



Identidad  
*digital* @



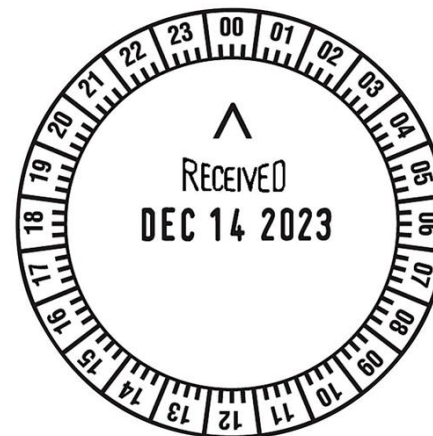
# SERVICIO DE SELLADO DE TIEMPO

**PSVA-TSA-RENIEC**



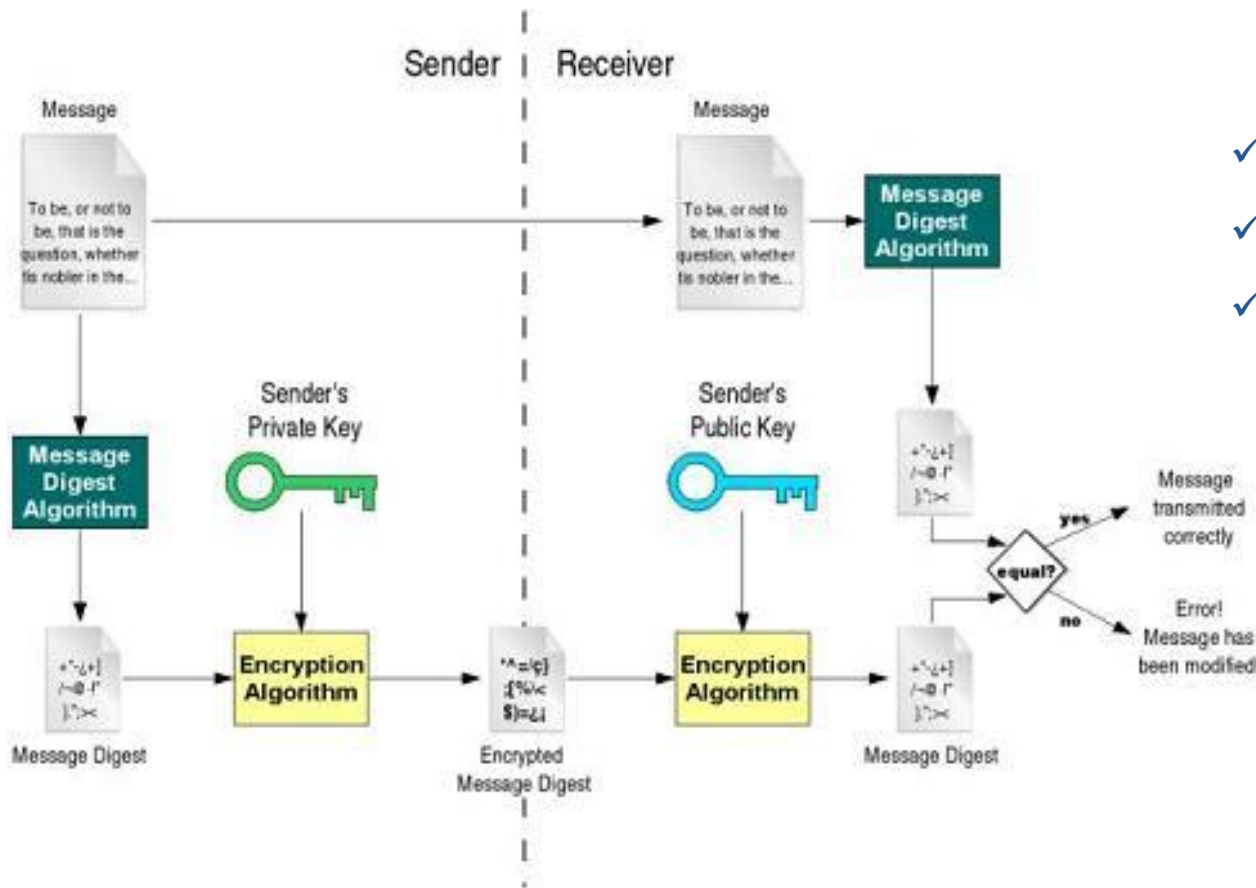
## CONTENIDO

1. Conceptos: Firmas digitales, Sello y sellado de Tiempo
2. Estándares internacionales
3. Normativa Peruana
4. PSVA-TSA-RENIEC
5. Usos del sello de tiempo
6. Preguntas





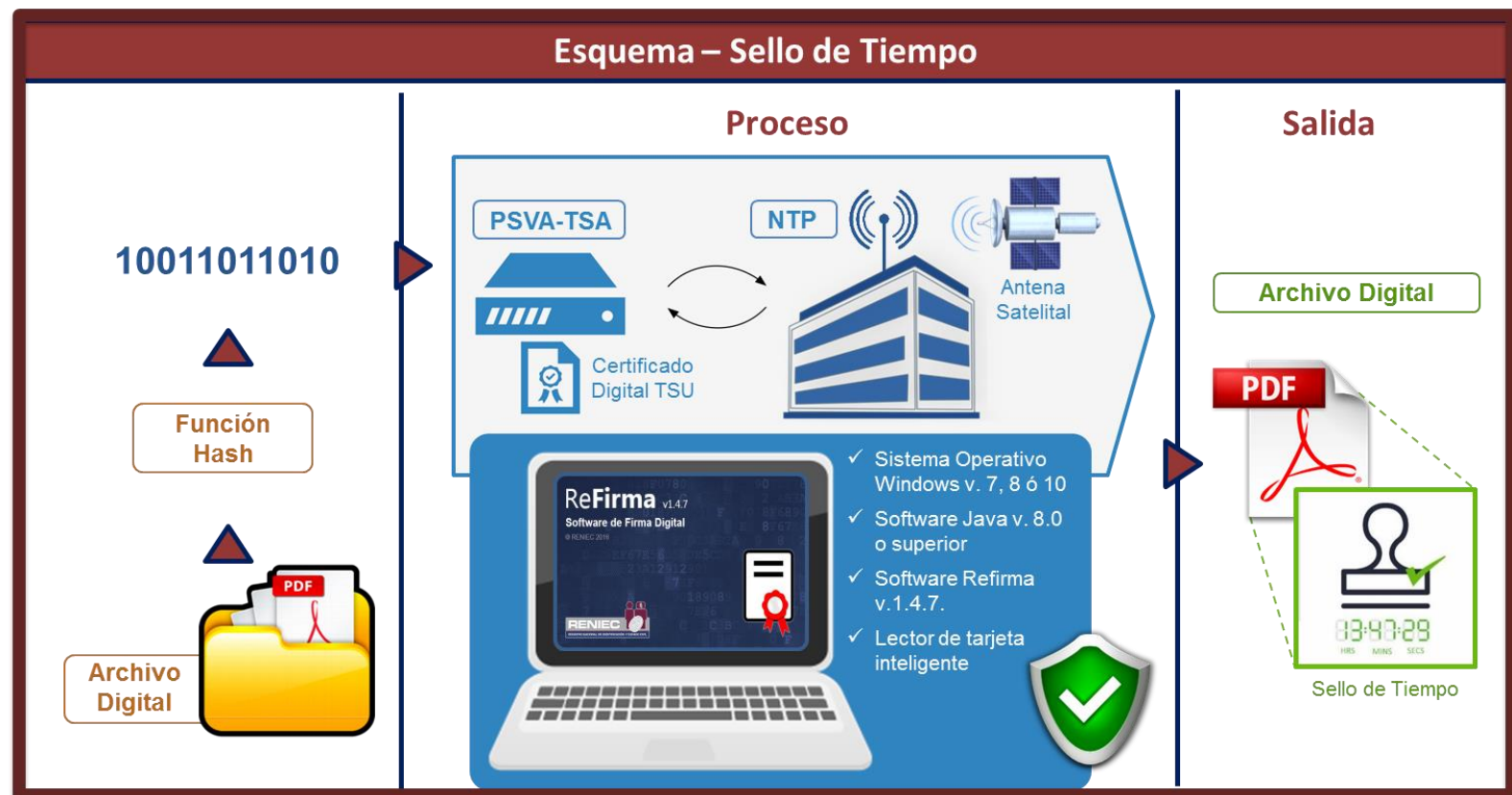
# 1. CONCEPTOS BÁSICOS – FIRMA DIGITAL



- ✓ *Identidad del firmante*
- ✓ *Mensaje no alterado*
- ✓ *No repudio*



# 1. CONCEPTOS BÁSICOS – SELLO DE TIEMPO



- ✓ *Mensaje no alterado*
- ✓ *Existencia del mensaje en el momento que se selló*



Identidad  
*digital* @



## 1. CONCEPTOS BÁSICOS – SELLO DE TIEMPO

*“A time-stamp on a document shows that this document existed at a certain point in time and has not been changed since.”*

**Msc. Martín Augusto Gagliotti Vigil**  
**T trustworthy and Efficient Protection Schemes for Digital Archiving**

*“Un sello de tiempo en un documento indica que ese documento existió en un determinado instante de tiempo y que no ha cambiado desde entonces”*



## 1. CONCEPTOS BÁSICOS – AUTORIDAD DE SELLADO DE TIEMPO



✓ *TSA: Time-Stamping Authority*

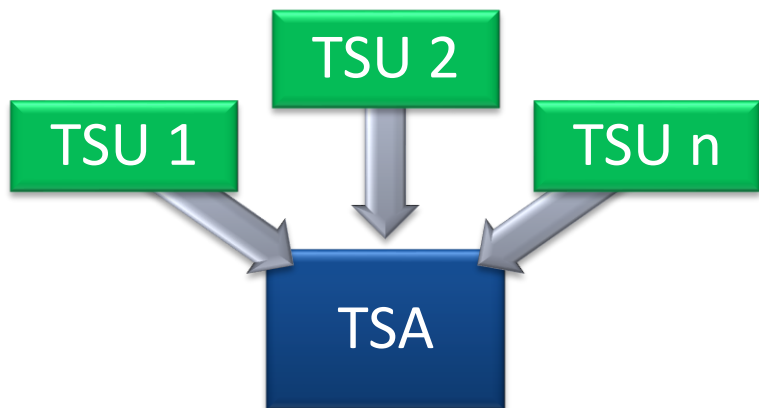


✓ *PSVA-TSA: Prestador de Servicios de Valor Añadido en modalidad de TSA*

✓ *PSVA-TSA-RENIEC: PSVA en modalidad TSA del RENIEC.*



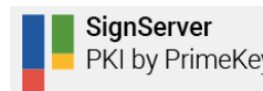
## 1. CONCEPTOS BÁSICOS – TSU



✓ *Hardware*



✓ *Software*



✓ *Llaves*



✓ *Certificado*



**Time-Stamping Unit (TSU):** set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

**ETSI EN 319-422**

*TSU: El conjunto de hardware y software que es gestionado como una unidad y tiene asociada una llave de emisión de sellos de tiempo a la vez.*



## 2. ESTÁNDARES INTERNACIONALES

Normativos

Técnicos



### RFC 3628

Internet X.509 Public Key Infrastructure  
Time-Stamp Protocol (TSP)

### RFC 3161

Internet X.509 Public Key Infrastructure  
Time-Stamp Protocol (TSP)



### ETSI EN 319 421

Policy and Security Requirements for Trust  
Service Providers issuing Time-Stamps

### ETSI EN 319 422

Time-stamping protocol and time-stamp  
token profiles





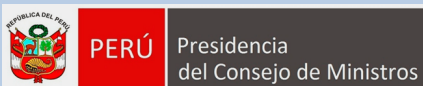
## 3. NORMATIVA PERUANA

1



- ❖ Ley de Firmas y Certificados Digitales Ley N° 27269

2



- ❖ Reglamento de la Ley de Firmas y Certificados Digitales D.S. 052-2008-PCM (19JUL2008)
- ❖ Modificatoria D.S. 026-2016-PCM (29ABR2016)

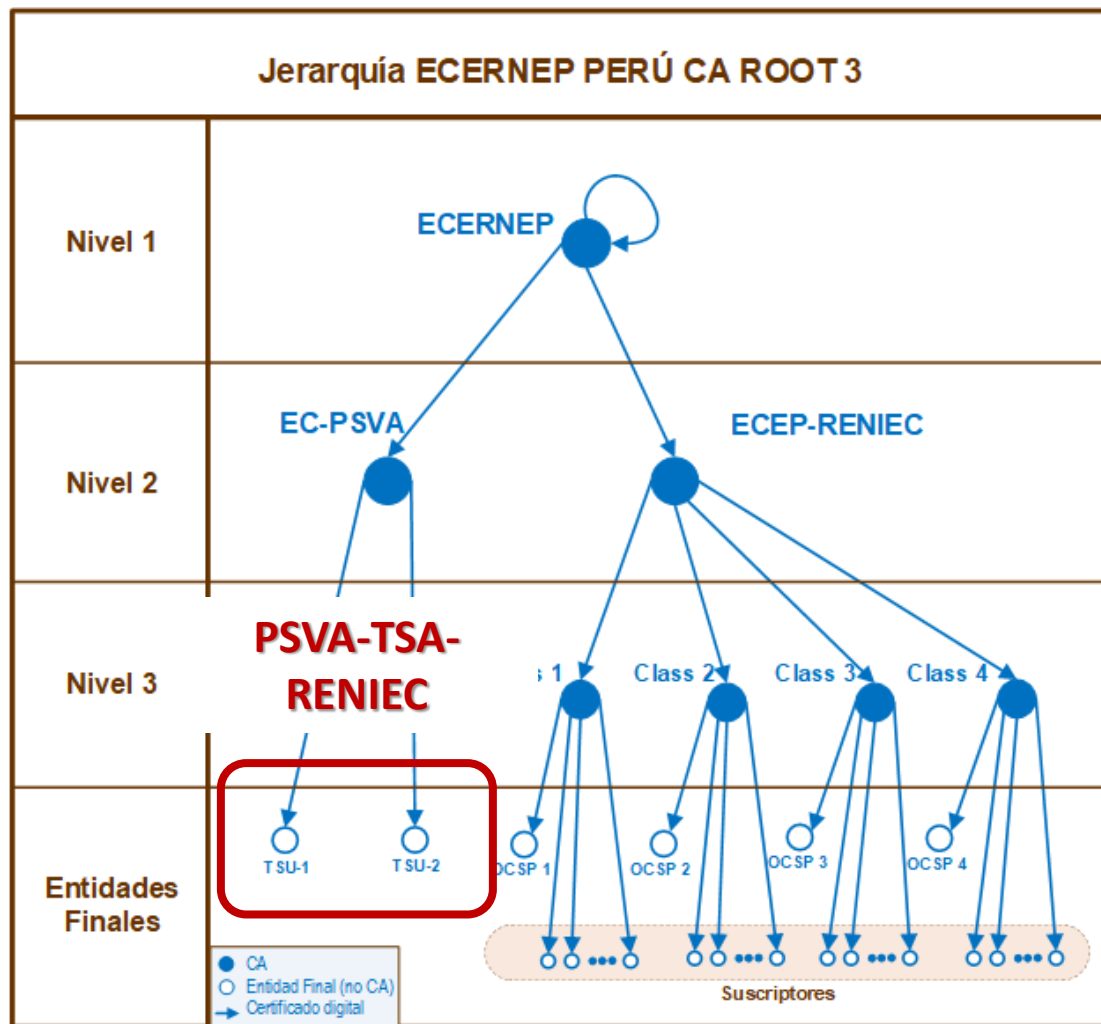
3



- ❖ Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA



## 4. PSVA-TSA-RENIEC



✓ 2 certificados TSU



## 4. PSVA-TSA-RENIEC

Certificado

General Detalles Ruta de certificación

**Información del certificado**

**Este certif. está destinado a los siguientes propósitos:**

- Permite que los datos sean firmados con la hora actual
- 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0
- 0.4.0.2023.1

\*Para ver detalles, consulte la declaración de la entidad de ce

**Emitido para:** PSVA-TSA-RENIEC TSU-01

**Emitido por:** EC-PSVA

**Válido desde** 10/ 08/ 2017 **hasta** 10/ 08/ 2029

Instalar certificado... Declaración del emisor

Obtener más información acerca de [certificados](#)

Aceptar

Certificado

General Detalles Ruta de certificación

**Información del certificado**

**Este certif. está destinado a los siguientes propósitos:**

- Permite que los datos sean firmados con la hora actual
- 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0
- 0.4.0.2023.1

\*Para ver detalles, consulte la declaración de la entidad de ce

**Emitido para:** PSVA-TSA-RENIEC TSU-02

**Emitido por:** EC-PSVA

**Válido desde** 10/ 08/ 2017 **hasta** 10/ 08/ 2029

Instalar certificado... Declaración del emisor

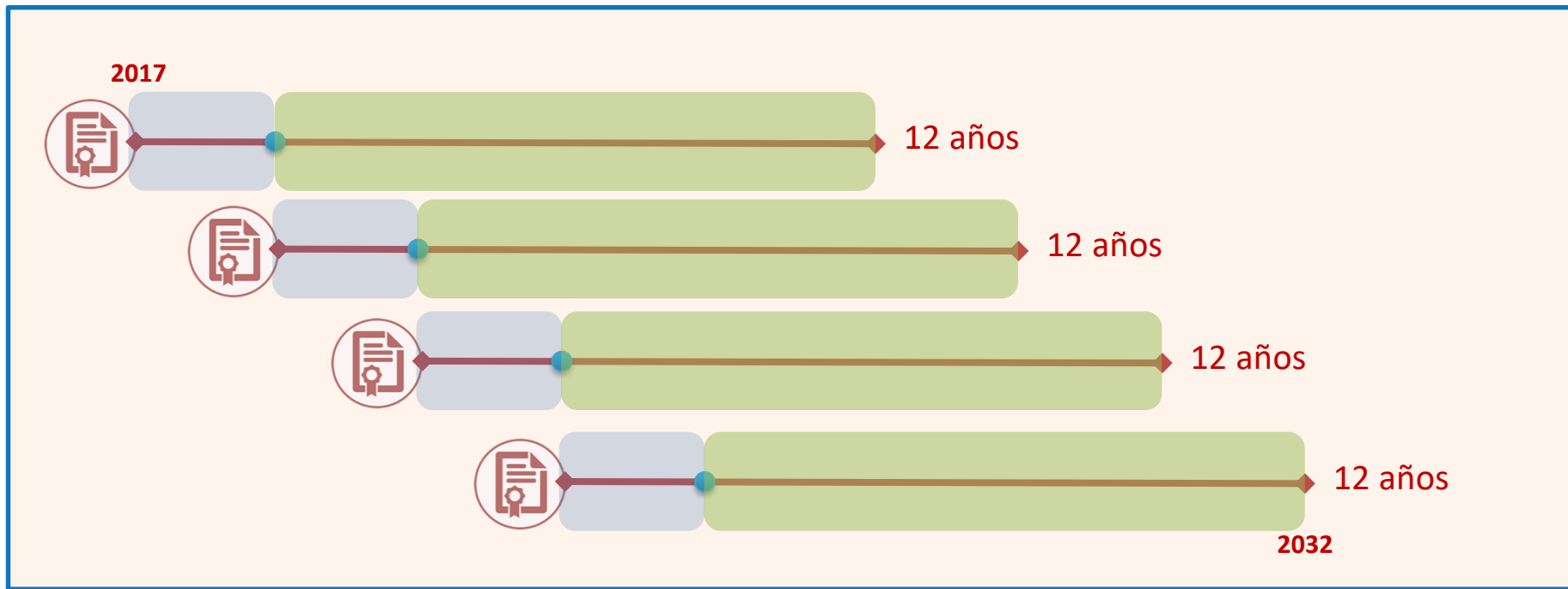
Obtener más información acerca de [certificados](#)

Aceptar

**12 años de validez**



## 4. PSVA-TSA-RENIEC: CICLO DE VIDA DEL CERTIFICADO TSU



■ Periodo de uso de la llave privada: 1 año

■ Periodo mínimo de verificación: 11 años



## 4. CERTIFICADOS TSU

Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Identificador de clave del tit...	62 74 a6 10 ff b1 05 77 ee 39 ...
Uso de la clave	Firma digital, Sin repudio (c0)
Restricciones básicas	Tipo de asunto=Entidad final, ...
Uso mejorado de claves	Impresión de fecha (1.3.6.1.5...
Algoritmo de identificación	sha1
Huella digital	36 6c 47 98 34 04 3b 29 51 2a...

Impresión de fecha (1.3.6.1.5.5.7.3.8)

Editar propiedades... Copiar en archivo...

Más información acerca de los [detalles del certificado](#)

Aceptar

Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Identificador de clave del tit...	29 27 62 21 ef 47 b9 a7 b7 5a...
Uso de la clave	Firma digital, Sin repudio (c0)
Restricciones básicas	Tipo de asunto=Entidad final, ...
Uso mejorado de claves	Impresión de fecha (1.3.6.1.5...
Algoritmo de identificación	sha1
Huella digital	5e 9f ba 8b e2 0e 72 fb ef 97 ...

Impresión de fecha (1.3.6.1.5.5.7.3.8)

Editar propiedades... Copiar en archivo...

Más información acerca de los [detalles del certificado](#)

Aceptar



## 4. PSVA-TSA-RENIEC

<http://tsa.reniec.gob.pe/service/>  
<http://tsa2.reniec.gob.pe/service/>

### PSVA-TSA-RENIEC DE LA JERARQUÍA ECERNEP PERU CA ROOT 3

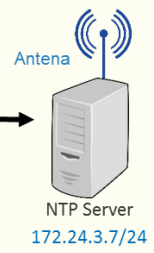
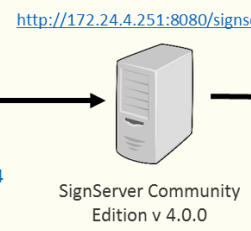
#### Servicios



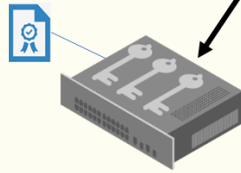
<http://tsa.reniec.gob.pe/service/>  
<http://tsa2.reniec.gob.pe/service/>



#### Sede Jr. Cusco



Certificado Digital TSU



172.24.3.208/24





## 5. USOS DEL SELLO DE TIEMPO

1



❖ Sin firma digital

2



❖ Con firma digital



## 5. USOS DEL SELLO DE TIEMPO

Sin firma digital

Documento de Prueba\_sellado.pdf - Adobe Acrobat Reader DC

Archivo Edición Ver Ventana Ayuda

Inicio Herramientas

Documento de Pru... x



Firmado y todas las firmas son válidas.

Firmas

Validar todas

✓ Rev. 1: Firmado por PSVA-TSA-RENIEC TSU-02

**PSVA-TSA-RENIEC TSU-02**

La firma es una firma de marca de hora de docu

La firma está activada para LTV

> Detalles de la firma

Última comprobación: 2018.06.14 10:34:58 -05'00'

Campo: Signature2 (firma invisible)

[Haga clic para ver esta versión](#)



Documento de Prueba para Sello de tiempo

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."





## 5. USOS DEL SELLO DE TIEMPO

Con firma digital

ReFirma PDF 1.5.2 - [D:\MAPU\TSA\Sensibilización\Documento de Prueba para Sello de tiempo[R].pdf]

Archivo Ver Documento Herramientas Ayuda

159% 1:1 Firmar Validar

Marcadores Buscar Miniaturas Firmas Digitales

- Firmado por ENCINAS ZEVALLOS Maria Pau
  - Fecha y hora: 14/06/2018 11:49:50:000-0500
  - Subfiltro: ETSI.CAdES.detached
  - Algoritmo de firma: SHA256withRSA
  - Lugar: mencinas:Especialista18:172.24.6.18:5
  - Motivo: Soy el autor del documento
- Sello de tiempo (SigTimestamp)**
  - Fecha y hora: 14/06/2018 11:49:57:000-0500
  - Algoritmo de firma: SHA256withRSA
  - Emisor: PSVA-TSA-RENEC TSU-02

**PSVA-TSA-RENEC TSU-02**

FIRMA DIGITAL

Firmado digitalmente por:  
ENCINAS ZEVALLOS Maria Paula FAU 20295613620 hard  
Motivo: Soy el autor del documento  
Fecha: 14/06/2018 11:49:50-0500

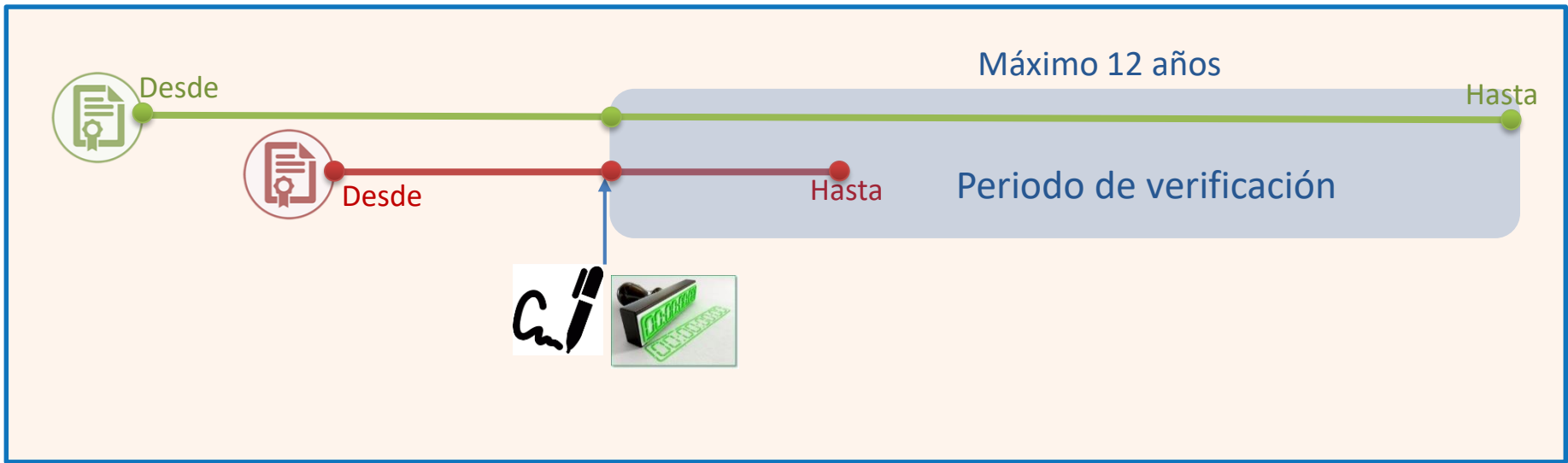
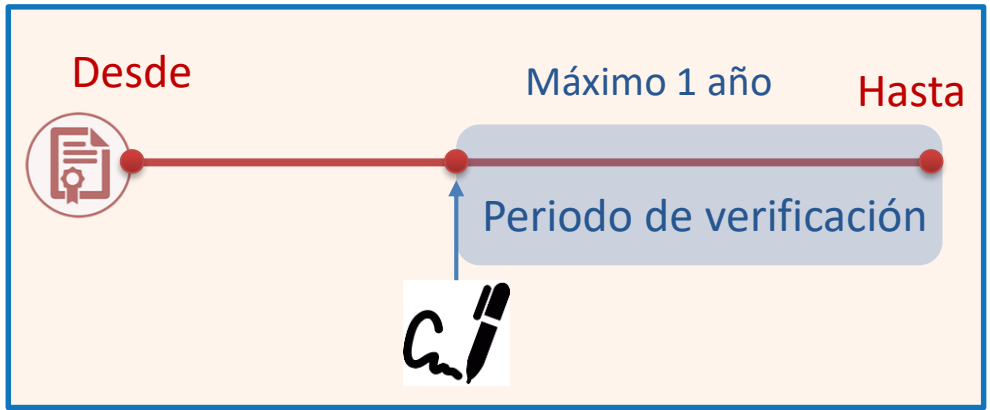
Identidad digital @  
ENTIDAD DE REGISTRO DIGITAL DEL ESTADO PERUANO

Documento de Prueba para Sello de tiempo

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.



## 5. USOS COMUNES





## 5. USOS DEL SELLO DE TIEMPO

Sin firma digital



Resellado periódico



Long-term Validation (LVT)  
→ Validez a largo plazo

Con firma digital



Microformas



Facturas electrónicas



Planillas del personal



Identidad  
*digital* @



# SERVICIO DE SELLADO DE TIEMPO

**PSVA-TSA-RENIEC**

*Gracias*

