RENIEC

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

NORMA ADMINISTRATIVA INTERNA

FEDATACIÓN JURAMENTADA PARA LA GENERACIÓN DE MICROFORMAS CON VALOR LEGAL

RESOLUCIÓN SECRETARIAL N° 12 -2018/SGEN/RENIEC		
NAI-411-SGEN/002	VERSIÓN: 02	FECHA DE APROBACIÓN
	N° PÁGINAS: 14	01 MAR. 2018

ÍNDICE

I. OBJETIVO

Establecer y regular las actividades realizadas por el Fedatario Juramentado del RENIEC durante el proceso de aplicación de la firma digital en un documento electrónico para su conversión a microformas con valor legal.

El presente documento es de aplicación obligatorio por los Fedatarios Juramentados del RENIEC, y debe ser fuente de consulta por los órganos y unidades orgánicas que participan en el proceso de generación de microformas con valor legal.

II. BASE LEGAL

2.1 **Ley N° 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, del 12 de julio de 1995 y sus modificatorias.

2.2 **Ley N° 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y sus modificatorias.

2.3 **Decreto Legislativo Nº 681**, Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras, del 14 de octubre de 1991 y sus modificatorias.

2.4 **Decreto Supremo Nº 052-2008-PCM**, aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, del 19 de julio de 2008 y sus modificatorias.

2.5 **Resolución Directoral Nº 016-2015/INACAL/DN**, aprueba la Norma Técnica Peruana NTP 392.030-2:2015 MICROFORMAS. Requisitos para las organizaciones que administran sistemas de producción y almacenamiento. Parte 2: Medios de archivo electrónico. 3ra Edición, que remplaza a la NTP 392.030-2:2005, del 31 de diciembre de 2015.

2.6 **Resolución Jefatural N° 073-2016/JNAC/RENIEC**, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 01 de junio del 2016.

2.7 **Resolución Secretarial N° 55-2017/SGEN/RENIEC,** aprueba la Directiva DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", del 28 de agosto de 2017.

2.8 **Resolución Gerencial N° 000005-2015/GTI/RENIEC,** aprueba el Manual de Usuario MU-349-GTI/SGIS/146 "Software de Firma Digital ReFirma", del 12 de febrero de 2015.

2.9 **Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias N°140-2012/CNB-INDECOPI**, del 28 de diciembre de 2012.

III. DESCRIPCIÓN

3.1 COBERTURA DEL PROCESO DE FEDATACIÓN JURAMENTADA

3.1.1 Comprende la firma digital de los archivos electrónicos para su conversión a microformas con la intervención del Fedatario Juramentado, según los requisitos de la NTP 392.030-2:2015 y regulaciones asociadas a la normatividad peruana vigente.

3.1.2 El dueño del proceso es el Fedatario Juramentado y el cliente es el órgano o unidad orgánica quien administra el Sistema de Producción de Microformas.

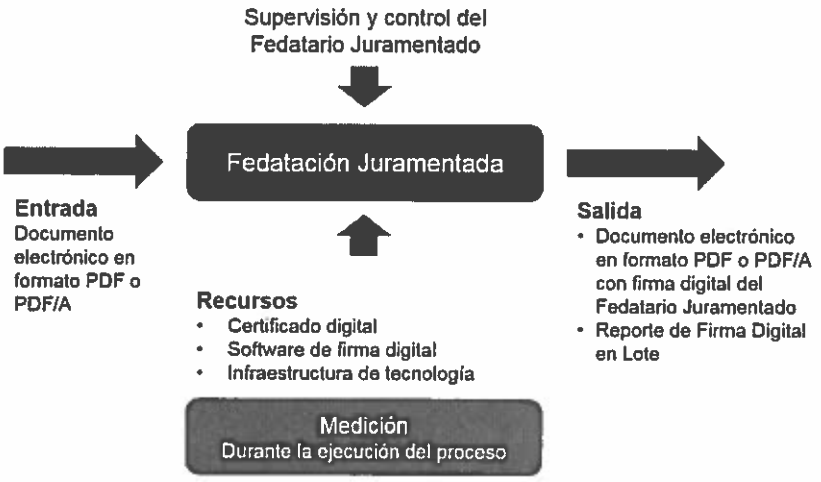
3.1.3 El proceso de Fedatación Juramentada es realizado por el Fedatario Juramentado, quien debe contar con su certificado digital vigente. Para llevar a cabo este proceso, se debe tener en ejecución del Software de Firma Digital ReFirma, sobre el soporte de la Infraestructura de Tecnología de la Información necesaria.

3.1.4 Son procesados los documentos electrónicos en formato PDF o PDF/A, a los cuales se les incorpora la firma digital del Fedatario Juramentado, para dar lugar a las microformas con valor legal.

3.1.5 La medición de la eficiencia y eficacia del proceso se realiza durante el procesamiento, es decir, conforme se ejecuta el ReFirma, emitiendo como resultado final un Reporte de Firma Digital en Lote.

3.1.6 La Figura N° 01 muestra una representación ilustrativa del Diagrama del Proceso de Fedatación Juramentada.

Figura N° 01. Diagrama del Proceso de Fedatación Juramentada



3.2 CONSIDERACIONES DEL PROCESO DE FEDATACIÓN JURAMENTADA

3.2.1 Los documentos electrónicos que serán convertidos a microformas, son indicados por el Fedatario Juramentado, determinando el ámbito del mismo.

Nota 1. El ámbito se basa en el costo, tiempo, riesgo, restricción, limitación, entre otros aspectos a considerarse por parte del Fedatario Juramentado.

3.2.2 Una microforma generada anteriormente, puede volver a ser firmada por el Fedatario Juramentado, acorde al presente proceso regulado.

3.2.3 Una microforma con valor legal es generada dentro del alcance de una certificación de idoneidad técnica para producción de microformas, en cumplimiento de las normas técnicas y legales aplicables.

3.2.4 Si no hay documentos electrónicos para su conversión a microformas, entonces no entra en aplicación la presente normativa interna.

3.2.5 Si alguno de los elementos del proceso no se encuentra disponible, no debe ejecutarse el presente procedimiento.

3.3 DEL FORMATO DEL ARCHIVO ELECTRÓNICO

3.3.1 El archivo electrónico contiene a uno o varios documentos electrónicos.

3.3.2 El documento electrónico o microforma debe tener el formato PDF o PDF/A (estándar ISO 32000) y solo debe contener imágenes en modo estático.

3.3.3 El documento electrónico contiene información registrada que puede ser tratada como una unidad. Es representado mediante una o varias imágenes.

3.3.4 Una microforma es una imagen o imágenes de un documento electrónico que se encuentra firmada digitalmente por el Fedatario Juramentado en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE) y que se encuentra grabada en un medio físico técnicamente idóneo.

3.3.5 La incorporación de la firma digital al documento electrónico conlleva a incrementar su magnitud, el mismo que no afecta su integridad.

3.3.6 La reproducción a partir de las microformas o microduplicados no se encuentra delimitada.

3.3.7 No es necesaria la delimitación de la magnitud (tamaño) del archivo electrónico en bytes. Excepcionalmente, pudiera darse si es que técnicamente no se cuenta con los recursos para su procesamiento.

3.4 DEL CERTIFICADO DE FIRMA DIGITAL

3.4.1 El certificado digital a ser utilizado en el proceso, es aquel emitido por la Entidad de Certificación del Estado Peruano representado por el Registro Nacional de Identificación y Estado Civil (ECEP RENIEC), el cual a su vez se encuentra acreditado ante la Autoridad Administrativa Competente representada por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

Nota 2. Resolución N° 140-2012/CNB-INDECOPI, corresponde al Expediente N° 009-2012-CNB/FD, con la cual se acredita a la Entidad de Certificación Digital Intermedia para el Estado Peruano (ECEP) del RENIEC, declarando cumplidos los requisitos establecidos en la Guía de Acreditación de Entidades de Certificación Digital para el nivel de seguridad medio.

3.4.2 Previo a la emisión del Certificado Digital, su titular ha sido identificado y autenticado, y aceptado y autorizada su solicitud de emisión de Certificado Digital por parte de la EREP RENIEC, la cual a su vez se encuentra acreditada ante el INDECOPI, dentro del marco de la IOFE.

3.4.3 El certificado digital vincula la identidad física de una persona con su identidad digital, por tanto, resulta ser un único certificado digital para el Fedatario Juramentado.

3.5 DE LA FIRMA DIGITAL

3.5.1 Una firma digital generada a partir de un certificado digital emitido por la ECEP RENIEC, previo registro de la EREP RENIEC, cumple con todas las funciones de la firma manuscrita, es decir, identificar a la persona que firma (signatario), vincular al documento a la persona que realiza la firma y preservar la integridad del documento firmado. Por consiguiente, tiene la misma validez y eficacia jurídica (equivalencia funcional) que la firma manuscrita de la persona, en tanto haya sido generada dentro de la IOFE.

3.5.2 La firma digital generada en el marco de la IOFE, e incorporada a la microforma es inalterable, fija, durable y comprobable su autenticidad en forma indubitable.

3.6 DEL SOFTWARE DE FIRMA DIGITAL

3.6.1 El software de firma digital que será empleado en este procedimiento es el ReFirma, el cual se encuentra registrado y acreditado ante el INDECOPI a nombre del RENIEC.

3.6.2 Las características del ReFirma descritas a la presente normativa han sido tomadas del Manual de Usuario MU-349-GTI/SGIS/146 "Software de Firma Digital ReFirma". Cumpliendo con las características descritas a continuación:

3.6.2.1 Capacidad de visualización, firma y verificación de documentos en formato PDF 1.7 (ISO 32000-1:2008).

- Es posible efectuar múltiples firmas digitales en un mismo documento.
- Es posible generar firmas digitales incluyendo sellos de tiempo.
- Es posible firmar documentos en lote o uno a la vez.
- Es posible verificar un documento con múltiples firmas digitales.
- Es posible verificar firmas digitales en documentos en lote o uno a la vez.
- Es posible visualizar, firmar y verificar un documento firmado usando otro software de firma digital.

3.6.2.2 Capacidad de verificación de documentos PDF firmados digitalmente

- Constata la integridad del documento firmado.
- Visualiza información de la firma y del certificado asociado.
- Visualiza información referida a la ruta de certificación de todas las firmas digitales del documento.

3.6.2.3 Capacidad de verificación de la validez de un certificado.

- Constata que el certificado sirve para efectuar firmas digitales.
- Constata que, al momento de la firma, el certificado se encuentre vigente o no haya expirado.

- Verifica el estado de revocación de un certificado de forma automatizada (procesamiento de CRLs, cuya URL es obtenida de los atributos del certificado procesado).

3.6.2.4 Capacidad de procesamiento de la TSL

- Obtención de la TSL (estándar ETSI TS 102 231) oficial del INDECOPI para la verificación de la ruta de certificación del certificado.
- Procesamiento de las Entidades de Certificación acreditadas en la TSL.
- Verificación de la integridad de la TSL.

3.6.2.5 Capacidad de desarrollar rutas de certificación. Una ruta de certificación es un árbol jerárquico compuesto de certificados, CRLs o respuestas OCSP.

3.6.2.6 Capacidad de procesamiento de la ruta de certificación. Para cada elemento de la ruta.

- Verifica las firmas del certificado, para lo cual, usa la clave pública del certificado del emisor.
- Verifica que la fecha de realización del proceso de firma se encuentra dentro del periodo de vigencia del certificado.
- Verifica que el uso del certificado es consistente con sus extensiones (distingue: firma, autenticación y cifrado).
- Verifica que el certificado no haya sido revocado.
- Si el elemento verificado es el certificado de una entidad de certificación raíz, verifica su estado en la TSL.
- Si una de las verificaciones anteriores no es satisfactoria, no se permite efectuar la firma digital.

3.6.2.7 Capacidad de interacción con dos fuentes de certificados.

3.6.2.8 Instalados y gestionados por el sistema operativo Ms Windows.

3.6.3 El ReFirma permite la realización de la firma digital de uno o varios documentos electrónicos (firma en lote). Es responsabilidad del signatario verificar y validar el contenido del documento previo a la generación de la firma digital. Al finalizar, la generación de las firmas digitales, el ReFirma emite un Reporte Resumen.

3.6.4 A fin de verificar la validez de las firmas digitales de los documentos electrónicos, el ReFirma emite el reporte de firma digital para validar la procedencia y vigencia de los certificados digitales.

3.6.5 El ReFirma debe tener activos los servicios TSL (Lista de estado de servicios de confianza), TS (Sellado de Tiempo) y/o OCSP (Protocolo del estado en línea del certificado).

3.6.6 Para el sellado de tiempo, puede configurarse el servicio brindado por el RENIEC; caso contrario, puede optarse por la hora local del servidor o estación cliente desde donde se generará la firma de documentos electrónicos. En este último caso, el Fedatario Juramentado debe

asegurarse de que se encuentre correctamente sincronizada la fecha y hora del computador.

3.6.7 Si fuera el caso de que el servicio TSL del INDECOPI no se encontrase en línea, entonces se debe acudir a la CRL (Lista de Certificados Digitales Revocados) del RENIEC, a manera de contingencia. Particularmente, el Fedatario Juramentado del RENIEC debe disponer de un certificado digital de firma emitido por la ECEP RENIEC, del cual es posible su validación efectiva en un entorno de la INTRANET RENIEC.

Nota 3. La CRL (Lista de Certificados Digitales Revocados) del RENIEC opera en la Planta PKI del RENIEC, por tanto, si las operaciones de firma y verificación ocurren en un entorno de INTRANET, no es necesarios que se acceda a la TSL del INDECOPI.

3.6.8 El ReFirma opera según los requerimientos de hardware y software indicados en el Manual de Usuario MU-349-GTI/SGIS/146 "Software de Firma Digital ReFirma", que corresponde a la Infraestructura de Tecnología.

3.7 DEL PROCEDIMIENTO

Para efecto del presente procedimiento, el proceso de Fedatación Juramentada se realiza como parte de una línea de producción de microformas que cuenta con su respectivo certificado de idoneidad técnica vigente, requiriéndose para tal efecto contar con un módulo de operaciones (un proceso) asignado al Fedatario Juramentado (ver Figura N° 01).

PREVIO AL PROCEDIMIENTO

3.7.1 Se debe coordinar con la Gerencia de Tecnología de la Información, la asignación de un repositorio de tipo *filesystem* en un servidor virtual seguro, para ejecutar el proceso de Fedatación Juramentada.

3.7.2 Los documentos electrónicos en formato PDF o PDF/A, deben encontrarse en una ruta ***Origen***, en el repositorio del tipo *filesystem*.

3.7.3 Debe haberse creado el repositorio ***Destino*** en el *filesystem* asignado. El directorio ***Destino*** debe encontrarse libre de algún archivo electrónico.

3.7.4 El software de firma digital debe encontrarse operativo, con los servicios asociados requeridos activos en relación a la conectividad interna (LAN o MAN) y externa (Internet), sin ningún documento electrónico en formato PDF o PDF/A iniciado.

3.7.5 El certificado de firma digital debe ser el emitido por la Entidad de Certificación para el Estado Peruano (ECEP), previo registro ante la Entidad de Registro para el Estado Peruano (EREP), y encontrarse vigente para su utilización por parte del Fedatario Juramentado.

3.7.6 El Fedatario Juramentado debe tener su certificación de idoneidad técnica vigente, para la realización del proceso.

DURANTE EL PROCESAMIENTO

3.7.7 Ubicar las rutas de ***Origen*** (repositorio/directorio) de los documentos electrónicos en formato PDF o PDF/A y las rutas de ***Destino***.

3.7.8 Verificar y validar los contenidos de los documentos electrónicos, previo a la incorporación de la firma digital en los mismos. Este paso

es opcional, si previamente se ha ejecutado un control de calidad a los documentos electrónicos.

3.7.9 Seleccionar el certificado digital del Fedatario Juramentado que se empleará en el proceso.

3.7.10 Ejecutar el software de firma digital ReFirma.

3.7.11 Revisar el reporte resumen del procedimiento de la incorporación de la firma digital a los documentos electrónicos.

3.7.12 Inspeccionar los documentos electrónicos firmados en la ruta de ***Destino***.

3.7.13 En caso de existir alguna observación, revisar las consideraciones que se deben tener en cuenta para el procesamiento, así como los pasos previos a fin de subsanarlos, e iniciar nuevamente el procedimiento.

3.7.14 Caso contrario, al no existir ninguna observación, se dará por terminado el procedimiento.

POSTERIOR AL PROCESAMIENTO

3.7.15 En caso sea requerido la realización de la verificación de la firma digital incorporada en los documentos electrónicos, deberá ejecutarse la opción de Firma Digital en Lote del software ReFirma.

3.7.16 El paso anterior, puede ser ejecutado inmediatamente después a la realización de la firma digital en lote, o en otro momento posterior. Debiéndose tener especial cuidado en el manejo del directorio ***Destino***.

3.7.17 Esta verificación, puede ser realizada al 100% o según criterio del Fedatario Juramentado.

3.7.18 Requerir la generación de respaldo de los medios de archivo electrónico.

3.7.19 Proceder con la limpieza de los repositorios de ***Origen*** y ***Destino***.

3.7.20 Enseguida, debe procederse con los subsiguientes procesos de la micrograbación.

3.8 DE LA SEGURIDAD Y CONTINUIDAD DE LAS OPERACIONES

3.8.1 Los requisitos técnicos para la operatividad del proceso definidos en el presente procedimiento deben cumplirse, de lo contrario las operaciones no podrían ejecutarse, por tratarse de un proceso automático y solo requerir de la presencia del Fedatario Juramentado con fines de supervisión.

3.8.2 Las microformas, bajo la modalidad de documentos producidos por procedimientos informáticos y medios similares, deben tener sistemas de seguridad de datos e información que aseguren su inalterabilidad e integridad. Estos sistemas de seguridad se encuentran a cargo de la Gerencia de Tecnología de la Información, quien debe brindar el soporte técnico correspondiente.

3.8.3 En caso de registrarse alguna incidencia respecto de los servicios de tecnología, debe comunicarse al servicio de Mesa de Ayuda a cargo de la Gerencia de Tecnología de la Información. Caso contrario, la incidencia registrada y asociada a los servicios de certificación digital, son comunicadas a la Gerencia de Certificación y Registro Digital.

3.8.4 La ausencia de servicios no listados en el presente procedimiento, relacionados a infraestructura física, mobiliario, servicios de agua, energía eléctrica, entre otros similares, deben ser comunicados a la Gerencia de Administración.

3.8.5 Los respaldos de los documentos electrónicos existentes en los repositorios Origen y Destino del servidor de trabajo, se encuentran a cargo de la Gerencia de Tecnología de la Información, según las indicaciones dadas por el Fedatario Juramentado.

IV. VIGENCIA

Entrará en vigencia a partir de su aprobación.

V. APROBACIÓN

Será aprobada mediante Resolución Secretarial.

VI. ANEXOS

ANEXO N° 01. GLOSARIO DE TÉRMINOS

1. **Archivo electrónico.** Conjunto de documentos electrónicos conservados por cualquier técnica, en cualquier medio electrónico.
2. **Autoridad Administrativa Competente**. Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados de reconocer estándares tecnológicos aplicables en la IOFE; de supervisar dicha infraestructura y las otras funciones señaladas en el Reglamento de la Ley de Firmas y Certificados Digitales o aquellas que requieran en el transcurso de sus operaciones (Decreto Supremo N° 052-2008-PCM).

   De acuerdo a las atribuciones conferidas por medio del D. S. N° 052-2008-PCM, el Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual (INDECOPI) es la Autoridad Administrativa Competente para acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y los Prestadores de Servicios de Valor Añadido.
3. **Certificado digital.** Es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.
4. **Documento electrónico.** Unidades estructuradas de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesadas o conservadas por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.
5. **Fedatario Juramentado.** Depositario de la fe pública que cuenta con su respectivo diploma de idoneidad técnica vigente de acuerdo a los requisitos exigido en el D. Leg. N° 681 y S.S. N° 009-92-JUS.
6. **Firma digital.** Es un tipo de firma electrónica que utiliza una técnica de criptografía asimétrica (basada en el sistema de pares de claves) y garantiza la autoría, la integridad y la aceptación de los documentos electrónicos "suscritos" con ella.

   Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil. (D. S. N° 052-2008-PCM).

   Las características mínimas de la firma digital generada dentro de la IOFE son:

   a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado.
   b) Es exclusiva del suscriptor y de cada documento electrónico firmado por este.

c) Es susceptible de ser verificada usando la clave pública del suscriptor.
d) Su generación está bajo el control exclusivo del suscriptor.
e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado.

7. **Imagen.** Representación por apropiados medios de un apropiado receptor (pantalla, superficie fotosensible, etc.) de un objeto o de un dato correspondiente a dicho objeto.

8. **Infraestructura Oficial de Firma Electrónica (IOFE).** Es el sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente. Tiene como principales objetivos los siguientes:

   a) Generar firmas digitales en las que participan Entidades de Certificación y Entidades de Registro o Verificación acreditadas ante la Autoridad Administrativa Competente.

   b) Proporcionar diversos niveles de seguridad con respecto a la integridad del documento electrónico y la identidad del autor del mismo.

9. **Medio de Archivo Electrónico (Medio).** Medio con aptitud para contener archivos en formato digital. Para efectos del presente procedimiento, un medio de archivo electrónico es aquel que contiene archivos de microformas digitales (CD, DVD, Blu-Ray, otros).

10. **Microforma.** Un término genérico para cualquier medio que contiene imágenes. (NTP 392.030-2:2015).

    Imagen reducida y condensada o compactada o digitalizada de un documento, que se encuentra grabados en un medio físico técnicamente idóneo, que le sirve de soporte material portador, mediante un proceso fotoquímico, informático, electrónico, electromagnético, o que emplee alguna tecnología de efectos equivalentes, de modo que tal imagen se conserve y pueda ser vista y leída con la ayuda de equipos visores o métodos análogos; y pueda ser reproducida en copias impresas, esencialmente iguales al documento original.

    Están incluidos en el concepto de microforma tanto los documentos producidos por procedimientos informáticos o telemáticos en computadoras o medios similares como los producidos por procedimientos técnicos de microfilmación. (D. Leg. N° 681).

11. **Micrograbación.** Proceso técnico por el cual se obtienen las microformas, a partir de los documentos originales en papel o material similar; o bien directamente de los medios o soportes electromagnéticos, digitales u otros en que se almacena información producida por computador u ordenador.

12. **Sellado de tiempo (TS).** Se refiere al servicio que permite consignar la fecha y hora cierta de la existencia de un documento electrónico.

13. **Lista de Estado de Servicio de Confianza (TSL).** Es la lista de confianza que incluye a los PSCs acreditados, autorizados a operar en el marco de la IOFE. Su propósito consiste en proveer de modo ordenado información del estado de los proveedores de servicios considerados confiables (acreditados) y los proveedores supervisados por la Autoridad Administrativa Competente.

ANEXO N° 02. CUADRO DE CONTROL DE CAMBIOS

CUADRO DE CONTROL DE CAMBIOS	
IDENTIFICACIÓN DEL CAMBIO	
Numeral vigente	**Numeral modificado**
I OBJETIVO	I OBJETIVO
No existía en esta versión	II BASE LEGAL
No existía en esta versión	Numeral 2.1
No existía en esta versión	Numeral 2.2
No existía en esta versión	Numeral 2.3
No existía en esta versión	Numeral 2.4
No existía en esta versión	Numeral 2.5
No existía en esta versión	Numeral 2.6
No existía en esta versión	Numeral 2.7
No existía en esta versión	Numeral 2.8
No existía en esta versión	Numeral 2.9
II DESCRIPCION	III DESCRIPCION
Numeral 2.1	Eliminado
Numeral 2.1.1	Numeral 3.1
Literal a	Numeral 3.1.1
Literal b	Numeral 3.1.2
Literal c	Numeral 3.1.3
Literal d	Numeral 3.1.4
Literal e	Numeral 3.1.5
Literal f	Numeral 3.1.6
Numeral 2.1.2	Numeral 3.2
Literal a	Numeral 3.2.1
Literal b	Numeral 3.2.2
Literal c	Numeral 3.2.3
Literal d	Numeral 3.2.4
Literal e	Numeral 3.2.5
Numeral 2.2	Numeral 3.3
Literal a	Numeral 3.3.1
Literal b	Numeral 3.3.2
Literal c	Numeral 3.3.3
Literal d	Numeral 3.3.4
Literal e	Numeral 3.3.5
Literal f	Numeral 3.3.6
Literal g	Numeral 3.3.7
Numeral 2.3	Numeral 3.4
Numeral 2.3	Numeral 3.4.1
Numeral 2.3	Numeral 3.4.2
Numeral 2.3	Numeral 3.4.3
Numeral 2.4	Numeral 3.5
Numeral 2.4	Numeral 3.5.1
Numeral 2.4	Numeral 3.5.2
Numeral 2.5	Numeral 3.6
Numeral 2.5	Numeral 3.6.1
Numeral 2.5	Numeral 3.6.2
Numeral 2.5	Numeral 3.6.3
Numeral 2.5	Numeral 3.6.4
Numeral 2.5	Numeral 3.6.5

CUADRO DE CONTROL DE CAMBIOS	
IDENTIFICACIÓN DEL CAMBIO	
Numeral vigente	**Numeral modificado**
Numeral 2.5	Numeral 3.6.6
Numeral 2.5	Numeral 3.6.7
Numeral 2.5	Numeral 3.6.8
Numeral 2.6	Numeral 3.7
No existía en esta versión	Numeral 3.7.1
Numeral 2.6.1	Numeral 3.7.2
Numeral 2.6.2	Numeral 3.7.3
Numeral 2.6.3	Numeral 3.7.4
Numeral 2.6.4	Numeral 3.7.5
Numeral 2.6.5	Numeral 3.7.6
Numeral 2.6.6	Numeral 3.7.7
Numeral 2.6.7	Numeral 3.7.8
Numeral 2.6.8	Numeral 3.7.9
Numeral 2.6.9	Numeral 3.7.10
Numeral 2.6.10	Numeral 3.7.11
Numeral 2.6.11	Numeral 3.7.12
Numeral 2.6.12	Numeral 3.7.13
Numeral 2.6.13	Numeral 3.7.14
Numeral 2.6.14	Numeral 3.7.15
Numeral 2.6.15	Numeral 3.7.16
Numeral 2.6.16	Numeral 3.7.17
Numeral 2.6.17	Numeral 3.7.19
Numeral 2.6.18	Numeral 3.7.18
Numeral 2.6.19	Numeral 3.7.20
Numeral 2.7	Numeral 3.8
Numeral 2.7	Numeral 3.8.1
Numeral 2.7	Numeral 3.8.2
Numeral 2.7	Numeral 3.8.3
Numeral 2.7	Numeral 3.8.4
Numeral 2.7	Numeral 3.8.5
III VIGENCIA	IV VIGENCIA
IV APROBACIÓN	V APROBACIÓN
V ANEXO	VI ANEXOS