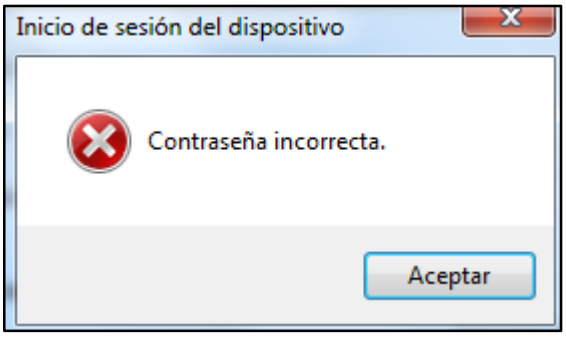

Figura 29 – Contraseña incorrecta

Cuando sea el caso del token criptográfico, el sistema le permitirá ingresar 15 veces su contraseña, y si se equivocó las 15 veces permitidas se bloqueará el acceso al token criptográfico.

4. Para poder realizar una firma debe seleccionar un certificado válido, si en caso seleccione un certificado de no repudio. El sistema le mostrará el siguiente mensaje de alerta. (Figura 30)

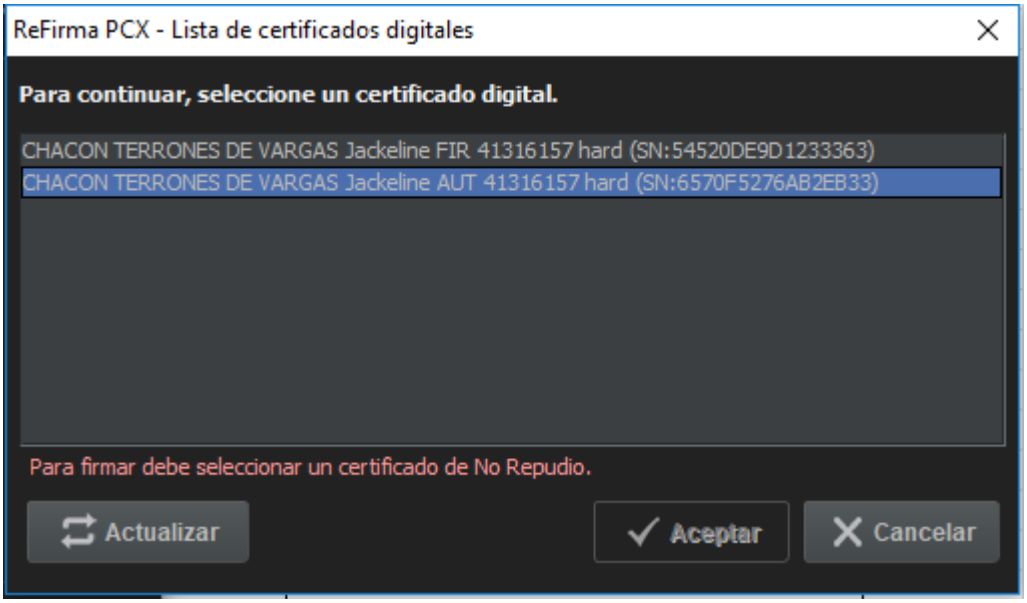

Figura 30 – Certificado de No repudio

5. Si el certificado seleccionado va a expirar el sistema te envía un mensaje de alerta. (Figura 31)

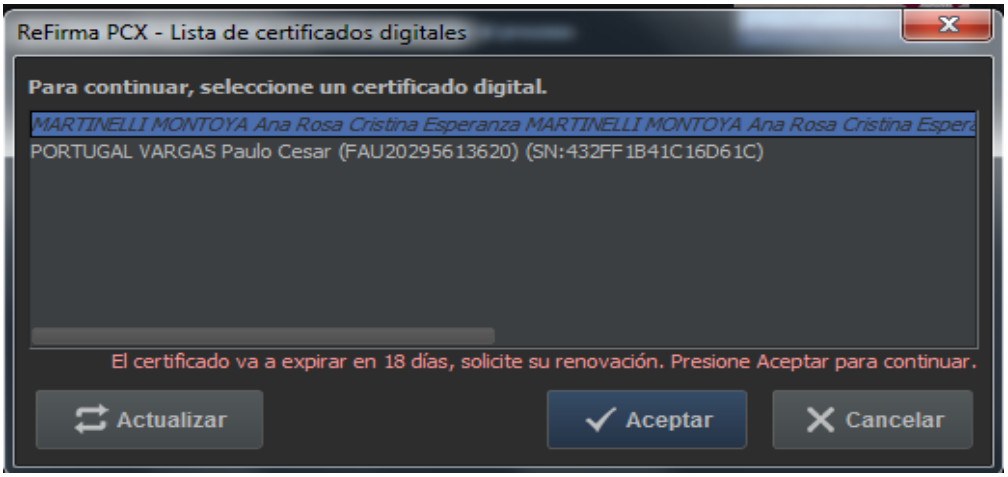

Figura 31 – Certificado va a expirar

6.4. Validar PDF

Esta opción permitirá validar documentos PDF.

Realice los siguientes pasos para validar documentos PDF:

1. Haga clic en la opción “Validar PDF”. (Figura 32)

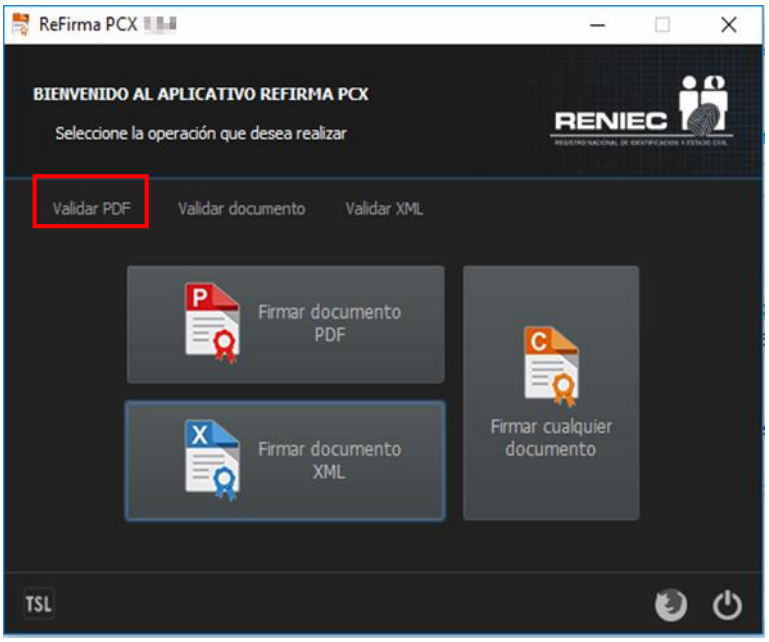

Figura 32 – Validar PDF

2. Automáticamente se mostrará un cuadro de diálogo, elegir el archivo que desea seleccionar y haga clic en el botón “Abrir”. (Figura 33)

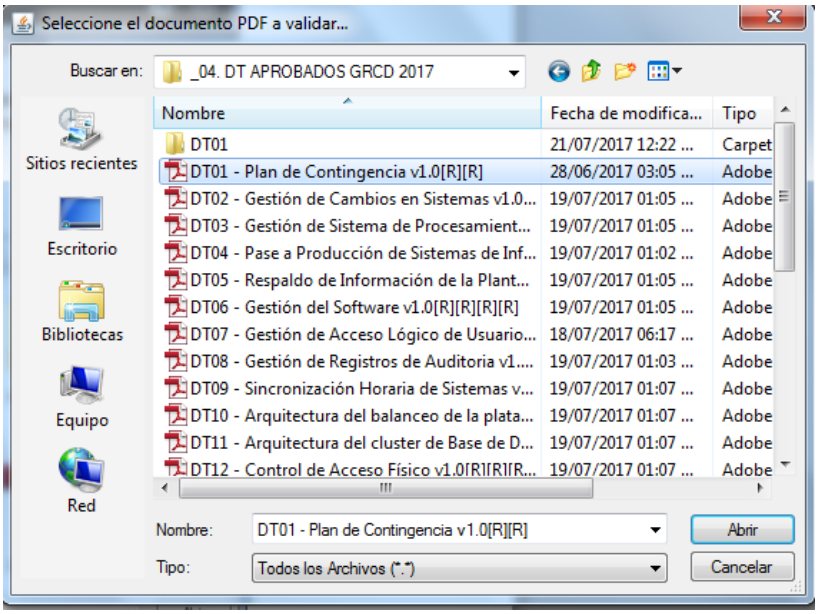

Figura 33 – Abrir Archivo

3. Automáticamente se realizar la validación el sistema mostrará el resultado obtenido.

- Si el estado es válido el sistema muestra un icono de validación verde que indica que el archivo fue validado correctamente. (Figura 34).

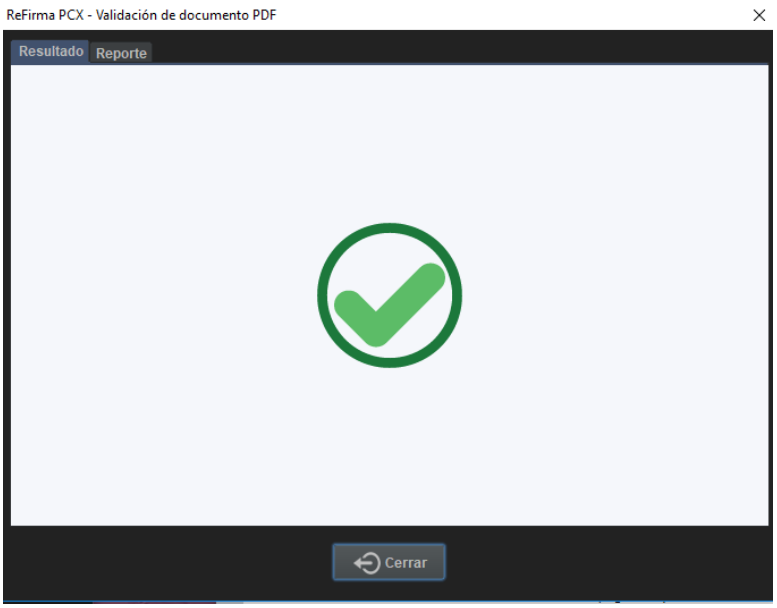

Figura 34 – Estado válido

- Si el estado es indeterminado el sistema muestra un icono de validación anaranjado. Esto indica que el archivo puede ser indeterminado por dos motivos:

1. Que el estado es indeterminado porque mantiene su integridad, pero los certificados digitales ya expiraron. (Figura 35)

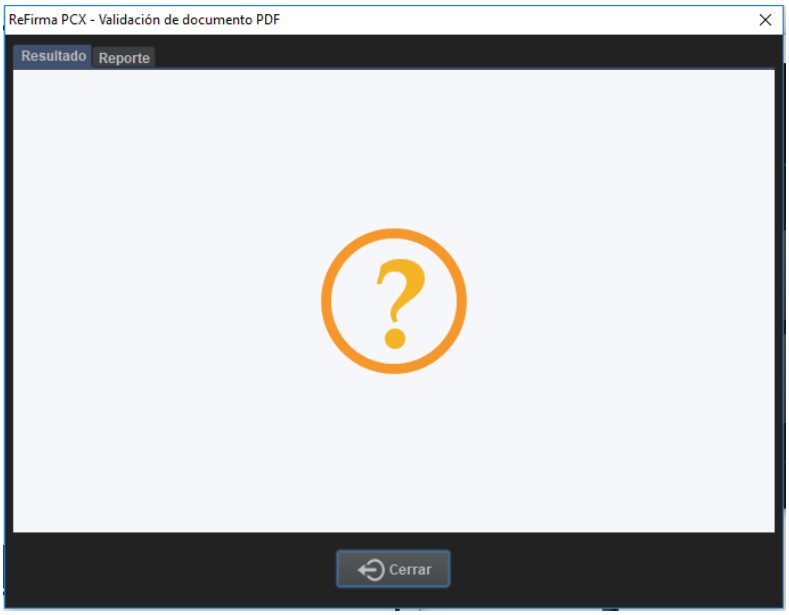

Figura 35 – Estado indeterminado certificados expirados

2. Que el estado es indeterminado porque el archivo mantiene su forma original, pero se agregó documentación adicional al documento. (Figura 36).

Figura 36 – Estado indeterminado cambios en el documento

- Si el estado es inválido el sistema muestra un icono de validación rojo, esto indica que la firma fue alterada. (Figura 37).

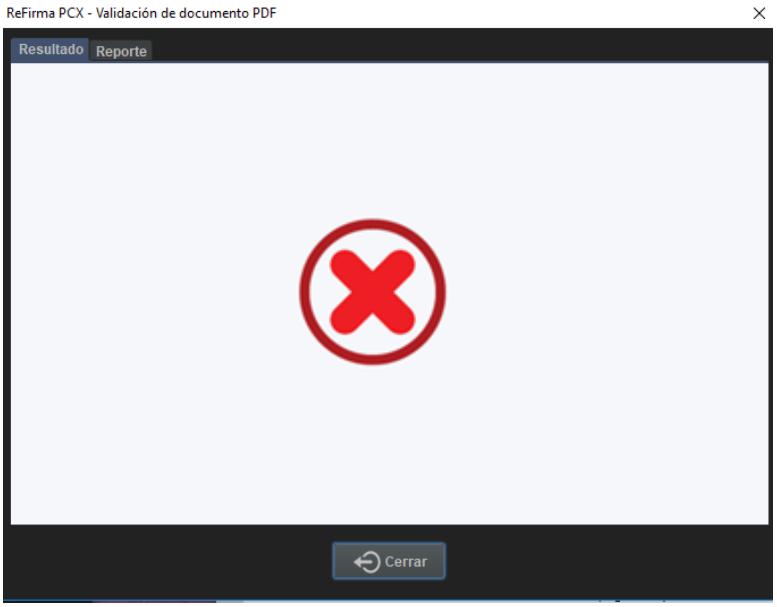

Figura 37 – Estado inválido

4. El sistema también mostrará el reporte de cada validación, para revisar el reporte haga clic en la pestaña “Reporte”. (Figura 38)

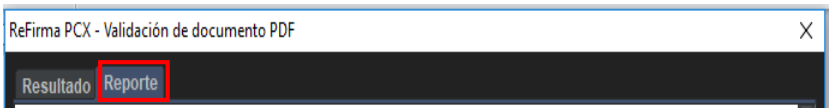

Figura 38 – Pestaña reporte

- Si el estado es válido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 39)

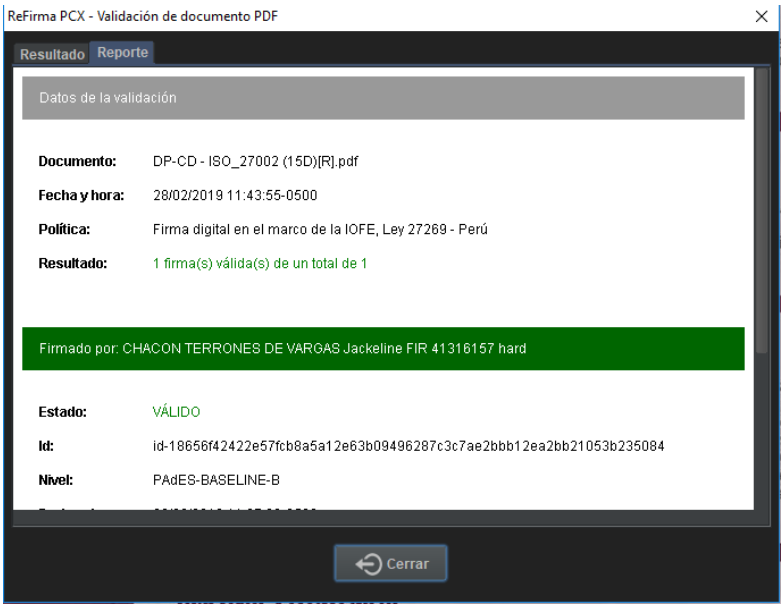

Figura 39 – Reporte de estado válido

- Si el estado es indeterminado el sistema mostrará el siguiente reporte

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 40)

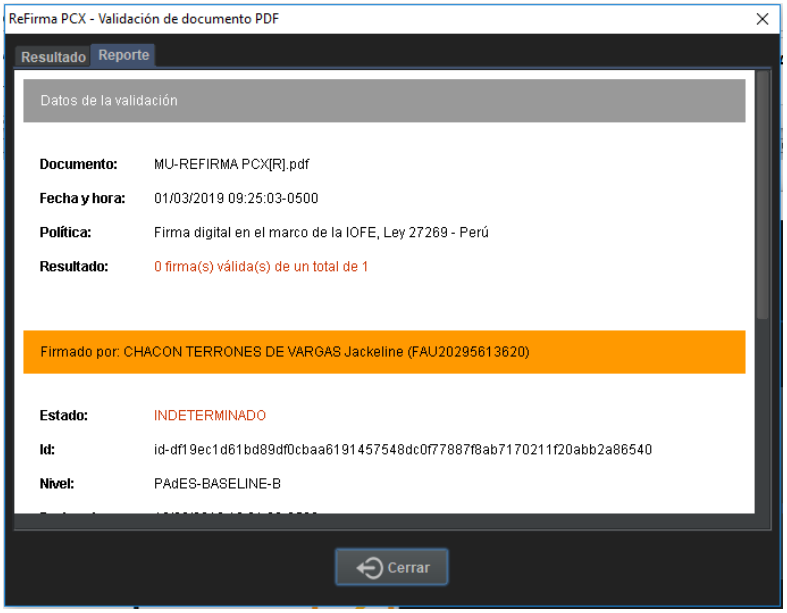

Figura 40 – Reporte certificados expirados

- Si el estado es inválido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital

y el resultado de cuantas firmas válidas tiene el documento. (Figura 41)

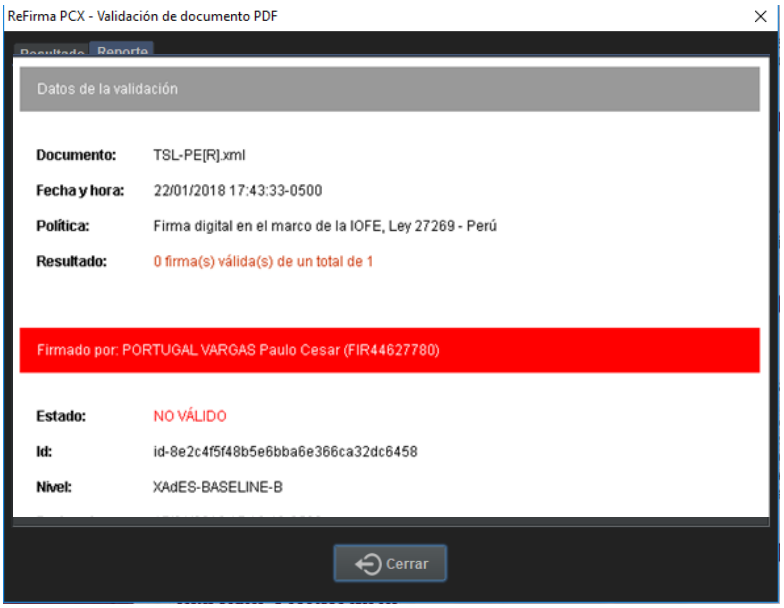

Figura 41 – Reporte de estado invalido

6.5. Validar Documento

Esta opción permitirá validar cualquier tipo de documentos.

Realice los siguientes pasos para validar documentos:

1. Haga clic en la opción “Validar documento”. (Figura 42)

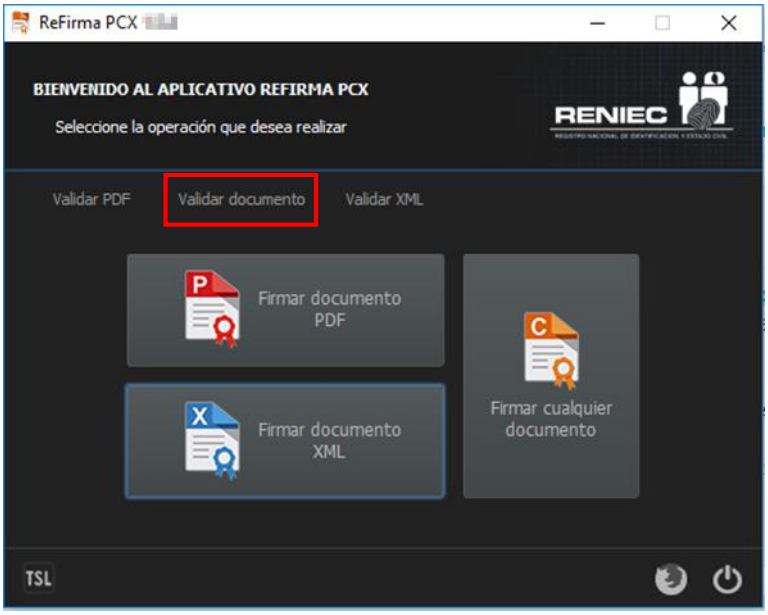

Figura 42 – Validar documento

2. Automáticamente se mostrará un cuadro de diálogo, elegir el archivo que desea seleccionar y haga clic en el botón “Abrir”. (Figura 43)

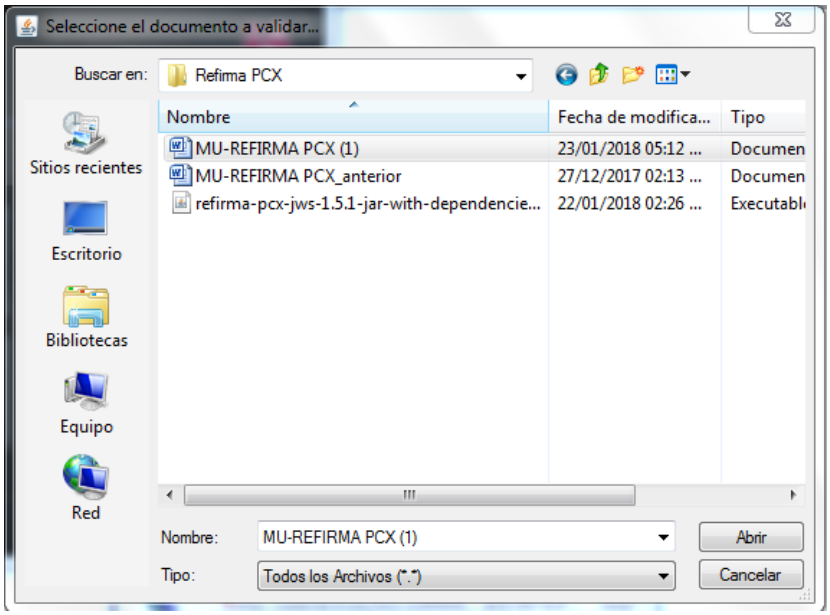

Figura 43 – Abrir Archivo

3. Automáticamente se realizar la validación el sistema mostrará el resultado obtenido.

   - Si el estado es válido el sistema muestra un icono de validación verde que indica que el archivo fue validado correctamente. (Figura 44).

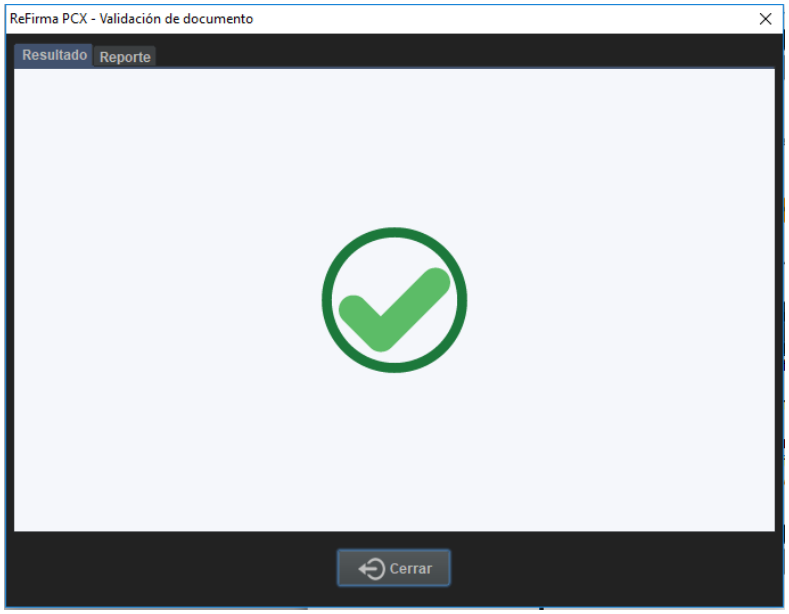

Figura 44 – Estado válido

- Si el estado es indeterminado el sistema muestra un icono de validación anaranjado. Esto indica que el archivo es indeterminado. por qué los certificados digitales ya expiraron. (Figura 45)

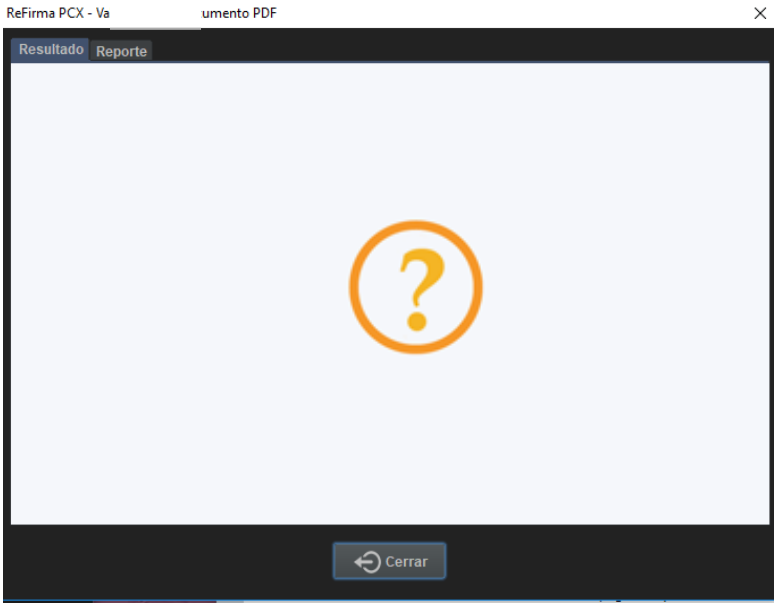

Figura 45 – Estado indeterminado certificados expirados

- Si el estado es inválido el sistema muestra un icono de validación rojo, esto indica que el archivo fue alterado. (Figura 46).

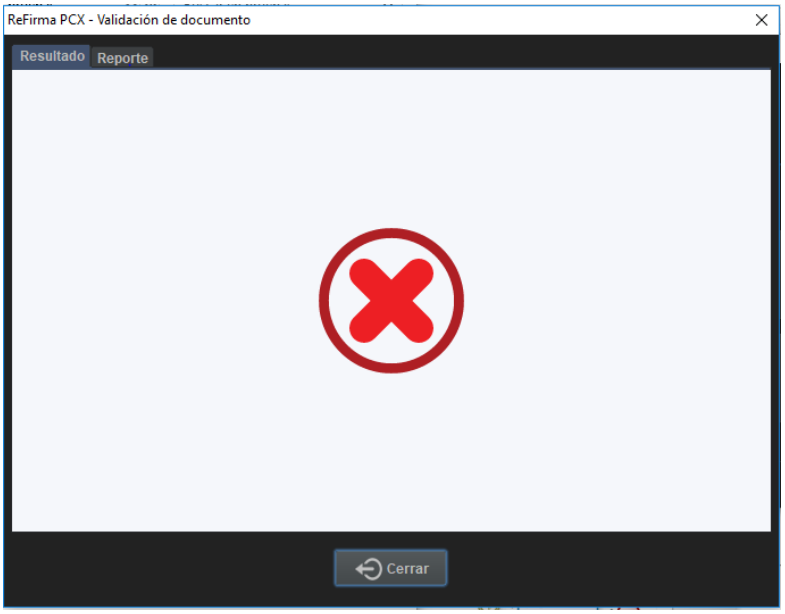

Figura 46 – Estado inválido

4. El sistema también mostrará el reporte de cada validación, para revisar el reporte haga clic en la pestaña “Reporte”. (Figura 47)

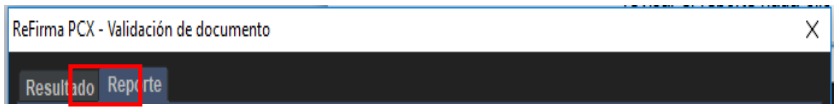

Figura 47 – Pestaña reporte

- Si el estado es válido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 48)

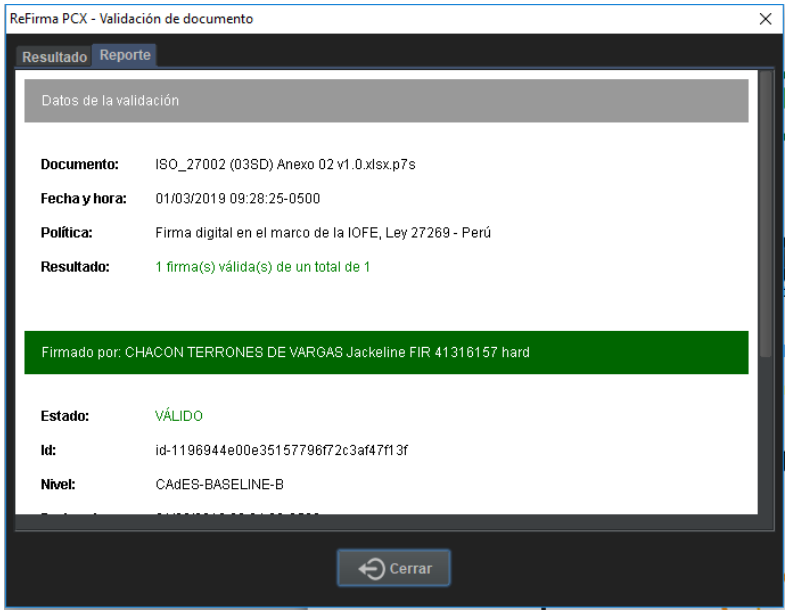

Figura 48 – Reporte de estado válido

- Si el estado es indeterminado el sistema mostrará el siguiente reporte

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 49)

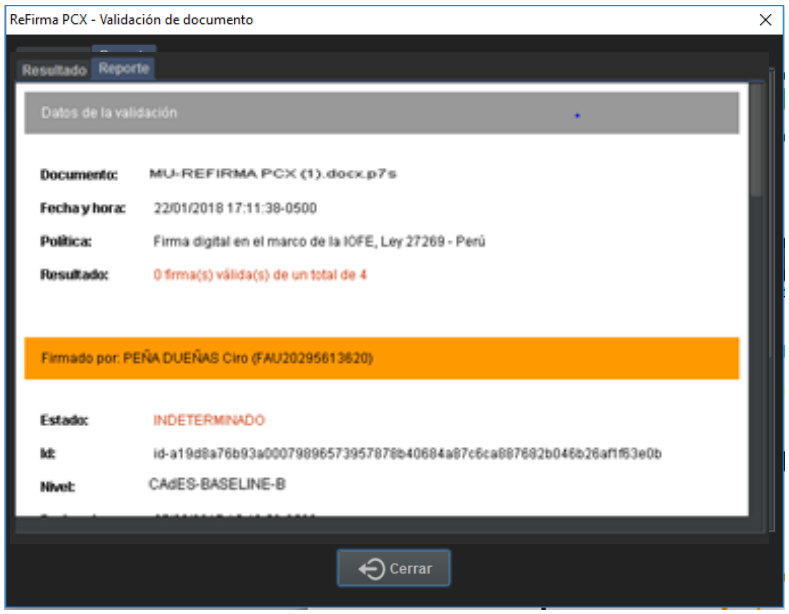

Figura 49 – Reporte certificados expirados

- Si el estado es inválido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 50)

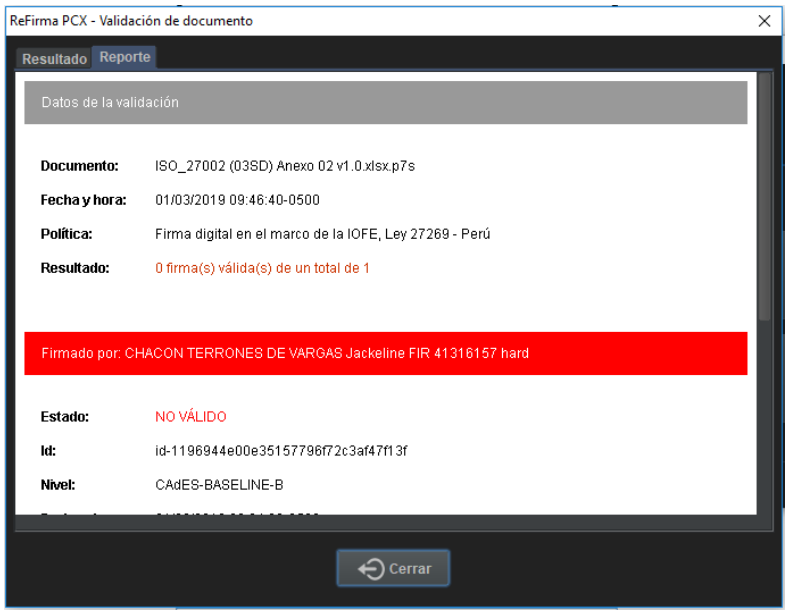

Figura 50 – Reporte de estado inválido

6.6. Validar XML

Esta opción permitirá validar cualquier tipo de documentos.

Realice los siguientes pasos para validar documentos XML:

1. Haga clic en la opción “Validar XML”. (Figura 51)

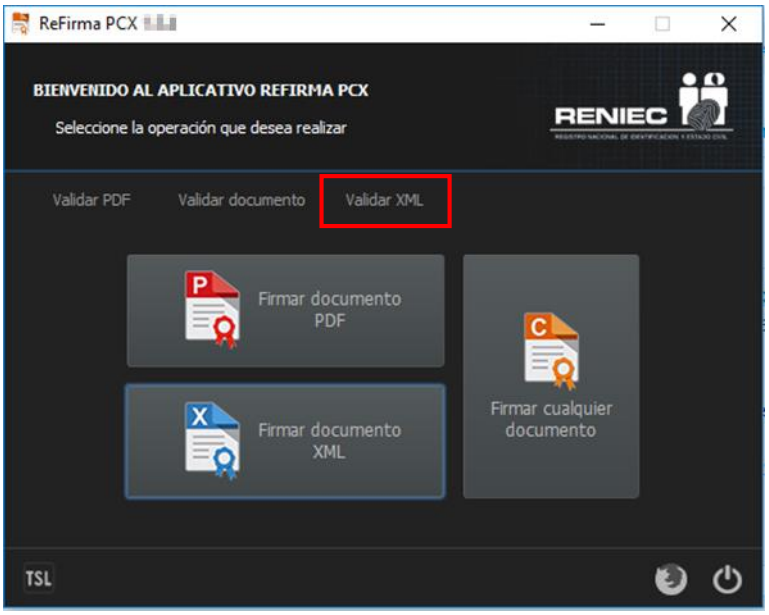

Figura 51 – Validar XML

2. Automáticamente se mostrará un cuadro de diálogo, elegir el archivo que desea seleccionar y haga clic en el botón “Abrir”. (Figura 52)

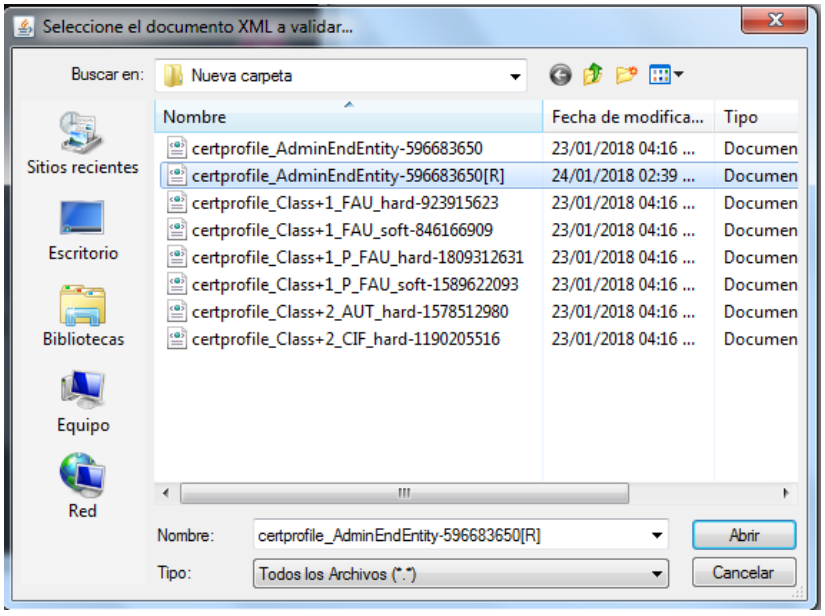

Figura 52 – Abrir Archivo

3. Automáticamente se realizar la validación el sistema mostrará el resultado obtenido.

   - Si el estado es válido el sistema muestra un ícono de validación verde que indica que el archivo fue validado correctamente. (Figura 53).

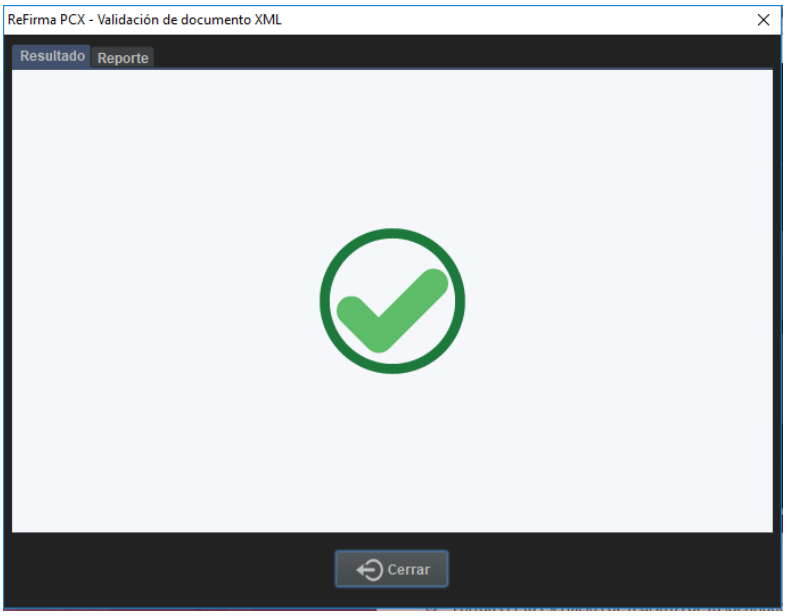

Figura 53 – Estado válido

- Si el estado es indeterminado el sistema muestra un icono de validación anaranjado. Esto indica que el archivo es indeterminado. por qué los certificados digitales ya expiraron. (Figura 54)

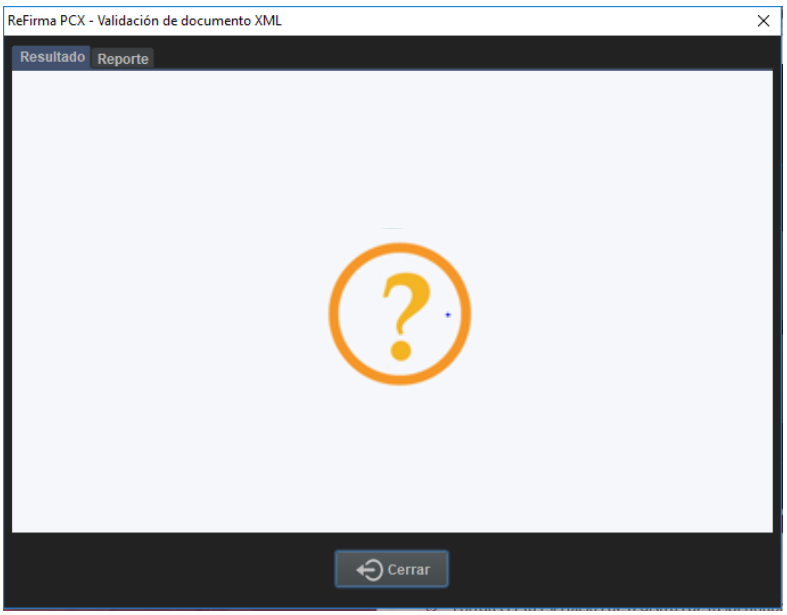

Figura 54 – Estado indeterminado certificados expirados

- Si el estado es inválido el sistema muestra un ícono de validación rojo, esto indica que el archivo fue alterado. (Figura 55).

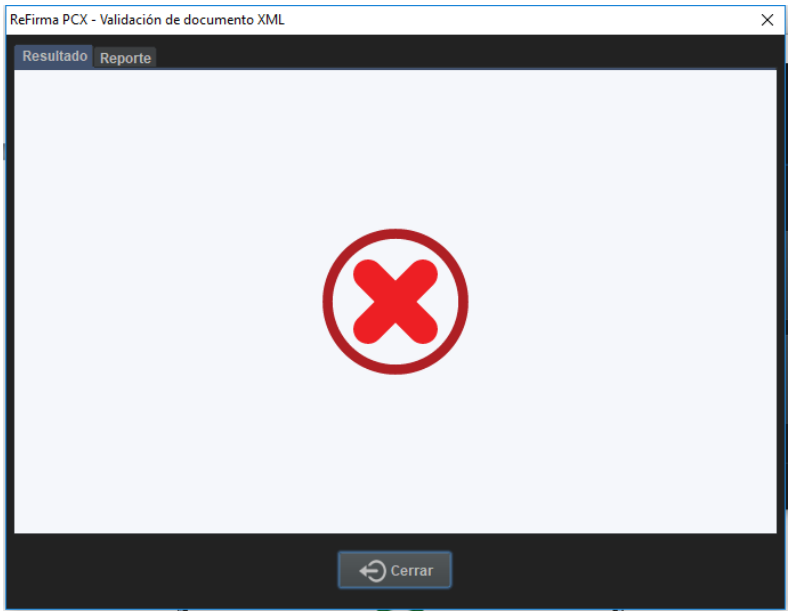

Figura 55 – Estado invalido

4. El sistema también mostrará el reporte de cada validación, para revisar el reporte haga clic en la pestaña “Reporte”. (Figura 56)

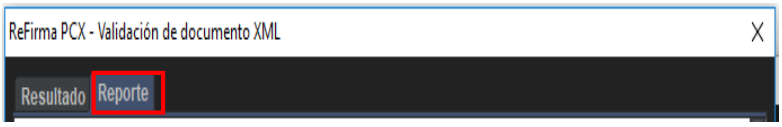

Figura 56 – Pestaña reporte

- Si el estado es válido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 57)

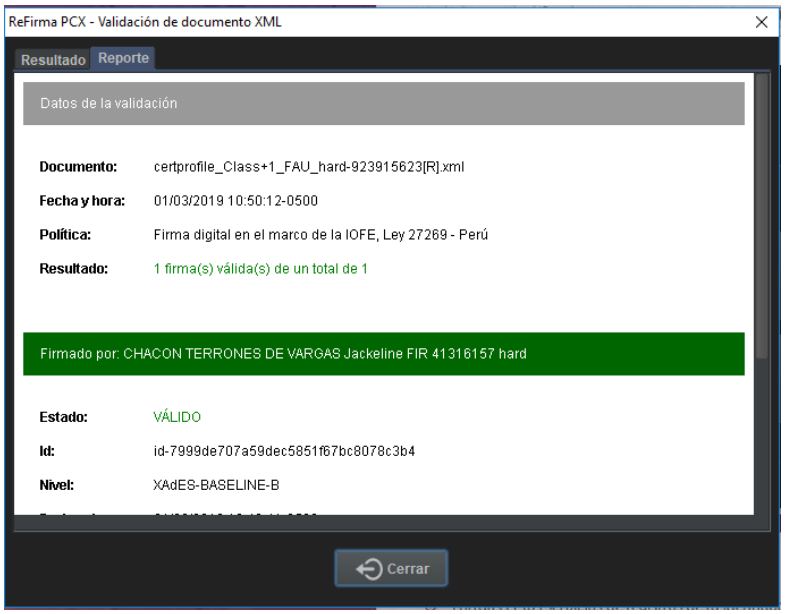

Figura 57 – Reporte de estado válido

- Si el estado es indeterminado el sistema mostrará el siguiente reporte

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital y el resultado de cuantas firmas válidas tiene el documento. (Figura 58)

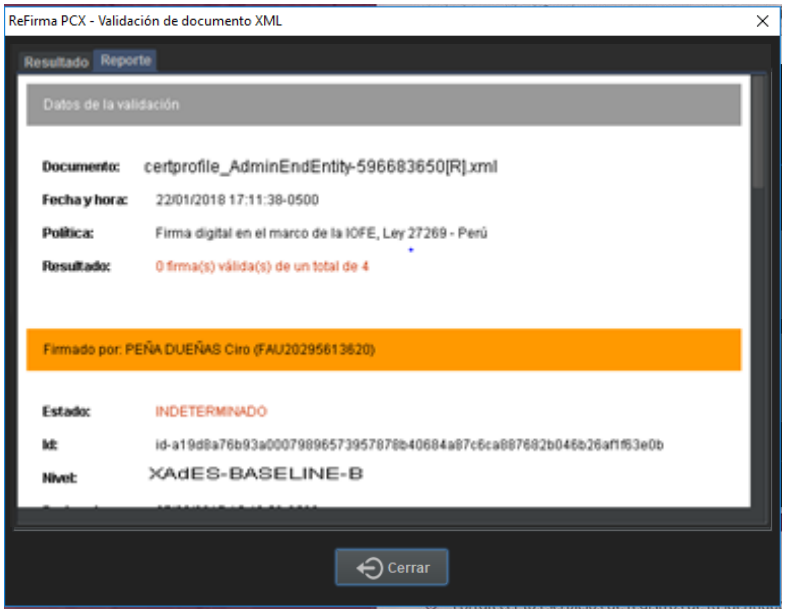

Figura 58 – Reporte certificados expirados

- Si el estado es inválido el sistema mostrará el siguiente reporte:

  ✓ Este reporte mostrará el nombre del documento, la fecha y la hora en que fue validado, las políticas de la firma digital

y el resultado de cuantas firmas válidas tiene el documento. (Figura 59)

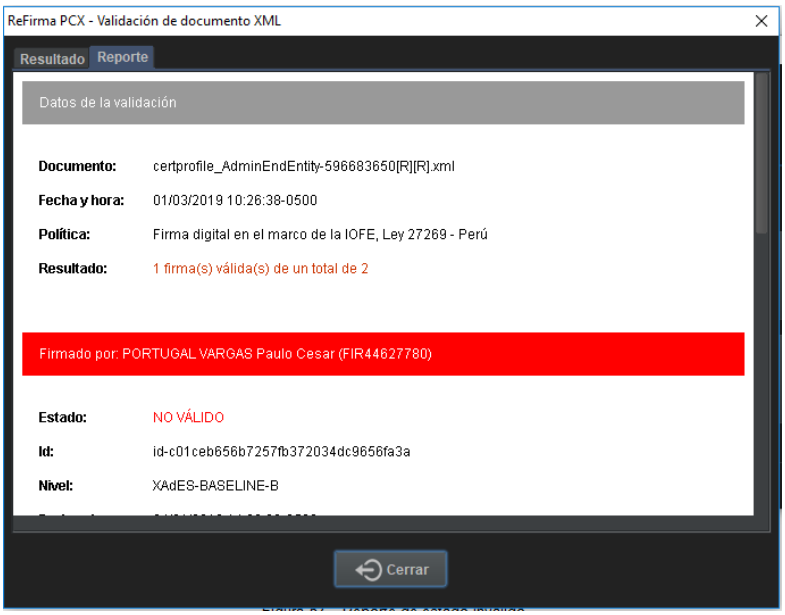

Figura 59 – Reporte de estado invalido

Resultado de validación según el nivel de firma elegido:

a) Si realizó la firma de un documento PDF, XML o cualquier documento en firma Básica, el reporte de validación mostrará el siguiente nivel B. (Figura 60)

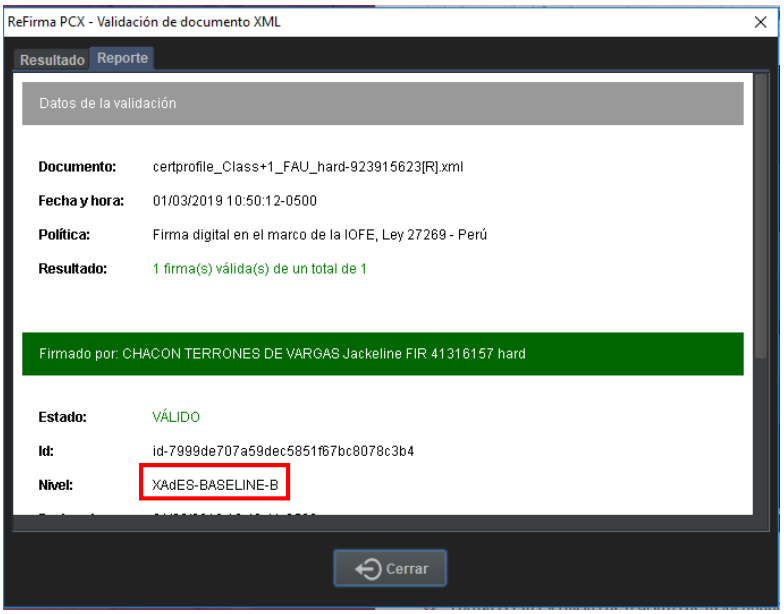

Figura 60 – Reporte con nivel B

b) Si realizó la firma de un documento PDF, XML o cualquier documento en firma Básica +TSA, el reporte de validación mostrará el siguiente nivel T. (Figura 61)

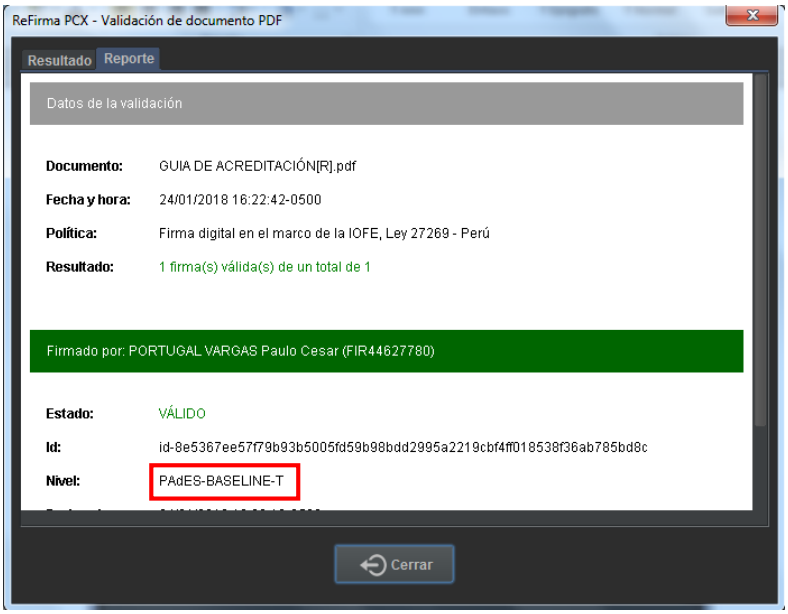

Figura 61 – Reporte con nivel T

c) Si realizó la firma de un documento PDF, XML o cualquier documento en firma Básica +TSA + datos de validación, el reporte de validación mostrará el siguiente nivel LT. (Figura 62)

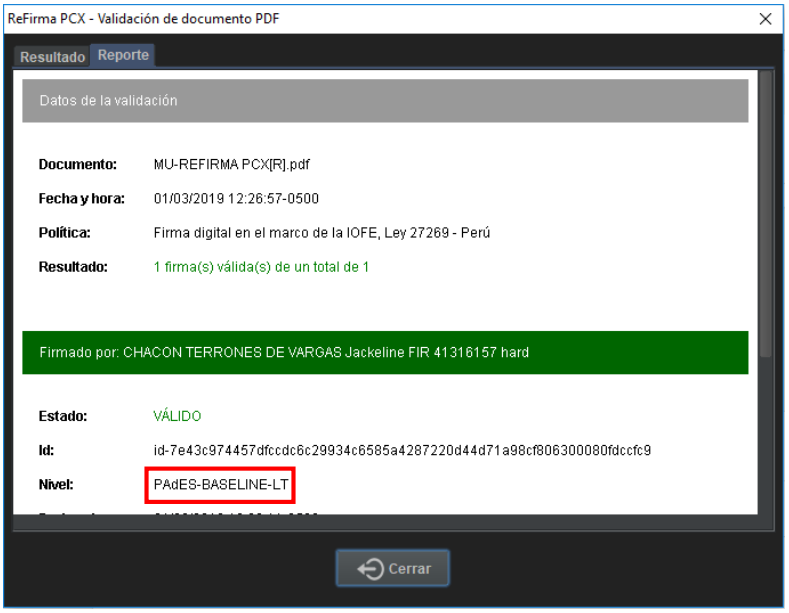

Figura 62 – Reporte con nivel LT

d) Si realizó la firma de un documento PDF, XML o cualquier documento en firma Básica +TSA + datos de validación + TSA, el reporte de validación mostrará el siguiente nivel LTA. (Figura 63)

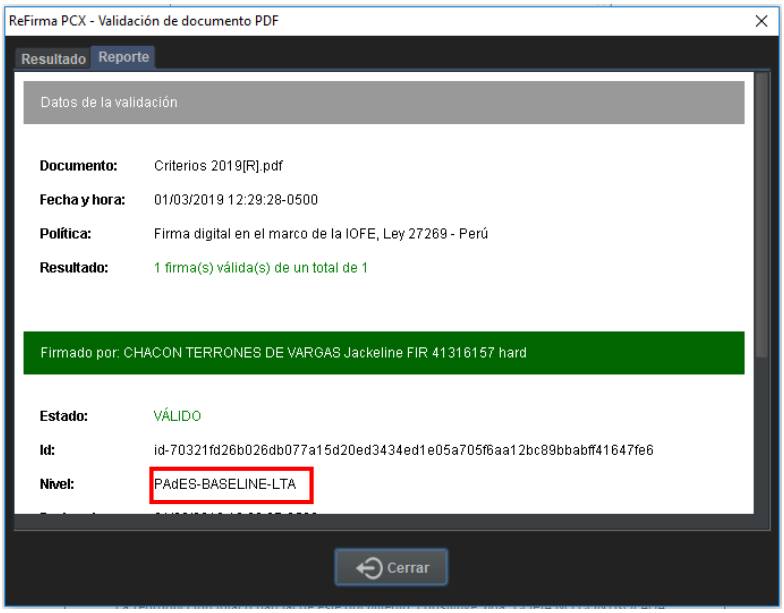

Figura 63 – Reporte con nivel LTA

6.7. Lista de Certificados de Confianza

Esta opción permitirá observar la lista de certificados de confianza.

Realice los siguientes pasos:

1. Haga clic en la opción “TSL”. (Figura 64)

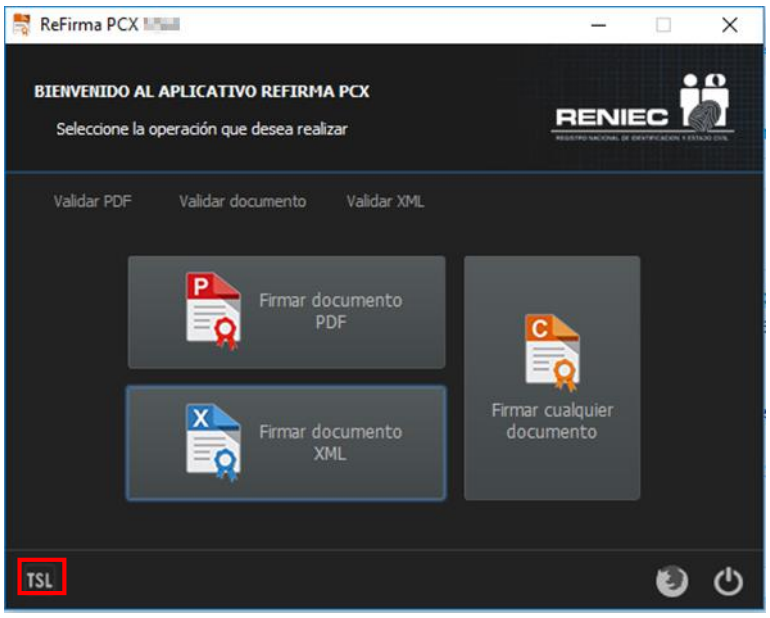

Figura 64 – Opción TSL

2. Automáticamente mostrará la siguiente pantalla, donde muestra la lista de Servicios de Confianza TSL de la URL de INDECOPI. (Figura 65)

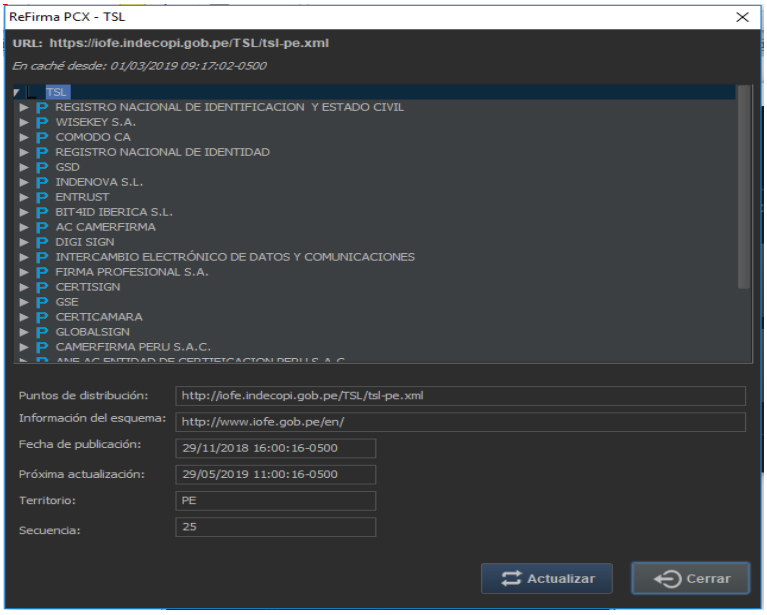

Figura 65 – Lista de TSL

3. Si desea actualizar la lista haga clic en el botón “Actualizar”. (Figura 66)

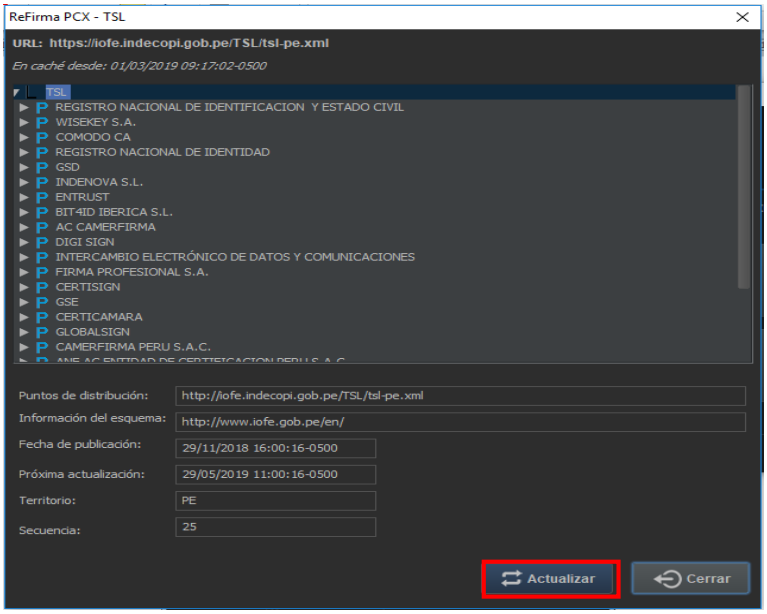

Figura 66 – Actualizar lista de TSL

Verificación del estado de validez:

Las funciones de verificación del estado de validez de los certificados digitales siempre estarán activas, esta configuración solo se podrá modificar siempre y cuando la AAC así lo disponga. Para ese caso se deberá de generar una nueva versión del producto.

ANEXO 01

MARCO LEGAL

- El Registro Nacional de Identificación y Estado Civil (RENIEC) es un organismo constitucional y autónomo con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante la Ley Orgánica N° 26497. Goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

- Mediante la Ley Nº 27269, Ley Firmas y Certificados Digitales, publicada el 28 de Mayo del 2000, modificada mediante Ley Nº 27310 del 17 de Julio del 2000, se regula en el Perú la utilización de la firma electrónica y los certificados digitales, así como el establecimiento de los prestadores de servicios de certificación digital.

- El Decreto Supremo Nº 052-2008-PCM del 19 de Julio del 2008, aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, que luego es modificado mediante el Decreto Supremo Nº 070-2011-PCM del 27 de Julio del 2011.

- El Reglamento vigente reglamentó el empleo de la firma digital para los sectores público y privado, otorgando a la firma digital generada dentro la Infraestructura Oficial de Firma Electrónica (IOFE) la misma validez y eficacia jurídica que una firma manuscrita. Así mismo, estableció el régimen de la IOFE, definida como un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: (i) La integridad de los documentos electrónicos y (ii) La identidad de su autor.

- Mediante Decreto Supremo N° 105-2012-PCM, publicado en el diario oficial El Peruano, se realizan diversas modificaciones de la normativa que regula el uso de la firma digital, sin afectar la validez y eficacia jurídica de las firmas digitales generadas bajo la Infraestructura Oficial de Firma Electrónica.

- Resolución de la Comisión de Reglamentos Técnicos y Comerciales Nº 030-2008/CRTINDECOPI, del 19 de marzo de 2008, que aprueba las Guías de Acreditación de Entidades de Certificación Digital, Entidades de Registro o Verificación de Datos y Entidades de Prestación de Servicios de Valor añadido, así como la Guía para la Acreditación del Software de Firmas Digitales.

- Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias N° 094-2012/CNB-INDECOPI, del 24 de Octubre del 2012, que acredita el software de firma digital del RENIEC.

ANEXO 02

POLÍTICAS DE PRIVACIDAD

El software ReFirma PCX ha sido diseñado de tal forma que:

1. No es necesario que los usuarios se registren en ningún medio para usar el aplicativo, por lo tanto, no se guarda ninguna información personal.

2. No copia, guarda ni expone el PIN del usuario.

3. No copia, guarda ni expone la clave privada del usuario.

4. Registra los siguientes datos en el documento firmado:

    a. Fecha de firma y datos del firmante

    b. Certificados de la ruta de certificación

    c. Número IP y MAC address del computador

    d. Nombre del servidor de tiempo, en el caso de estar siendo usado

5. No registra ningún dato del usuario en los servidores del RENIEC en ninguna de sus operaciones de uso. Sin embargo, es importante señalar que el software envía automáticamente un aviso al RENIEC cada vez que una firma digital es: (1) efectuada con éxito o (2) verificada; esto con fines estadísticos.

ANEXO 03

POLÍTICAS DE SEGURIDAD

Las políticas de seguridad conforman el conjunto de lineamientos que los usuarios deben cumplir a fin de garantizar la seguridad en el uso del software de firma digital. Las siguientes políticas regulan la confidencialidad, integridad y no repudio de las operaciones a ser realizadas con el software ReFirma PCX:

1. La seguridad del certificado digital radica en la adecuada custodia de su clave privada asociada, por tanto, es muy importante que el suscriptor recuerde los usos apropiados e inapropiados.

   Entre los usos apropiados tenemos:
   a. Proteger el acceso al repositorio del certificado digital (computadora personal, tarjeta inteligente o token criptográfico).
   b. Poseer un PIN de acceso a la clave privada del certificado digital.
   c. Custodiar el PIN de acceso, esto es, no compartirlo, ni anotarlo en lugares de acceso público.
   d. Es recomendable para una mayor seguridad, configurar el Sistema Operativo u otro mecanismo, a fin que éste solicite el ingreso de la contraseña de acceso a la clave privada cada vez que se deba firmar un documento.

   Entre los usos inapropiados tenemos:
   a. Compartir el uso del certificado digital. Recuerde que el certificado digital significa el uso de su identidad digital por tanto, es personal e intransferible y debe ser usado únicamente por el suscriptor del mismo.
   b. Divulgar el PIN de acceso a su clave privada. Si esto ocurre, en caso de extravío o pérdida de su tarjeta inteligente o token criptográfico, alguien que no es Ud. podrá hacer uso de su certificado digital.

2. El suscriptor del certificado digital debe ser razonablemente diligente en la custodia de su clave privada, así como, con la en la custodia del PIN (Personal Identification Number) de acceso a la misma, con el fin de evitar usos no autorizados. Esta contraseña es creada por el suscriptor y debe ser conocida únicamente por él. La falta de diligencia adecuada por parte del suscriptor del certificado digital (propietario de la clave privada) le podría generar implicancias legales si un tercero suplanta su identidad firmando digitalmente documentos o mensajes a nombre del suscriptor.

3. El suscriptor del certificado digital deberá solicitar inmediatamente a la EREP la cancelación de su certificado, en cuanto se produzcan los siguientes hechos:

   a. Pérdida, robo o extravío de su dispositivo criptográfico (computadora personal, tarjeta inteligente o token criptográfico) que almacena su clave privada.
   b. Cuando sospeche el compromiso potencial de su clave privada, debido a la exposición o pérdida de su PIN o si sospecha que un tercero pueda deducirlo.

c. Por deterioro, alteración o cualquier otro hecho o acto que afecte la clave privada o el PIN de acceso a su clave privada.

ANEXO 04

TÉRMINOS DE USO

Estos Términos de Uso son vinculantes para RENIEC y la entidad o usuario que los acepta ("Usted"). Los Términos de Uso regulan el uso del Software de Firma Digital ReFirma PCX. Al instalar o usar ReFirma PCX, Usted manifiesta que ha revisado y acepta los siguientes términos:

- Propiedad. RENIEC es propietario del Software, por lo que la propiedad intelectual y/o derechos de autor son exclusivos del RENIEC, así como, los derechos legales de copia, patentes, marcas, manuales de usuario, secretos comerciales y cualquier otro vinculado que pudiese surgir, incluida toda la información o documentación que el RENIEC proporcione a la Entidad.
- Costo. RENIEC cede a Usted la licencia de uso, copia, distribución y publicación del Software sin costo alguno y bajo su responsabilidad, debiendo ser usado dentro del marco legal y técnico vigente.
- Licencia Limitada. Usted no puede, parcial o total y bajo ninguna forma o medio (y no permitirá a ningún tercero que lo haga): (1) Reproducir, modificar o adaptar el Software. (2) Alquilar, arrendar, prestar, ceder o vender el Software. (3) Retirar los logos incluidos en el Software. (4) Usar o introducir cualquier tipo de dispositivo, componente o rutina que interfiera o pueda intentar interferir con las operaciones del Software. (5) Usar el Software quebrantando las licencias de las librerías listadas en los "Créditos" del presente documento.
- Privacidad y Seguridad. Usted afirma conocer, aceptar y cumplir las "Políticas de Privacidad y Seguridad" declaradas en el presente documento.
- Terceros. Si Usted utiliza el Software con certificados de Terceros, o si de otra forma un Tercero hace uso del Software usando sus certificados, siendo Usted autorizado o no, RENIEC no se responsabiliza por las operaciones de firma digital efectuadas, ya que se estarían violando las "Políticas de Seguridad" descritas en el presente documento.
- Exclusión de Garantías. RENIEC no otorga garantías de ningún tipo por el uso del Software, ya sea de manera expresa, implícita, legal o de cualquier otra forma.
- Limitación de Responsabilidad. RENIEC no será responsable por la pérdida de ingresos o daños directos e indirectos, especiales, incidentales, derivados, o punitivos, incluso si los daños directos no son suficientes para servir de compensación. Por lo tanto, ninguna forma de indemnización podrá ser reclamada ni al RENIEC ni a ninguno de sus funcionarios y personal.
- Limitación de Responsabilidad. RENIEC no será responsable por la pérdida de ingresos o daños directos e indirectos, especiales, incidentales, derivados, o punitivos, incluso si los daños directos no son suficientes para servir de compensación. Por lo tanto, ninguna forma de

indemnización podrá ser reclamada ni al RENIEC ni a ninguno de sus funcionarios y personal.

- Vigencia y Resolución. RENIEC puede dar por terminado los presentes Términos de Uso en cualquier momento sin previo aviso. A la terminación del presente, RENIEC dará de baja el software y Usted deberá dejar de usar el mismo y deberá borrar todas las copias del software existentes bajo su responsabilidad.
- Modificaciones de los Términos de Uso y Políticas. RENIEC puede cambiar o modificar, sin previo aviso, estos términos o cualquier otra política que regule el uso del Software para, por ejemplo, reflejar cambios en la ley o adicionar o remover funcionalidades. La modificación de estos términos o la de las políticas mencionadas serán anunciadas en www.reniec.gob.pe.
- El Sellado de Tiempo solo está disponible para entidades de la administración pública que suscriban un Convenio TSA con RENIEC.

ANEXO 05

SOPORTE TÉCNICO

- Web: http://pki.reniec.gob.pe
- e-mail: identidaddigital@reniec.gob.pe
- Teléfono: 315-4000 anexo 3017 - Lunes a Viernes de 08:30 a 16:30

ANEXO 06

CARTILLA DE INSTALACIÓN DE REFIRMA PCX

1. OBJETIVOS

El presente documento detallará los pasos a seguir para realizar una correcta instalación antes de comenzar a utilizar Software ReFirma PCX.

2. PASOS DE INSTALACION

Para realizar la instalación del software ReFirma PCX se requiere Java 8 para la aplicación desde la web.

Debe seguir los siguientes pasos:

1. Ingresar a la siguiente URL

https://dsp.reniec.gob.pe/refirma_suite/pcx/web/main.jsf

2. Se mostrará la siguiente pantalla donde podrá realizar la descarga del instalador del software ReFirma PCX. Haga clic en el botón “INSTALAR ReFirma PCX” (Figura 67)

Figura 67. Instalación ReFirma PCX

3. Se mostrará el siguiente cuadro de diálogo que consulta donde desea guardar el instalador, para ello deberá seleccionar la ubicación respectiva y luego haga clic en el botón Guardar. (Figura 68).

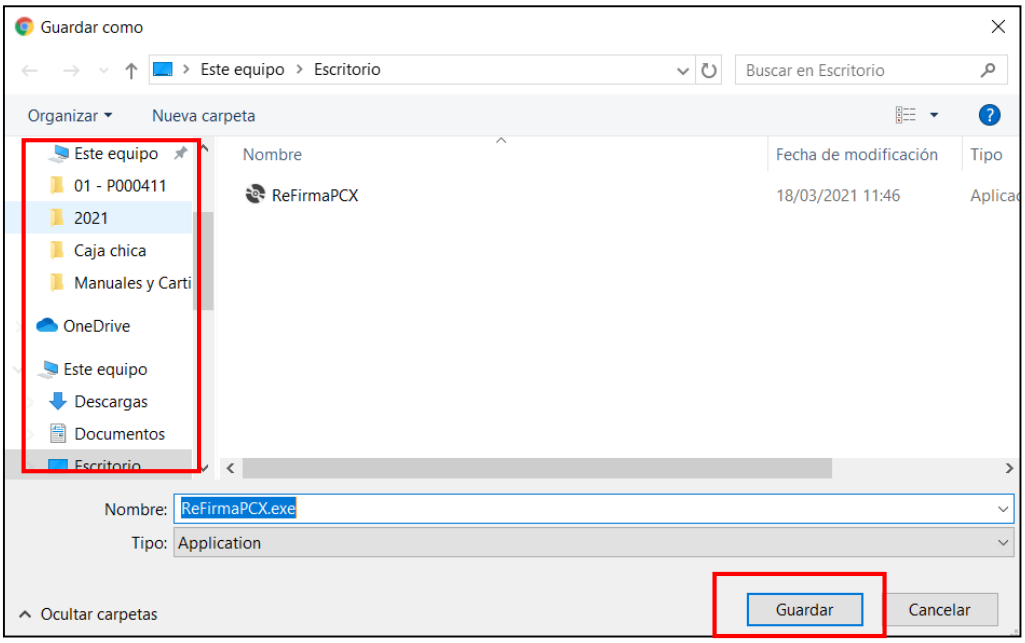

Figura 68. Descargar Instalador

FORMAS DE EJECUCIÓN DEL INSTALADOR DEL REFIRMA PCX:

A continuación, se mostrará las formas de cómo proceder con la ejecución del instalador.

- Opción 01, puede ejecutar el instalador desde el navegador donde realizó la descarga. (Figura 69)

Figura 69. Ejecutar instalador

- Opción 02, puede ejecutar el instalador desde la ubicación donde descargó el instalador. (Figura 70)

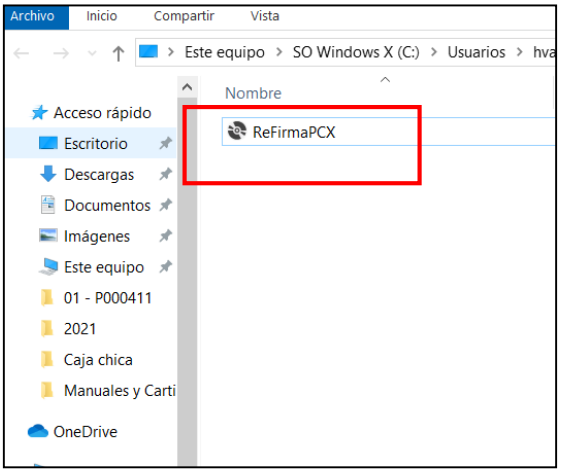

Figura 70. Ejecutar instalador

4. A continuación, se solicitará confirmar la instalación (Figura 71)

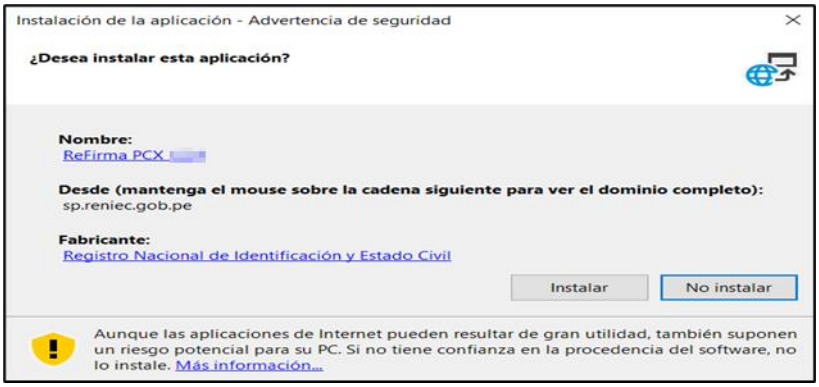

Figura 71. Aceptar la instalación

5. Luego de aceptar se mostrará la comprobación de los requerimientos de la aplicación. (Figura 72)

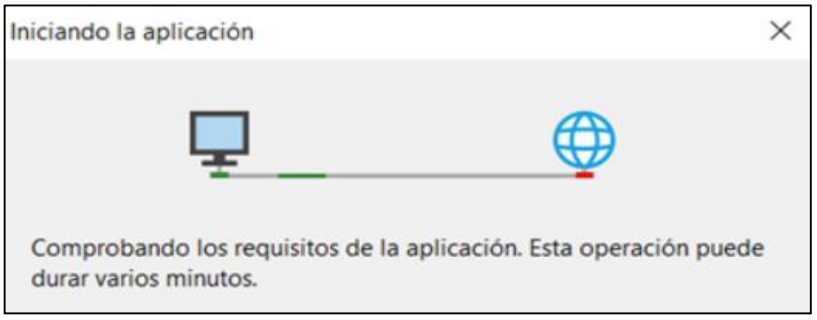

Figura 72. Comprobación de requerimientos

6. Al finalizar la comprobación de los requerimientos se mostrará automáticamente la pantalla del software ReFirma PCX. (Figura 73)

Figura 13. Pantalla del software ReFirma PCX

7. Automáticamente se mostrará la pantalla inicial del ReFirma PCX, con las opciones disponibles. (Figura 74)

Figura 74. Opciones disponibles ReFirma PCX

8. Una vez realizada la instalación del ReFirma PCX, se creará un icono de acceso directo en el escritorio de la PC. (Figura 75)

Figura 75. Acceso directo ReFirma PCX