Gobierno de Reconciliación y Unidad Nacional

El Pueblo, Presidente!

MHCP

DIRECCIÓN GENERAL DE TECNOLOGÍA

NORMATIVA PARA LA VERIFICACIÓN SEGURA DE FIRMA

Managua, diciembre 2022

CONTROL DE REVISIÓN Y ACTUALIZACIÓN (VERSIONES)

Nº	Fecha	Elaborado/ Entrevistado	Revisado	Aprobado	Autorizado
0	Diciembre / 2022	Daysi Romero Responsable Departamento de Acreditación y Registro Yuri Dompé Responsable Departamento de Supervisión e Inspección	Hans Espinoza Responsable Dirección Firma Electrónica	Hans Espinoza Responsable Dirección Firma Electrónica	José Diaz Responsable Dirección General de Tecnología

ÍNDICE

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público - MHCP ha elaborado el documento "Normativa para la verificación segura de firma", que permitirá a las partes interesadas realizar una verificación segura de Firma Electrónica Certificada generada a través de un certificado de firma electrónica certificada expedida por un Proveedor de Servicios de Certificación - PSC, en cumplimiento de los requisitos u obligaciones que deben sustentar en la prestación de sus servicios ante el público en general.

II. OBJETIVO

Proporcionar a las partes interesadas, ya sean Proveedores de Servicios de Certificación, Personal interno conducente de la Entidad Rectora, Personas Usuarias o las partes que confían, un instrumento normativo que regula los principales aspectos generales y técnicos a tener en cuenta al momento de realizar una verificación segura de firma.

III. BASE LEGAL

- Ley No. 729 "Ley de Firma Electrónica", Publicada en la Gaceta No. 165 del 30 de agosto del 2010.
  - Art. 15, Entidad Rectora de Acreditación de Firma Electrónica, inciso 11.
  - Art. 24, Requisitos para la Verificación Segura de Firma.

- Decreto No. 57-2011 "Reglamento de la ley 729 – Ley de Firma Electrónica".
  - Art. 9, De la entidad rectora de acreditación, inciso 1 e inciso 4.
  - Art. 20, inciso 2, inciso 3, inciso 4 e inciso 13(ii).
  - Art. 22, inciso 2, inciso 3, inciso 4, inciso 8, inciso 9, inciso 10, inciso 13, inciso 14 e inciso 18.

- Referencias Normativas:
  - Documento: "Normativa de formatos de Firma Electrónica";
  - Ley Modelo de la CNUDMI sobre Firmas Electrónicas
    - ✓ Art. 9, Proceder del prestador de servicios de certificación, inciso (c) y (d).
    - ✓ Art. 11, Proceder de la parte que confía en el certificado, inciso (a) y (b).

IV. GLOSARIO DE TÉRMINOS Y SIGLAS

Los siguientes términos son definidos en la Ley 729 "Ley de firma electrónica":

Aplicación de validación de firma: Aplicación automatizada que implementa el proceso de verificación de firmas electrónicas certificadas.

Certificado: Certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.

Datos de creación de firma: Son los datos únicos, códigos o claves criptográficas privadas que el firmante utiliza para crear la firma electrónica certificada.

Datos de verificación de firma: Son los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica certificada.

Firma electrónica certificada: Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control de manera que vinculada al mismo y a los datos a los que se refiere permite que sea detectable cualquier modificación ulterior a estos.

Proveedor de Servicios de Certificación - PSC: Entidades que otorgan, registran, mantienen y publican los Certificados de Firma Electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica.

Los siguientes términos son definidos en el Decreto 57-2011 “Reglamento de la Ley 729”:

Parte que Confía: Persona o entidad que recibe un mensaje de datos o un documento electrónico firmado con una Firma Electrónica Certificada.

Los siguientes términos son definidos o complementados en esta normativa:

Bloques de Construcción (o “Building Blocks” por su acepción inglesa): Para el presente documento se entenderá que los “Bloques de Construcción” son soluciones digitales abiertas y reutilizables basadas en estándares que permiten capacidades básicas, como la “Verificación Segura de Firma”.

Clave Pública: Es la clave del par de claves de una entidad que se conoce públicamente.

Ley: Ley 729 – Ley de Firma Electrónica, publicada en la Gaceta Diario Oficial.

Lista de Certificados Revocados: Es una lista firmada que indica un conjunto de certificados de clave pública que la autoridad de certificación (CA) emisora ya no considera válidos. Además del término genérico lista de revocación de certificados (CRL), se definen algunos tipos de CRL específicos para las CRL que cubren ámbitos particulares. 3

Reglamento: DP 057-2011, Reglamento de Ley de Firma Electrónica publicado en la Gaceta Diario Oficial No. 211 de noviembre del 2011.

Restricciones (de firma): Formulación abstracta de reglas, valores, rangos y resultados de computo contra los que se puede validar una firma electrónica certificada.

Verificación: Conjunto de actividades relacionadas con procedimientos y/o servicios que deben ser puestos a disposición de las partes que requieran comprobar ya sea de forma manual o automatizada, la fiabilidad de las firmas electrónicas certificadas aplicadas por los <<Firmantes>> a los mensajes de datos o documentos electrónicos recibidos por la <<Parte que Confía>>.

Verificador: Persona o entidad que quiere validar o verificar una Firma Electrónica Certificada.

Las siguientes siglas/acrónimos son definidos o complementados en esta normativa:

DGTEC: Dirección General del Tecnología.

DPC: Declaración de Practicas de Certificación.

LCR: Lista de Certificados Revocados.

PC: Política de Certificados.

V. NORMATIVA

1. De Carácter General

1.1. La parte que confía en la firma debe verificar mediante la clave pública recibida los aspectos de fiabilidad técnica que garantizan la validez de la misma, haciendo uso de las herramientas que pongan a su disposición los emisores de los certificados de firma electrónica autorizados (PSC) por el Ente Rector de firma electrónica.

1.2. Los Proveedores de Servicios de Certificación están obligados a proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

1.2.1. El método utilizado para comprobar la identidad del firmante.

1.2.2. Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado.

1.2.3. Si los datos de creación de la firma son válidos y no están en entredicho.

1.2.4. Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación.

1.2.5. Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho.

1.2.6. Si se ofrece un servicio para revocar oportunamente el certificado.

1.3. La aplicación del proceso de verificación segura de firma debe garantizar que se satisfagan al menos los siguientes requisitos:

1.3.1. Que los datos utilizados para verificar la firma correspondan a los datos mostrados al verificador para lo cual, en la aplicación del proceso se deberá:

1.3.1.1. Utilizar la clave pública del firmante para verificar la firma electrónica aplicada en el mensaje de datos (o documento electrónico).

1.3.1.2. Utilizar el proceso denominado “función control” o “función HASH” para verificarla huella digital de la firma.

1.3.2. Que la firma se verifique de forma fiable y el resultado de esa verificación figure correctamente para lo cual, en la aplicación del proceso se deberá:

1.3.2.1. Vincular o rechazar al firmante identificado con una clave pública determinada, en base a la confirmación que devuelva el PSC sobre la fiabilidad de la identificación del titular del certificado con el que se generó la firma electrónica certificada.

1.3.3. Que el verificador pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados para lo cual, en la aplicación del proceso se deberá:

1.3.3.1. Comparar los resultados de las dos huellas digitales (funciones hash generadas), y si son iguales informar en el reporte que el mensaje de datos o documento electrónico no ha sido modificado

después de la firma o, por el contrario, que el contenido del mensaje de datos o documento electrónico ya no es confiable.

1.3.4. Que se verifiquen, de forma fiable, la autenticidad y la validez del certificado exigido al verificarse la firma para lo cual, en la aplicación del proceso se deberá:

1.3.4.1. Verificar que el certificado que genero la firma cumpla con la cadena de confianza establecida por el Ente Rector de firma electrónica para la Infraestructura Nicaragüense de Clave Pública y para el Proveedor de Servicios de Certificación emisor del certificado objeto de la revisión.

1.3.4.2. Verificar que el mensaje de datos contenga un sello cronológico fiable para poder determinar con certeza si la firma electrónica fue creada durante el "periodo de validez" indicado en el certificado.

1.3.4.3. Verificar que el certificado este publicado en el repositorio Protocolo de estado de certificado en línea del Proveedor de Servicio de Certificación emisor.

1.3.4.4. Verificar el estatus del certificado (si es válido, o si está suspendido, o si esta revocado).

1.3.5. Que figuren correctamente el resultado de la verificación y la identidad del firmante para lo cual, en la aplicación del proceso se deberá:

1.3.5.1. Aplicar el método establecido por el Proveedor de Servicio de Certificación para identificar al firmante, haciendo uso de los "medios de acceso" establecidos por el Proveedor de Servicio de Certificación a las partes que confían.

1.3.6. Que conste claramente la utilización de un seudónimo para lo cual, en la aplicación del proceso se deberá:

1.3.6.1. Verificar como parte de la identidad del firmante, este utilizo el seudónimo pre-establecido por el mismo al momento de establecer la relación contractual con el PSC.

1.3.7. Que pueda detectarse cualquier cambio pertinente relativo a la seguridad para lo cual, en la aplicación del proceso se deberá:

1.3.7.1. Verificar en el repositorio del LCR del Proveedor de Servicio de Certificación que los certificados utilizados no sean rechazados por encontrarse revocados o por el vencimiento de la validez del certificado.

1.4. Los Proveedores de Servicios de Certificación deben facilitar al menos una aplicación de validación de firma automatizada y una guía de procedimiento manual, para que las partes que confían puedan realizar la verificación de las firmas haciendo uso de los datos de verificación de firma que tengan a su disposición.

1.5. La utilización de cualquier "Aplicación de validación de firma" no desarrollada por el Proveedores de Servicios de Certificación que presta los servicios de firma electrónica al público, no se considerara fiable en el marco de esta normativa y por lo tanto no acarrea responsabilidad alguna para el Proveedores de Servicios de Certificación que presta los servicios de firma electrónica, ni para el Ente Rector de firma electrónica; ya que esta normativa no regula ese tipo de aplicaciones, así aclarado lo anterior si los firmantes y las partes que confían deciden utilizar alguna aplicación de validación de firma de ese tipo será considerado al tenor de un acuerdo entre las partes.

1.6. Para efectos de facilitar la gestión de verificación de firmas de la cadena de confianza de la Infraestructura Nicaragüense de Clave Pública, tanto los Proveedores de Servicios de Certificación como el Ente Rector de firma electrónica deberá publicar en su sitio web los certificados de clave pública válidos y revocados; en el caso de los Proveedores de Servicios de Certificación los correspondientes a las Autoridad de Certificación Principales que le han sido autorizadas a través del tiempo por el mismo ente rector, y en el caso del Ente Rector los certificados válidos y revocados de su Autoridad de Certificación Raíz Nicaragüense en correspondencia con el "Modelo de Confianza" establecido por el Ente Rector.

2. De Carácter Técnico

2.1. La "Guía de procedimientos manual de verificación de firmas" que facilite el Proveedores de Servicios de Certificación a las <<partes que confían>> deben incluir al menos:

- La verificación de la validez de un certificado electrónico de firma, es decir sin necesidad de recurrir a entidades externas.

- Generalmente es realizada en forma automática por el sistema automatizado con el que se esté utilizando la firma electrónica, ya sea que se trate de un producto comercial adquirido, como puede ser el caso de un cliente de correo electrónico, o como puede ser el caso de un desarrollo particular realizado con un fin específico.

  En líneas generales, se deberá seguir la siguiente secuencia:

2.1.1. Validar que el certificado contenga los siguientes campos.

Nº	Nombre de Campo	Descripción del Campo
1	Versión	Numero de versión (Constante, X-509 Versión 3).
2	Serial Number	Un código de identificación único del certificado.
3	Issuer	Identificación del PSC, con indicación de su nombre o razón social, RUC, dirección de correo electrónico.
4	Signature	Firma de la Autoridad Certificadora del PSC.
5	Subjet	Los datos de identidad del titular, entre los cuales deben necesariamente incluirse su nombre o razón social (en caso de ser persona jurídica), dirección de correo electrónico y cedula de identidad o RUC (en caso de ser persona jurídica).
6	Validity	Plazo de Vigencia (fecha de inicio y fecha de vencimiento).
7	Subjet Public Key Info	Información de la clave pública del usuario (Algoritmo y Valor de la clave pública).
8	Unique Identifiers	Identificador único de la entidad emisora.

2.1.2. Validar los siguientes atributos adicionales:

2.1.2.1. Restricciones básicas del uso de los certificados <<BASIC CONSTRAINS>>.

2.1.2.2. Usos Específicos los cuales se definen en la Política de Certificados relacionada; el certificado debe contener la extensión <<POLITICAS DE CERTIFICACION>> o <<CERTIFICATE POLICIES>> que contiene un enlace (URL) de internet donde se encuentra publicada la "Política de Certificados" correspondiente.

2.1.2.3. <<USO DE CLAVES>> o <<KEYUSAGE>> que es un campo crítico para todos los certificados, en que se describen los usos permitidos de la clave pública, en esta extensión se establecen los usos permitidos para la clave pública incluida en el certificado, los cuales pueden ser:

Nº	Campo	Descripción
1	digitalSignature	Utilizado para verificar la firma electrónica en procesos de autenticación de entidades, autenticación de datos y de integridad.
2	nonRepudiation	Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
3	keyEncipherment	Utilizado para cifrar claves u otra información de seguridad.
4	dataEncipherment	Utilizado para cifrar datos de usuario, pero no claves u otra información de seguridad.
5	keyAgreement	Utilizado para indicar que se utiliza la clave pública para realizar un acuerdo de claves.
6	keyCertSign	Utilizado para indicar que se utiliza la clave pública para verificar las firmas en los certificados.
7	cRLSign	Utilizado para indicar que la clave pública es empleada para la verificación de firmas en las listas de revocación de certificados.
8	encipherOnly	Utilizado para cifrar los datos durante la realización de un acuerdo de claves.
9	decipherOnly	Utilizado solo para descifrar los datos durante la realización de un acuerdo de claves.

2.1.2.4. <<USO DE CLAVES EXTENDIDO>> o <<EXTENDEDKEYUSAGE>> que es otra extensión a considerar, ya que en ella se describen usos adicionales a los antes mencionados mediante la habilitación de distintos atributos:

Nº	Campo	Descripción
1	ServerAuth	Autenticación de SSL/TLS en modo servidor (Certificado de sitio)
2	ClientAuth	Autenticación de SSL/TLS en modo cliente
3	CodeSigning	Firma de código
4	emailProtection	Autenticación, firma y cifrado de correo electrónico
5	timeStamping	Firma de Sellos de tiempo
6	OCSPSigning	Firma de respuestas para el Protocolo de verificación en línea del estado de un certificado (OCSP).

2.1.2.5. <<ALGORITMO DE FIRMA>> o <<Signature Algorithm>>Este campo indica el tipo de algoritmo de firma utilizado según IETF PKIX RFC 5280, el valor mínimo de referencia debe de ser SHA256RSA.

2.1.2.6. <<CLAVE PUBLICA DEL SUJETO>> o <<Subjet Public Key>>Este campo indica el tamaño de la clave pública, así por ejemplo en el caso de la ACRN su contenido es: “Clave Publica RSA de 4096 bits”

2.1.3. Validar la cadena de certificación.

Para la validación de la cadena de certificación, es decir la verificación de que los certificados electrónicos certificados son válidos, debe comprobarse o verificarse en el certificado correspondiente lo siguiente:

a. Que ha sido emitido por una Autoridad de Certificación Emisora de un Proveedores de Servicios de Certificación autorizado, que a su vez está firmado por la Autoridad de Certificación principal del mismo Proveedores de Servicios de Certificación.

b. Que el certificado se encuentra dentro de su periodo de vigencia.

c. Que no se encuentre revocado ni suspendido.

Respecto al certificado de la Autoridad de Certificación Principal de un Proveedores de Servicios de Certificación se debe comprobar/verificar que:

a. Ha sido emitido por la Autoridad de Certificación -RAIZ de la Infraestructura Nicaragüense de Clave Pública o en ausencia de la Autoridad de Certificación - RAIZ de la Infraestructura Nicaragüense de Clave Pública por un Certificado Raíz autofirmado del Proveedor de Servicio de Certificación previamente autorizado por el Ente Rector de Firma electrónica.

b. El certificado se encuentra dentro de su periodo de vigencia.

c. No se encuentre revocado.

2.1.4. Validar el servicio de listas de certificados revocados.

Verificar las correspondientes Listas de Certificados Revocados - CRL (por sus siglas en ingles), tanto de la Autoridad de Certificación del Proveedores de Servicios de Certificación que emitió el certificado electrónico como de la Autoridad de Certificación - RAIZ de la Infraestructura Nicaragüense de Clave Pública; en las mismas se deberá validar los siguiente:

Nº	Campo	Descripción
1	Versión	Debe tener el valor “2”
2	No. LCR	Número que identifica de forma única cada LCR emitida por el PSC.
3	Algoritmo de firma	Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 6818. El algoritmo de firma debe ser como mínimo SHA 256 RSA
4	Nombre del emisor	Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados.
5	Última actualización	Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados.
6	Próxima actualización	Se deberá incluir en este campo la fecha en que se emitirá la próxima lista de certificados revocados
7	Certificados revocados	En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente, y el motivo de la revocación.

2.1.5. Validar el Servicio de Validación del estado de los Certificados en Línea - OCSP las respuestas posibles a cada consulta solamente podrán ser: “VALIDO” o “REVOCADO” o “DESCONOCIDO”.

Si como resultado de la secuencia antes indicada, la verificación es exitosa, se concluye que el certificado presentado fue emitido por una Autoridad de Certificación de un Proveedor de Servicios de Certificación autorizado por el Entidad Rectora DGTEC y, por lo tanto, es válida.
Si alguno de los pasos antes descritos arroja un resultado erróneo, se debe rechazar la firma electrónica por invalida.

2.1.6. Cuando la validación se tenga que realizar dentro de una herramienta ofimática de uso comercial (Adobe, Microsoft office, u otros), el Proveedor de Servicios de Certificación también debe especificar una guía de pasos a seguir dentro de esa herramienta ofimática para que el verificador pueda realizar la validación de la firma.

3. Las Aplicaciones de Validación de Firma que faciliten los Proveedores de Servicios de Certificación a las <<partes que confían>> deberán incluir al menos:

3.1. Las validaciones señaladas en el numeral V.2. Normativas de Carácter Técnico.

3.2. Ser configurables en base a:

3.2.1. Las entradas de los bloques de construcción de validación a realizar.

3.2.2. Las salidas de los bloques de construcción del reporte a presentar.

3.3. Todo el proceso de validación de la aplicación de validación de firma debe estar controlado por un conjunto de restricciones de validación las que se definen mediante políticas.

3.4. Los atributos, reglas, bloques de construcción y restricciones de validación que formen parte de las Aplicación de Validación de Firma deberán ser armonizados con la última versión de las ETSI referidas a continuación según corresponda en cada caso:

3.4.1. Para la estructuración de los bloques de construcción que sean requeridos en el Aplicación de Validación de Firma, se deberán armonizar los aspectos conducentes con el estándar:

- ETSI 319 102 Parte 1 - Procedimientos de Creación y Validación de Firmas Digitales AdES; Parte 1: Creación y Validación.

3.4.2. Para la estructuración e identificación de elementos del informe de validación que sean requeridos en el Aplicación de Validación de Firma, se deberán armonizar los aspectos conducentes con el estándar:

- ETSI 119 102 Parte 2 - Procedimientos para la Creación y Validación de Firmas Digitales AdES; Parte 2: Informe de validación de firma.

3.4.3. Las políticas de validación de firmas, Restricciones de Validación de firmas, Estructura y Semántica del informe de evaluación, y otros aspectos conducentes que sean requeridas para controlar los flujos de las entradas y salidas de la Aplicación de Validación de Firma deberán estar armonizadas con el estándar:

- ETSI 119 172 Parte 1 - Firmas e Infraestructuras Electrónicas (ESI); Políticas de firma; Parte 1: Bloques de construcción y tabla de contenido para documentos de políticas de firma legibles por humanos.

3.4.4. Para la validación de firmas electrónicas certificadas que utilicen el formato CADES se deben armonizar los aspectos conducentes de la aplicación de validación de firma con los estándares:

- ETSI 319 122 Parte 1 - Infraestructuras y firmas electrónicas (ESI); Firmas digitales CADES; Parte 1: Bloques de construcción y firmas de referencia CADES.

- ETSI 319 122 Parte 2 - Infraestructuras y firmas electrónicas (ESI); Firmas digitales CADES; Parte 2: firmas CAdES extendidas.

3.4.5. Para la validación de firmas electrónicas certificadas que utilicen el formato XADES se deben armonizar los aspectos conducentes de la Aplicación de Validación de Firma con los estándares:

- ETSI 319 132 Parte 1 - Infraestructuras y firmas electrónicas (ESI); firmas digitales XAdES; Parte 1: Bloques de construcción y firmas de referencia XAdES.

- ETSI 319 132 Parte 2 - Infraestructuras y firmas electrónicas (ESI); firmas digitales XADES; Parte 2: firmas XAdES extendidas.

3.4.6. Para la validación de firmas electrónicas certificadas que utilicen el formato PAdES se deben armonizar los aspectos conducentes de la Aplicación de Validación de Firma con los estándares:

- ETSI 319 142 Parte 1 - Infraestructuras y firmas electrónicas (ESI); firmas digitales PAdES; Parte 1: Bloques de construcción y firmas de referencia PAdES.

- ETSI 319 142 Parte 2 - Infraestructuras y firmas electrónicas (ESI); firmas digitales PAdES; Parte 2: perfiles de firmas PAdES adicionales.

3.4.7. Normativa de Formatos de firma electrónica.

3.4.8. Normativa de Dispositivos seguros de creación de firma.

3.5. Informe de validación de firma que presente los resultados de las validaciones realizadas, al verificador que utilice la aplicación con base en la estructura de los siguientes bloques de construcción:

3.5.1. Bloque de construcción básico utilizado para la validación de la propia firma (BBB SIG)

3.5.1.1. Chequeo de Formato.

3.5.1.2. Identificación del Certificado de firma.

3.5.1.3. Inicialización del contexto de validación.

3.5.1.4. Validación de Certificado X-509.

3.5.1.5. Verificación criptográfica.

3.5.1.6. Validación de aceptación de firma.

3.5.2. Bloque de construcción básico utilizado para la validación de la marca de tiempo (BBB TIMESTAMP)

3.5.2.1. Identificación del certificado de firma.

3.5.2.2. Validación del certificado x.509.

3.5.2.3. Verificación criptográfica.

3.5.2.4. Validación de aceptación de firma.

3.5.3. Bloque de construcción básico utilizado para la validación de las respuestas OCSP

3.5.3.1. Identificación del certificado de firma.

3.5.3.2. Validación del certificado x.509.

3.5.3.3. Verificación criptográfica.

3.5.3.4. Validación de aceptación de firma.

3.5.4. Verificación de Listas de confianza (cuando aplique).

3.6. Cada bloque de construcción deberá presentar los resultados individuales de los elementos evaluados con una leyenda de “APROBADO” o “NO APROBADO” según sea el caso de que “si cumple” o “no cumple” con la validación realizada.

3.7. El resultado final del informe de validación de firma deberá ser uno de los siguientes:

3.7.1. “FIRMA VALIDA” si y solo si los resultados de todas las validaciones de los distintos bloques de construcción configurados para validar una firma devuelven un resultado de “APROBADO”.

3.7.2. “FIRMA NO VALIDA” en caso de que al menos uno de los resultados de los bloques de construcción configurados para validar la firma electrónica certificada devuelva un resultado de “NO APROBADO”.