



Servicio de Verificación de Datos de la Credencial para Votar

Especificaciones Técnicas

	Instituto Nacional Electoral	
	Dirección de Infraestructura y Tecnología Aplicada	
	Especificaciones Técnicas	


Control de Cambios

SVCV 2.0 FECHA: octubre 2017	Descripción: Especificación Técnica del Servicio de Verificación de Datos 2.0	
Documentó	Revisó	Aprobó
Nombre:	Nombre:	Nombre:
Firma:	Firma:	Firma:

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Contenido

Control de Cambios	2
Contenido	3
1 – Introducción	4
1.1 – Propósito.....	4
2 – Descripción genérica de los Servicios	5
3 – Definición del Servicio	6
3.1 – Servicio de Verificación de Datos.....	6
3.1.1 - Acceso.....	6
3.1.2 - Parámetros	6
3.2 Cifrado de datos	33
3.2.1 Formato JSON.....	33
3.3 Firmado de datos.....	34
3.3.1 Formato JSON.....	34
3.4 Ejemplo de consulta	36
3.4.1 Formato JSON.....	36
3.5 Ejemplo de respuesta	38
3.5.1 Formato JSON.....	38
4 – Generación de certificados para comunicación HTTPS.....	40
5 Anexo.....	41
5.2 Códigos de Respuesta.....	41
5.3 Catálogo de Entidades Federativas.	44
5.4 Resultados de comparación	45


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

1 – Introducción

1.1 – Propósito

El presente documento constituye la descripción técnica de los servicios de verificación de datos de la credencial para votar emitida por el Instituto Nacional Electoral (INE).

La documentación está orientada para proveer de los elementos técnicos necesarios para el consumo de los servicios aquí definidos.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

2– Descripción genérica de los Servicios

El Instituto Nacional Electoral (INE) provee a las instituciones interesadas un servicio web para la consulta y/o verificación de datos de la credencial para votar.

VerifyData.- Permite realizar la verificación de todos los datos contenidos en la credencial para votar, así como las minucias de los ciudadanos.

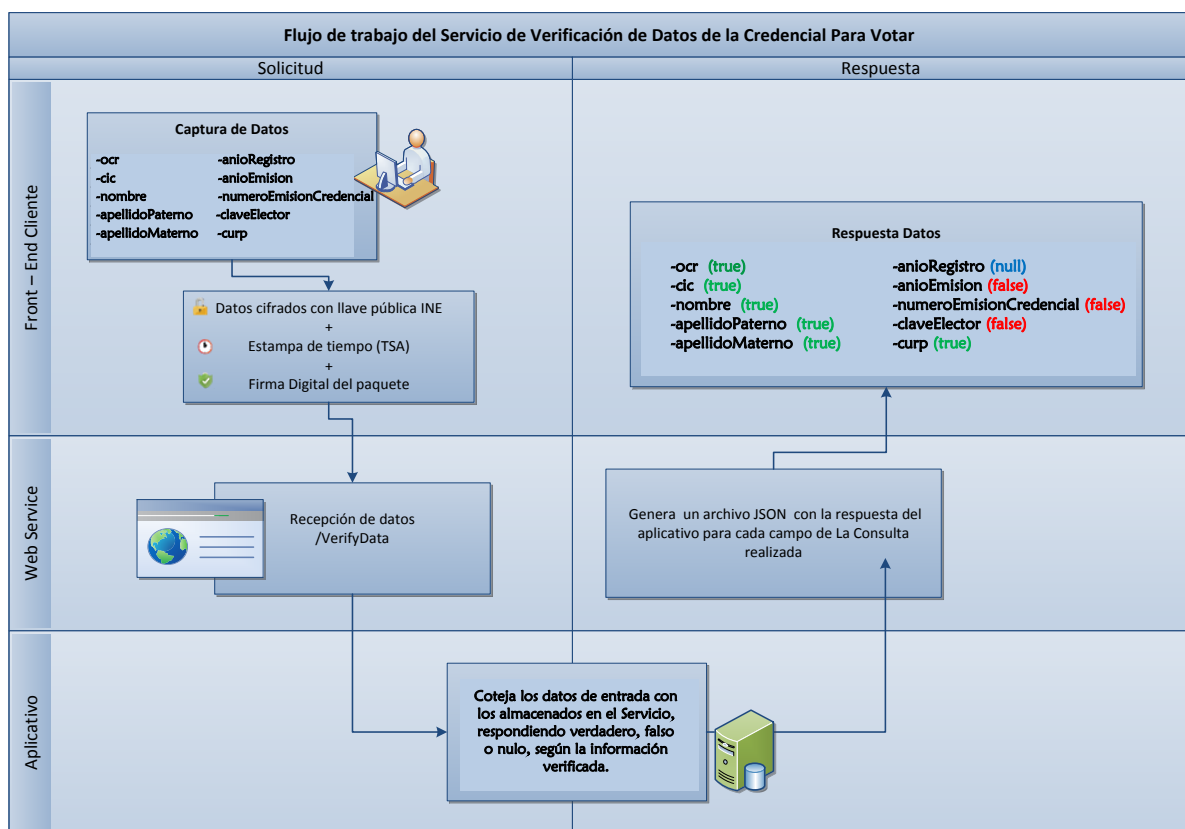



Figura 1 Descripción del Web Service de verificación de datos

Este servicio está disponible mediante solicitudes HTTP empleando el método POST para el envío de los parámetros de consulta. Estos parámetros podrán ser enviados como un documento XML o un documento JSON.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

3 – Definición del Servicio

3.1 – Servicio de Verificación de Datos

El Servicio de Verificación de Datos de la Credencial para Votar versión 2.0 permite realizar una consulta de los datos contenidos en la credencial para votar y las minucias para la verificación, máximo dos por solicitud, del ciudadano.

3.1.1 - Acceso

El acceso para el ambiente de pruebas del Servicio de Verificación de Datos de la Credencial para Votar versión 2.0 se encuentra disponible en la siguiente ruta:

URL
<a href="http://<direccionIP>/cxf/SVD/entidadesExternas/consulta">http://<direccionIP>/cxf/SVD/entidadesExternas/consulta

Tabla 1 URL para acceso al Servicio Web

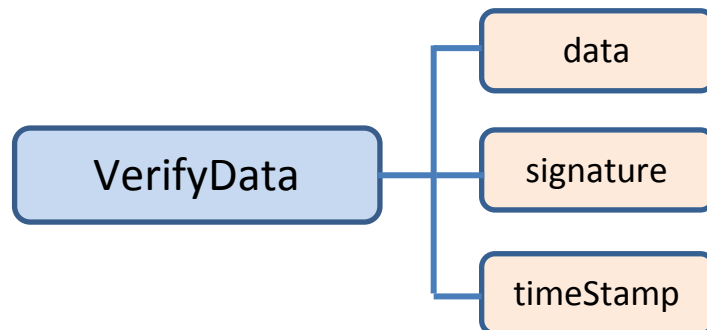
3.1.2 - Parámetros

Los parámetros aceptados por el servicio se componen de dos elementos: headers y cuerpo. Los headers son cabeceras HTTP que describen el tipo consulta enviada y la respuesta deseada:

- Content-Type:
 - application/json
- Accept:
 - application/json


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

El cuerpo es una petición POST con estructura de un documento json, en el que se incluyen los datos de texto y biométricos del ciudadano que se verificarán. La estructura de la petición es la siguiente:



Atributo	Descripción	Uso	Tipo
data	Contiene los datos del ciudadano y los biométricos.	Requerido	Elementos dependientes
signature	Contiene la digestión de la firma, la firma digital de los datos, el número de serie del certificado y parámetros de cálculo de la firma.	Requerido	Elementos dependientes
timeStamp	Contiene la estampa de tiempo empleada por la Institución de los datos y firma digital.	Requerido	Elementos dependientes

Tabla 2 Parámetros para el uso del Web Service para verificación de datos

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Antes de construir la petición (request) al Servicio de Verificación, es importante tener en cuenta lo siguiente:

- a. La llave primaria de búsqueda se realiza por medio del **CIC**; sin embargo, si la credencial para votar no cuenta con CIC, la llave de búsqueda se compone con los siguientes datos **OCR, clave de elector y número de emisión de credencial**
- b. Los datos del ciudadano deben ser enviados en mayúsculas y sin acentos, tal como aparecen en la credencial para votar.
- c. Emplear la codificación UTF-8.
- d. Respetar formato de estructura de JSON (ver pág. 36).

Para los datos cifrados, se deberá cumplir con:

- a. Cifrar los datos con el algoritmo RSA.
- b. Usar la llave pública del INE cuya longitud es de 4096 bits.
- c. El proceso puede realizarse dentro del o los HSM del Módulo de cifrado de información.
- d. El resultado (criptograma) debe estar codificado en base64.

Para la firma digital, se deberá cumplir con:

- a. Realizar la firma digital dentro del o los HSM del Módulo de cifrado de información.
- b. Usar la llave privada de la Institución con longitud de 2048 bits y el algoritmo de firma RSA-SHA256.
- c. El resultado (firma) debe estar codificado en base64.

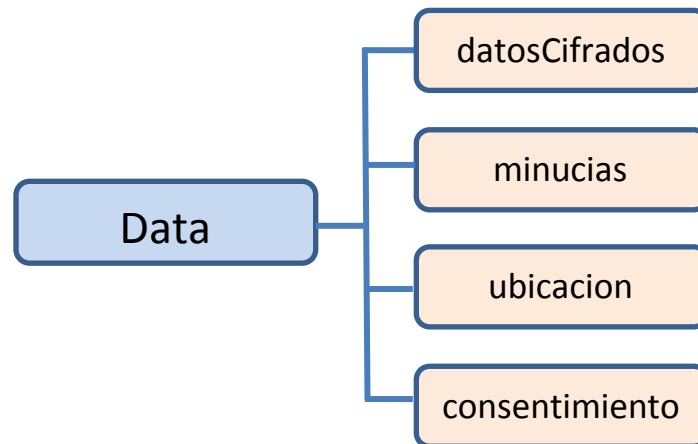
La institución solicitará la estampa de tiempo de todo el paquete que será enviado al INE, la TSA será una dispuesta por la institución o mediante el llenado de los campos requeridos.

A continuación, se especifica cómo construir la solicitud:

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


I. Elemento Data

Descripción: Contiene los datos cifrados del ciudadano y los datos de ubicación de la institución.

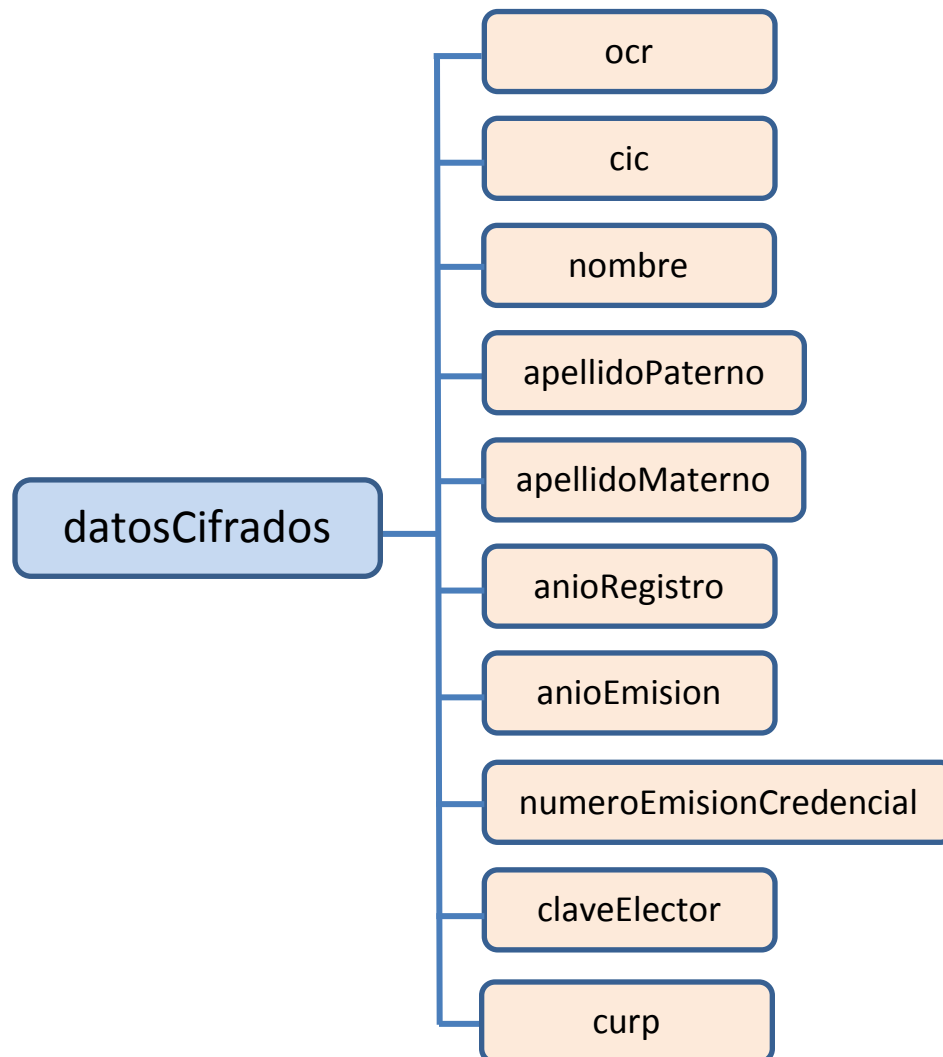


Atributo	Descripción	Uso	Tipo
datosCifrados	Contiene los datos del ciudadano cifrados con la llave pública RSA 4096 del INE.	Requerido	String Base64
minucias	Contiene los biométricos del ciudadano.	Opcional	Elementos dependientes
ubicación	Contiene los datos de la ubicación de la consola que realiza la solicitud.	Requerido	Elementos dependientes
consentimiento	Consentimiento del ciudadano para emplear sus datos en la verificación.	Requerido	Boolean


Tabla 3 Atributos del elemento data

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**datosCifrados**” contiene los datos a verificar del ciudadano, previo a su cifrado, se debe establecer la estructura:



NOTA: El orden de los datos a cifrar es indiferente, siempre y cuando se respete la estructura (ver página 33). En caso de no requerir verificar algún dato se tendrá que declarar como **null**.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

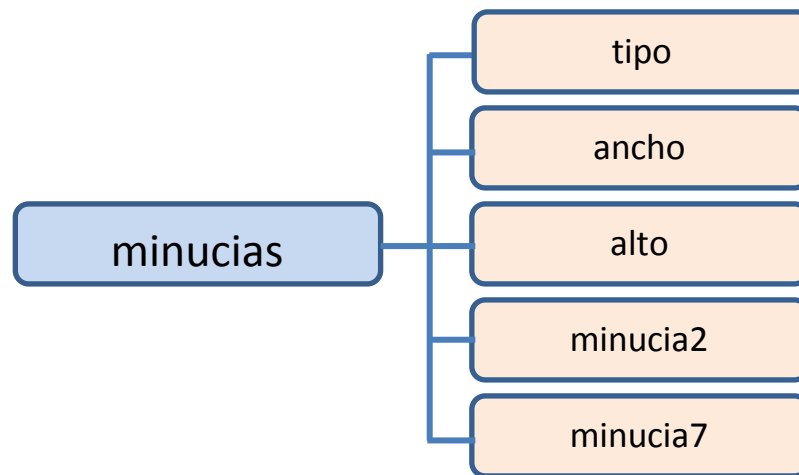
A continuación la descripción de cada dato:

Atributo	Uso	Tipo
ocr	Requerido* <i>*Si la credencial para votar no cuenta con CIC</i>	String Longitud: 13
cic	Requerido	String Longitud: 10
nombre	Opcional	String Longitud: 32
apellidoPaterno	Opcional	String Longitud: 32
apellidoMaterno	Opcional	String Longitud: 32
anioRegistro	Opcional	String Longitud: 4
anioEmision	Opcional	String Longitud: 4
numeroEmisionCredencial	Requerido* <i>*Si la credencial para votar no cuenta con CIC</i>	String Longitud: 2
claveElector	Requerido* <i>*Si la credencial para votar no cuenta con CIC</i>	String Longitud: 18
curp	Opcional	String Longitud: 18

Tabla 4 Atributos Elemento datosCifrados


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**minucias**” contiene los elementos que identifican el tipo y valor de las minucias a ser verificadas, en caso de no contenerlas, definimos el nodo de la siguiente forma “**minucias**”: **null**.

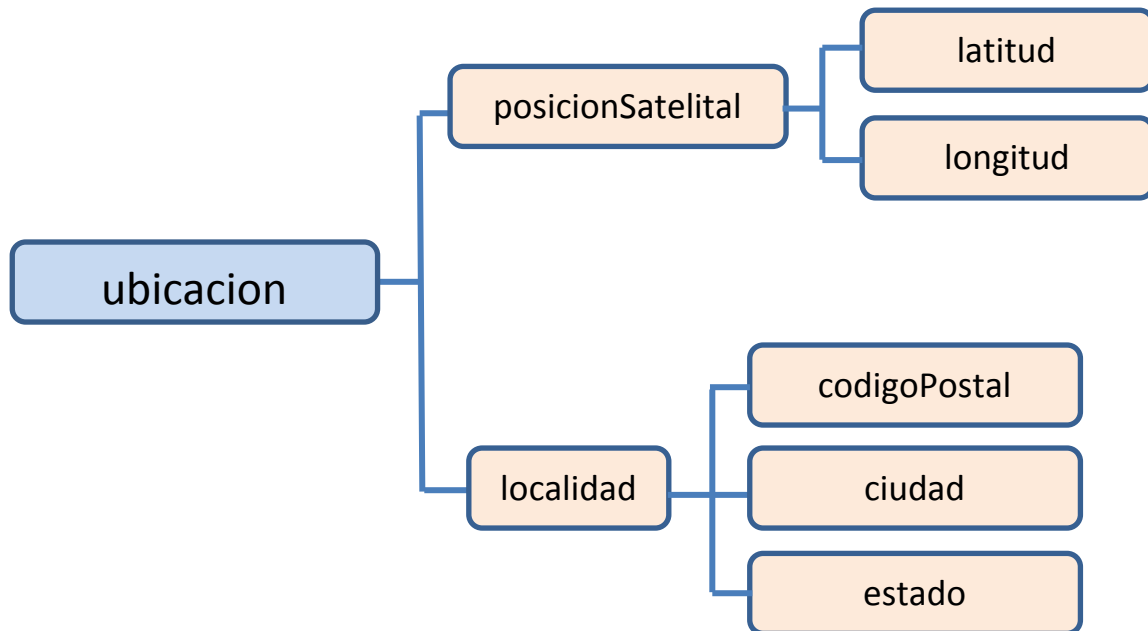


Atributo	Uso	Tipo
tipo	Requerido	Int (1=ansi, 2=wsq, 3=raw)
ancho	Requerido	Int ANSI y WSQ = null
alto	Requerido	Int ANSI y WSQ = null
minucia2	Requerido (al menos una huella)	String Base64 de la huella del índice derecho
minucia7	Requerido (al menos una huella)	String Base64 de la huella del índice izquierdo


Tabla 5 Atributos del elemento minucias

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**ubicación**” contiene los datos de la ubicación de la institución, la posición satelital o la localidad. **Se requiere al menos un atributo del nodo “ubicación”.**



NOTA: En caso de habilitar el atributo “**localidad**”, son requeridos los elementos: “codigoPostal”, “ciudad” y “estado”, en caso contrario establecemos “**localidad**”: **null**.


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Atributo	Descripción	Uso	Tipo
posicionSatelital	Datos de la posición satelital de la consola que realiza la solicitud	Requerido	Elementos dependientes
localidad	Datos de la dirección de la consola que realiza la solicitud	Opcional	Elementos dependientes

Tabla 6 Atributos del elemento ubicación

Atributo	Uso	Tipo
latitud	Requerido	Float Longitud: 8
longitud	Requerido	Float Longitud: 8
codigoPostal	Requerido	String Longitud: 5
ciudad	Requerido	String Longitud: 20
estado	Requerido	Int Longitud: 1 o 2 cifras según el caso (Ver catálogo de entidades federativas, anexo al final)

Tabla 7 Atributos de posicionSatelital y localidad

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**consentimiento**” hace referencia al consentimiento otorgado por el ciudadano para emplear sus datos en la verificación, el valor debe ser “**true**”.



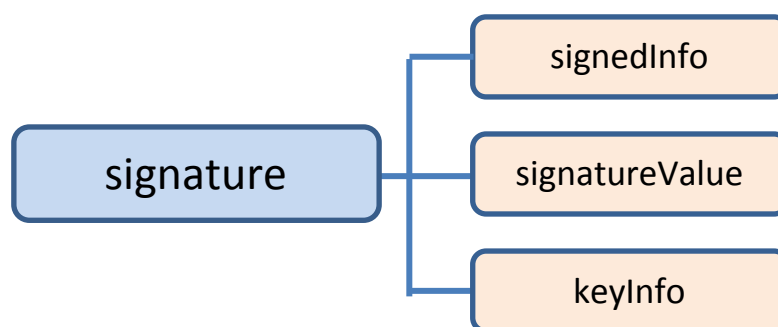
Atributo	Descripción	Uso	Tipo
consentimiento	Consentimiento del ciudadano para emplear sus datos en la verificación.	Requerido	Boolean

Tabla 8 Atributos de posicionSatelital y localidad

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

II. Elemento signature

Descripción: Contiene los elementos de la firma digital XML.

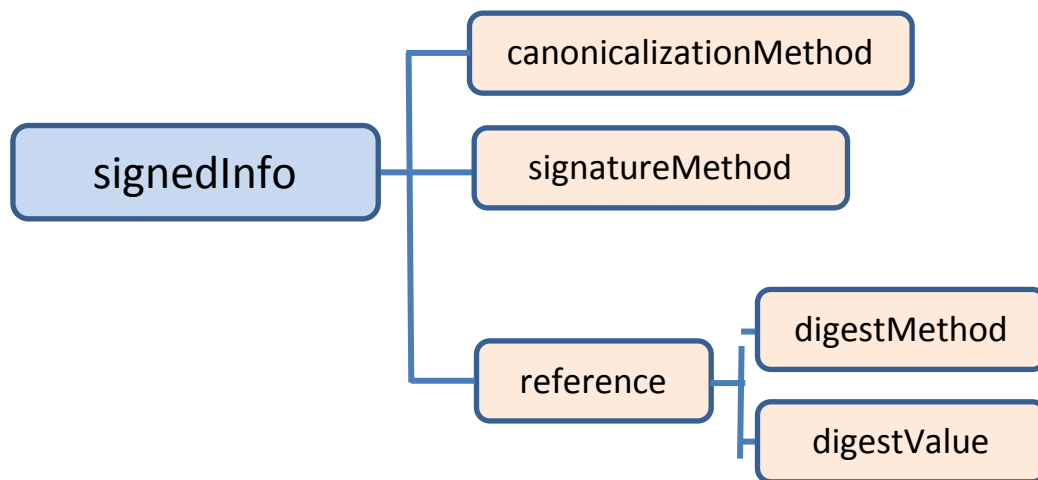


Atributo	Descripción	Uso	Tipo
signedInfo	Contiene los parámetros de cálculo de la firma.	Requerido	Elementos dependientes
signatureValue	Firma digital de la información enviada por la institución.	Requerido	String Base64
keyInfo	Información del certificado con el que se realizó la firma. (El número de serie del certificado es susceptible a mayúsculas y minúsculas, en caso de contener letra).	Requerido	Elementos dependientes

Tabla 9 Atributos del elemento signature

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**signedInfo**” contiene los parámetros de cálculo de la firma.

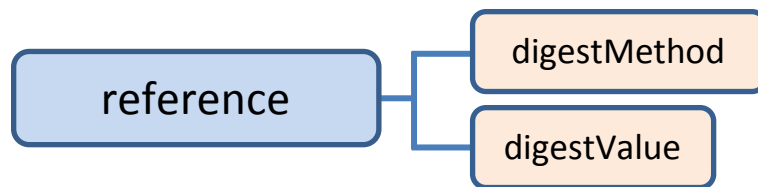


Atributo	Uso	Valor
canonicalizationMethod	Requerido	Por defecto: “ http://www.w3.org/TR/2001/REC-xml-c14n-20010315 ”
signatureMethod	Requerido	Por defecto: “ http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ”
reference	Requerido	Elementos dependientes

Tabla 10 Atributos elemento *signedInfo*


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**reference**” contiene los estándares que se deben cumplir.



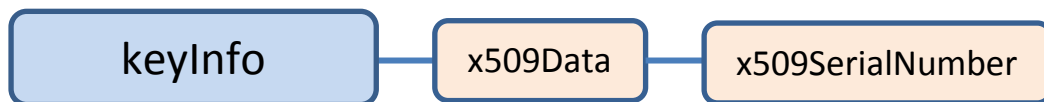
Atributo	Uso	Tipo	Valor
digestMethod	Requerido	Establecido por defecto	Por defecto: “ http://www.w3.org/2001/04/xmlenc#sha256 ”
digestValue	Requerido	Hash SHA-256 de la firma	Elemento dependiente

Tabla 11 Atributos elemento reference

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**keyInfo**”

Descripción: Información del certificado con el que se realizó la firma.




Atributo	Uso	Tipo
x509Data	Requerido	Elementos dependientes

Tabla 12 Atributos elemento *keyInfo*

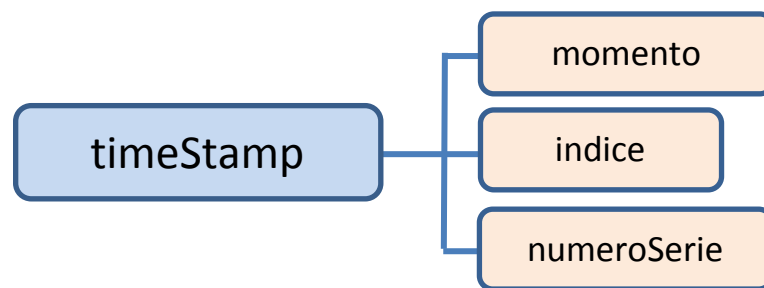
Atributo	Uso	Tipo
x509SerialNumber	Requerido	String Número de serie del certificado emitido por la CA del INE.

Tabla 13 Atributos elemento *x509Data*

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


III. Elemento timeStamp

Contiene la estampa de tiempo empleada por la institución de nodo “data”.



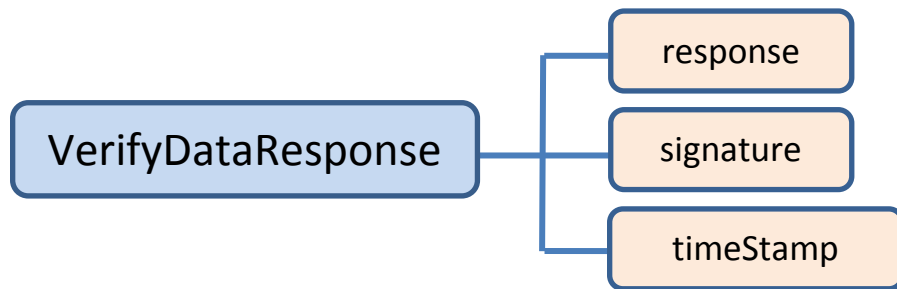
Atributo	Uso	Tipo
momento	Requerido	String Ej. "YYYYMMDDhhmmssZ" Estampa de tiempo en que se generó la solicitud.
Índice	Requerido	String Índice de la estampa de tiempo generada por la institución.
numeroSerie	Opcional	String Número de serie del certificado de la TSA con que fue firmada la estampa de tiempo

Tabla 14 Atributos de elemento timeStamp

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


3.1.3 Respuesta de VerifyData

Al realizar la petición al web service (request) la respuesta tendrá la siguiente estructura:



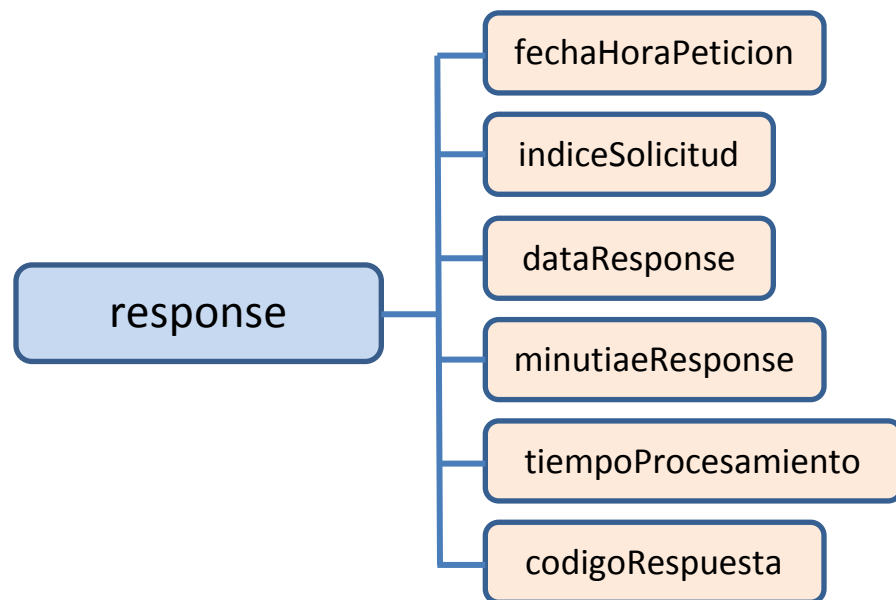
Atributo	Descripción	Tipo
response	Contiene la verificación de los datos del ciudadano, así como códigos de respuesta y folio de la transacción.	Elementos dependientes
signature	Contiene los elementos de la firma digital del INE	Elementos dependientes
timeStamp	Sello de tiempo de la respuesta enviada por el INE	Elementos dependientes


Tabla 15 Atributos elemento VerifyDataResponse

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

I. Elemento response


Contiene la verificación de los datos del ciudadano, así como códigos de respuesta y folio de la transacción.



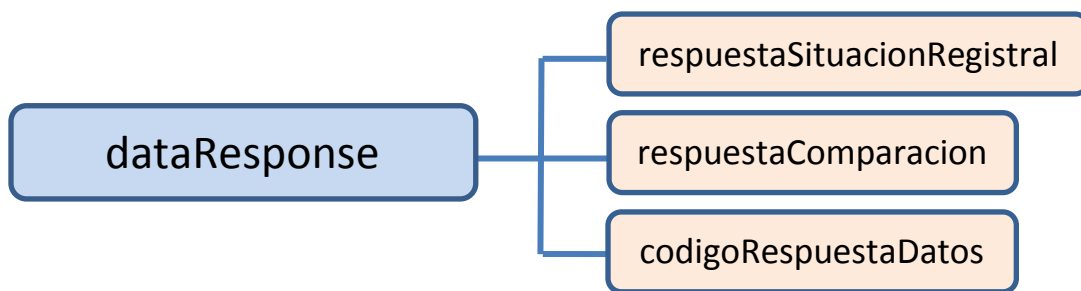
	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Atributo	Descripción	Tipo
fechaHoraPetición	Fecha y hora de llegada de la petición al Servicio de Verificación.	String (YYYY-MM-DD hh:mm:ss.ffffffffff)
indiceSolicitud	Índice enviado por la institución dentro del elemento TimeStamp.	String
dataResponse	Detalle de la respuesta del INE con respecto a los datos del ciudadano enviados a verificar.	Elementos dependientes
minutiaeResponse	Detalle de la respuesta del INE con respecto a las minucias enviadas a verificar.	Elementos dependientes
tiempoProcesamiento	Tiempo en milisegundos de procesamiento de la solicitud de verificación.	Long
codigoRespuesta	Código del estatus de la respuesta.	Int Ver tabla de códigos

Tabla 16 Atributos elemento response


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**dataResponse**” contiene el detalle de la respuesta del INE con respecto a los datos del ciudadano enviados a verificar.

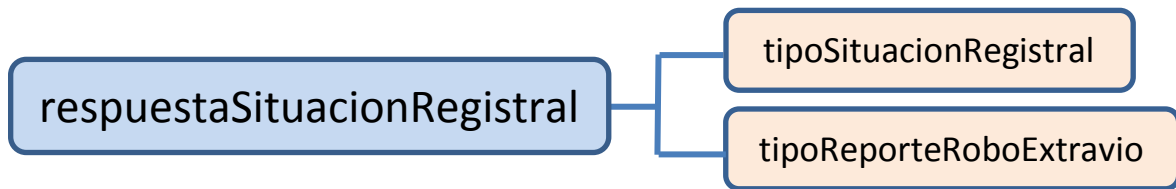


Atributo	Descripción	Tipo
respuestaSituacionRegistral	Muestra el tipo de situación registral del ciudadano	Elementos dependientes
respuestaComparacion	Elemento que contiene el detalle de los elementos enviados a verificar	Elementos dependientes
codigoRespuestaDatos	Código de respuesta de la solicitud enviada	Int Ver tabla de códigos

Tabla 17 Atributos elemento dataResponse

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

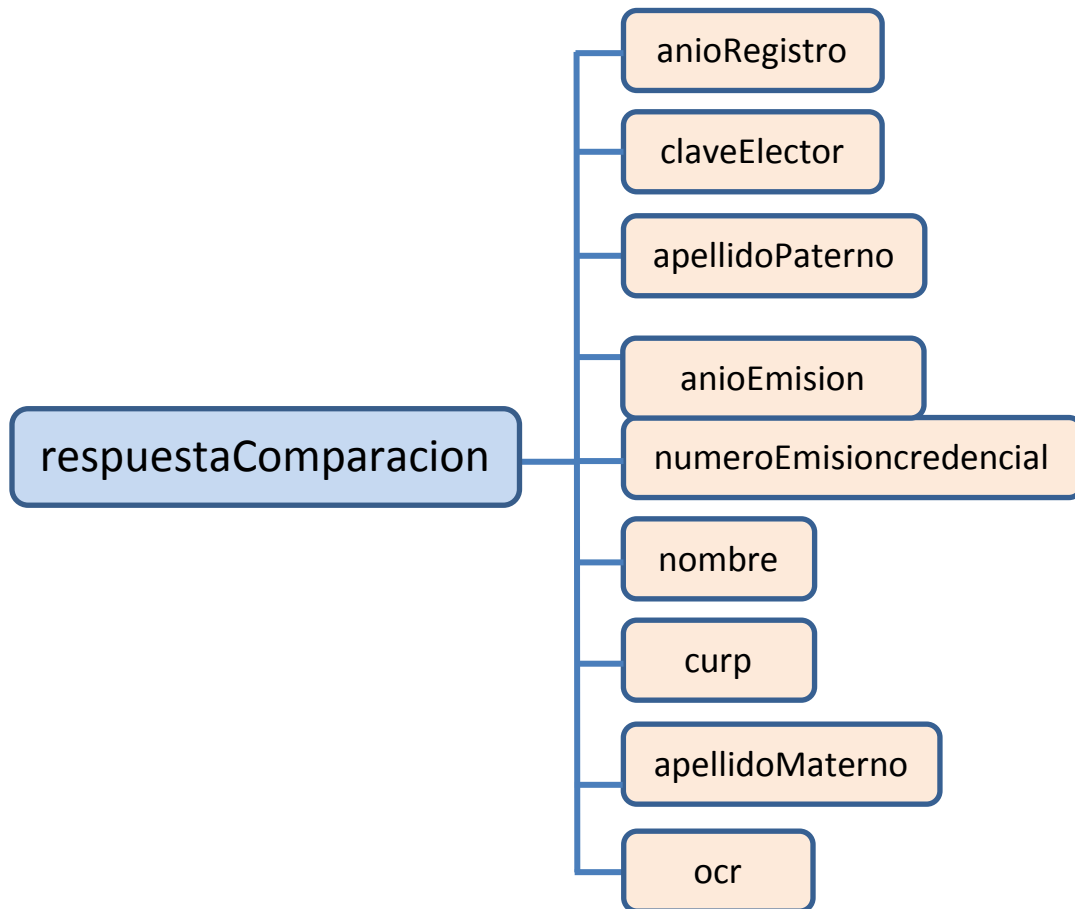
Dentro del elemento “**respuestaSituacionRegistral**” se muestra el tipo de situación registral del ciudadano.



Atributo	Tipo
tipoSituacionRegistral	String (Vigente NoVigente)
tipoReporteRoboExtravio	String

Tabla 18 Atributos elemento respuestaSituacionRegistral

Dentro del elemento “**respuestaComparacion**” contiene el detalle de los elementos enviados a verificar.



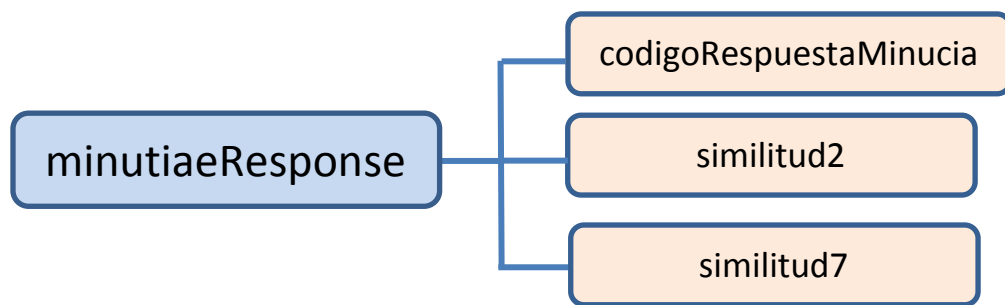
Atributo	Tipo
anioRegistro	Boolean
claveElector	Boolean
apellidoPaterno	Boolean
numeroEmisionCredencial	Boolean
Nombre	Boolean
Curp	Boolean
apellidoMaterno	Boolean
Ocr	Boolean

Tabla 19 Atributos elemento respuestaComparacion

NOTA: Ver anexo de resultados de comparación.


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**minutiaeResponse**” contiene detalle de la respuesta del INE con respecto a las minucias enviadas a verificar.



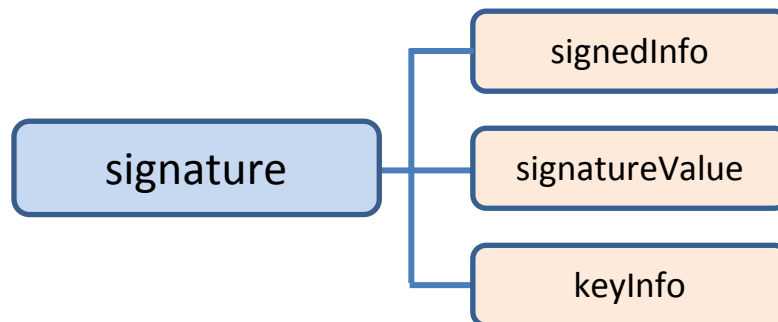
Atributo	Tipo
codigoRespuestaMinucia	Int Ver tabla de códigos
similitud2	String Resultado de la comparación de la huella del índice derecho
similitud7	String Resultado de la comparación de la huella del índice izquierdo

Tabla 20 Atributos del elemento *minutiaeResponse*

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


II. Elemento signature

Contiene los elementos de la firma digital del INE.



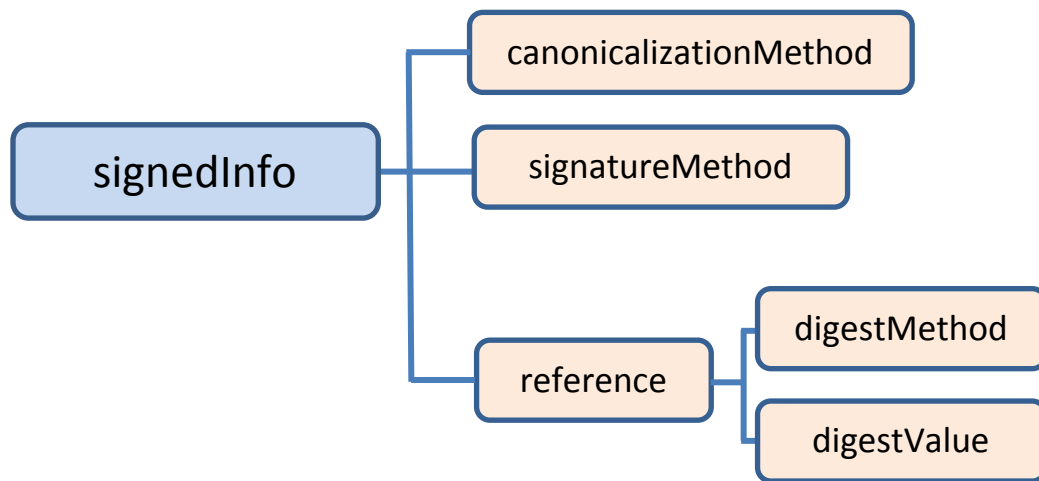
Atributo	Descripción	Tipo
signedInfo	Contiene elementos para el proceso de obtención de la firma	Elementos dependientes
signatureValue	Firma digital de la respuesta emitida por el INE	String Base64
keyInfo	Contiene información del certificado empleado para la firma digital	Elementos dependientes

Tabla 21 Atributos elemento signature

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


Dentro de “**signedInfo**”

Descripción: Contiene elementos para el proceso de obtención de la firma.



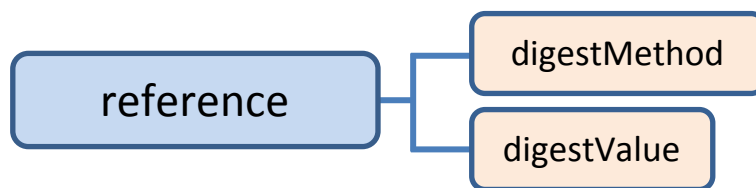
Atributo	Uso	Tipo
canonicalizationMethod	Requerido	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
signatureMethod	Requerido	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Reference	Requerido	Elementos dependientes

Tabla 22 Atributos elemento *signedInfo*

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas


Dentro del elemento “**reference**”

Descripción: Estándares que se deben cumplir.



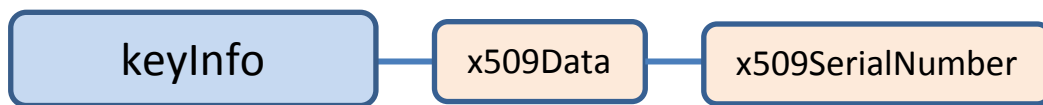
Atributo	Uso	Tipo
digestMethod	Requerido	http://www.w3.org/2001/04/xmlenc#sha256
digestValue	Requerido	String Base64

Tabla 23 Atributos elemento reference

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Dentro del elemento “**keyInfo**”

Descripción: Información del certificado con el que se realizó la firma.




Atributo	Uso	Tipo
x509Data	Requerido	Elementos dependientes

Tabla 24 Atributos elemento keyInfo

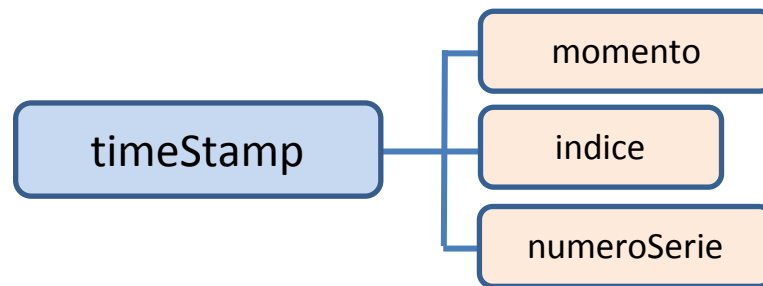
Atributo	Uso	Tipo
x509SerialNumber	Requerido	String Número de serie del certificado emitido por la CA del INE.

Tabla 25 Atributos elemento x509Data

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

III. Elemento timeStamp


Descripción: Sello de tiempo de la respuesta enviada por el INE.



Atributo	Uso	Tipo
Momento	Requerido	String Estampa de tiempo en que se generó la respuesta
Índice	Requerido	String Índice de la estampa de tiempo generada por la TSA de la institución.
numeroSerie	Requerido	String Número de serie del certificado de la TSA de la institución.

Tabla 26 Atributos elemento timeStamp

La estampa de tiempo es calculada con el elemento “response”. Para la respuesta en formato JSON, se calcula el hash del elemento colocándolo en una sola línea.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

3.2 Cifrado de datos

3.2.1 Formato JSON

En formato JSON, los datos que se cifrarán tendrán la siguiente forma:

```
{
  "ocr": "0720060838243",
  "cic": "80040529",
  "nombre": "VALERIA",
  "apellidoPaterno": "LEPE",
  "apellidoMaterno": "JARDINES",
  "anioRegistro": "2010",
  "anioEmision": "2014",
  "numeroEmisionCredencial": "04",
  "claveElector": "LPJRVL88110101H100",
  "curp": "LEJv881101HASJSN07"
}
```


Se creará una sola línea con los datos contenidos por “datosCifrados”.

```
{ "ocr": "0720060838243", "cic": "80040529", "nombre": "VALERIA", "apellidoPaterno": "LEPE", "apellidoMaterno": "JARDINES", "anioRegistro": "2010", "anioEmision": "2014", "numeroEmisionCredencial": "04", "claveElector": "LPJRVL88110101H100", "curp": "LEJv881101HASJSN07" }
```

La cadena será cifrada con la **llave pública RSA 4096 del INE**, utilizando el tipo de **padding OAEP**.

El resultado será colocado como valor de la misma etiqueta:

```
"datosCifrados": "J/tJEzVeD1R6A1s8nCKsB8iRia2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrN
POzG/sooJP35Kc1B72K97P/MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB/emOCGQgsEQ54UG+VC7Vacaq4XqBZI+8eMs/tQSis
9RHtCVcRSickZj+n117vjNNeSNWJ+IkxMzhIEJxUiuv16l6UcP0E6i4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkA
zNVCQktUvxRaNYgOICYutbVIG4Xtvmrvt8ffl1ofAatCCEh57Soz9lA8BjLb/qPduVJke+cHbsROV4fqXJeSKFYBnizFOwFhM
pJ4Pwk6NcTwhwk2MRj/+L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO+etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqp
XwQxKNzycTvoCaRTezf7RusuVK8RR1mNHdw44xUUISz/OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z/UIKd
ocBafT3X/mhF944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB+JhBrMrh
wGbWAp2UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD/qFdkVXS9/4=",
```


	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

3.3 Firmado de datos

3.3.1 Formato JSON

En formato JSON, los datos que se firmarán tendrán la siguiente forma:


```
{
  "datosCifrados":
    "J/JEzVeD1R6A1s8nCKsB8iRla2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrNPOzG/sooJP35K
    c1B72K97P/MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB/emOCGQgsEQ54UG+VC7Vacaq4XqBZI+8eMs/tQSis9RHtCVcRSick
    Zj+n1I7vjNNEsNWJ+IkxMzhIEJxUiuiV16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkAzNVCQktUvxR
    aNYgOICYutbVIG4Xtvmrvt8fff1ofAatCEh57Soz9IA8BjLb/qPduVJke+cHbsROV4fqXJeSKFYBnizFOWFhMjP4Pwk6NcTw
    hwk2MRj/+L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO+etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqpXwQxKNzycT
    voCaRTezf7RusuVK8RR1mNHdw44xUUISz/OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z/UIKdocBafT3X/mh
    F944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB+JhBrMrhwGbWAp2
    UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD/qFdkVXS9/4=",
  "minucias": {
    "tipo": 1,
    "ancho": null,
    "alto": null,
    "minucia2":
      "Rk1SACAyMAAAwGAAAAAAAAAGgAaAAxQDFAQAAAFabgKAAQG4AgNoAVWMAgOEAdHQAgoMAhpYAgKkArJ
      MAgRAAUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUAQM8A
      Z3MAQJEAeXsAQN4A874f4gAQRMArz4AQSSAujkAQIYAyJYAQR4A2E8AQPsa3K0AQJcBC0QAQK4BC0QAQG4BDU
      sAQPMBHIQAQK0BOU4AAAA=",
    "minucia7":
      "Rk1SACAyMAAA/gAAAAAAAAAGgAaAAxQDFAQAAAGQlQsAXJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKU
      ApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAvZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKY
      BB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAgMABTwcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQG
      QAI30AQLYAjngAQNsAmYoAQG0AnIgAQs0A4osAQOkA5XMAQT0A85YAQTYBAn8AQRcBFHUAQQEBOhoAQOkB
      WwwwAAAA=",
  },
  "ubicacion": {
    "posicionSatelital": {
      "latitud": 19.12345,
      "longitud": -99.12345
    },
    "localidad": {
      "codigoPostal": "01710",
      "ciudad": "CDMX",
      "estado": 9
    }
  },
  "consentimiento": true
}{
  "momento": "20170622130012Z",
  "indice": "6545665423523153",
  "numeroSerie": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c"
}
```

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

Se creará una sola línea con los datos contenidos por “data” y “timeStamp”, de las cuales se obtendrá el SHA256 (“digestValue”) y firmada con la llave privada RSA 2048 de la institución. El resultado será colocado como valor de la misma etiqueta:

```
{ "datosCifrados": "J/tJEzVeD1R6A1s8nCKsB8iRla2gWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVr
NPOzG/sooJP35Kc1B72K97P/MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB/emOCGQgsEQ54UG+VC7Vacaq4XqBZI+8eMs/tQS
is9RHtCVcRSickZj+n1l7vjNNeSNWJ+IkxMzhIEJxUiuv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrk
AzNVCQktUvxRaNYgOICYutbVIG4Xtvmrvt8fff1ofAatCCEh57Soz9lA8BjLb/qPduVJke+cHbsROV4fqXJeSKFYBnizFOWFh
MpJ4Pwk6NcTwhwk2MRj/+L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO+etnWq8dsWzqifn4AdKdCJGQ4u4FrBvm
qpXwQxKNzycTvoCaRTezf7RusuVK8RR1mNHdw44xUUISz/OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqjFkw17Z/UI
KdocBafT3X/mhF944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB+JhBr
MrhwGbWAp2UpNKwByyIqRGqb1NHHlf7HwtCiVOvKD/qFdkVXS9/4=", "minucias": { "tipo": 1, "ancho": null, "alto": null, "mi
nucia2": "Rk1SACAyMAAAwgAAAAAAAAAGgAaAAxQDFAQAAAFabgKAAQG4AgNoAVWMAgOEAdHQAqOMAhpYA
gKkArJMAgRAAuUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUA
QM8AZ3MAQJEAeXsAQN4A874f4gAQRMArz4AQSSaujKAQIYAyJYAQR4A2E8AQPsa3K0AQJcBC0QAQK4BC0QAQG
4BDUsAQPMBHIAQK0BOU4AAAA=", "minucia7": "Rk1SACAyMAAA/gAAAAAAAAAGgAaAAxQDFAQAAAGQlgQsA
XJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKUApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAv
ZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKYBB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAGMABT
wcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQGQAI30AQLYAjngAQNsAmYoAQG0AnIgAQs0A4osAQOkA5XMA
QT0A85YAQTYBAn8AQRCBFHUAQQEBOhoAQOkBWwwAAAA=", "ubicacion": { "posicionSatelital": { "latitud": 19.12345, "
longitud": -
99.12345 }, "localidad": { "codigoPostal": "01710", "ciudad": "CDMX", "estado": "9" }, "consentimiento": true, { "momento": "20170622
130012Z", "indice": "6545665423523153", "numeroSerie": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c" }
```

NOTA: Atención de no tener un salto de línea al final de la cadena y/o algún carácter sobrante que genere una alteración de la firma y resulte un error al consumir el servicio web.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

3.4 Ejemplo de consulta

3.4.1 Formato JSON


```
{
  "data": {
    "datosCifrados":
    "J/tJEzVeD1R6A1s8nCKsB8iRIa2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrNPOzG/sooJP35K
c1B72K97P/MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB/emOCGQgsEQ54UG+VC7Vacq4XqBZI+8eMs/tQSi9RHtCVcRSick
Zj+n117vjNNeSNWJ+IkxMzhIEJxUiuv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkAzNVCQktUvxR
aNYgOICyutbVIG4Xtvmrvt8fff1ofAatCCEh57Soz9IA8BjLb/qPduVJke+cHbsROV4fqXJeSKFYBnizFOwFhMpJ4Pwk6NcTw
hwk2MRj/+L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO+etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqpXwQxKNzycT
voCaRTezf7RusuVK8RR1mNHdw44xUUIsz/OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z/UIKdocBafT3X/mh
F944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB+JhBrMrhwGbWwAyP2
UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD/qFdkVXS9/4=",
    "minucias": {
      "tipo": 1,
      "ancho": null,
      "alto": null,
      "minucia2":
      "Rk1SACAyMAAAwgAAAAAAGgAaAAxQDFAQAAAFAbgKAAQG4AgNoAVWMAgOEAdHQAgoMAhpYAgKkArJ
MAgRAAAuUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUAQM8A
Z3MAQJEAeXsAQN4A874f4gAQRMArz4AQSSAujkAQIYAjYAQR4A2E8AQPsa3K0AQJcBC0QAQK4BC0QAQG4BDU
sAQPMBHIAQK0BOU4AAAA=",
      "minucia7":
      "Rk1SACAyMAAA/gAAAAAAGgAaAAxQDFAQAAAGQlqQsAXJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKU
ApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAvZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKY
BB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAGMABTwcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQG
QAi30AQLYAjngAQNsAmYoAQG0AnIgAQs0A4osAQOkA5XMAQT0A85YAQTYBAn8AQRcBFHUAQQEBOhoAQOkB
WwwAAAA=",
    },
    "ubicacion": {
      "posicionSatelital": {
        "latitud": 19.12345,
        "longitud": -99.12345
      },
      "localidad": {
        "codigoPostal": "01710",
        "ciudad": "CDMX",
        "estado": 9
      }
    },
    "consentimiento": true
  },
  "signature": {
    "signedInfo": {
      "canonicalizationMethod": {
        "algorithm": "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
      },
      "signatureMethod": {
        "algorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
      },
      "reference": {
        "digestMethod": {
          "algorithm": "http://www.w3.org/2001/04/xmllenc#sha256"
        }
      }
    }
  }
}
```

```

    "digestValue": "DE1F6A8933C7A6955F2E518AA15A37E6E11605CC9765E2B062EA2D762BA65AB6",
    "uri": "#DATA"
  }
},
"signatureValue":
"ZJS+pk3D2EvJ6iWE4LluLUJRQZSGJmL0SZ1zW1DtxCLAFJT54lmdJrirC0DTcH/vjYU9pkrGvWDOEdDTc8BqncwC/A68
wZu/VJdiOF/CWaEtDAIcGj0fF7KlaiezzKGHgkOlyLqxsSdbCbpUhUz12BF1VATdU7T2JZji8mTmGg0qJr+Ol7qdjPBLw/pe1
WgleZstczw2bQjhw+FRWCmlObONhJSaoFN6ojvtYpvk4UmuLyeqlozeAQAbOsKnymIPbsNx3toTHSSjA5RR3gyWwdsKB2v
CwC7T5wesYaBR/x9nqbIs6GqkI3bLPQvAQOjzllXyp8QtP+B3k5s5PXz7wNVLw==",
"keyInfo": {
  "x509Data": {
    "x509SerialNumber": "4m"
  }
},
"timestamp": {
  "momento": "20170622130012Z",
  "indice": "6545665423523153",
  "numeroSerie": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c "
}
}

```

NOTA: Los atributos “canonicalizationMethod”, “signatureMethod”, “reference” y “digestMethod” se incluyen en la petición JSON para conservar compatibilidad con XML.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

3.5 Ejemplo de respuesta


3.5.1 Formato JSON

```
{
  "response": {
    "fechaHoraPetición": "2017-07-12 16:47:19.947",
    "indiceSolicitud": "6545665423523153",
    "dataResponse": {
      "respuestaSituacionRegistral": {
        "tipoSituacionRegistral": "VIGENTE",
        "tipoReporteRoboExtravío": null
      },
      "respuestaComparacion": {
        "anioRegistro": true,
        "claveElector": true,
        "apellidoPaterno": true,
        "anioEmisión": true,
        "numeroEmisiónCredencial": true,
        "nombre": true,
        "curp": true,
        "apellidoMaterno": true,
        "ocr": true
      },
      "codigoRespuestaDatos": 0
    },
    "minutiaeResponse": {
      "codigoRespuestaMinucia": 0,
      "similitud2": "100.0%",
      "similitud7": "100.0%"
    },
    "tiempoProcesamiento": 506,
    "codigoRespuesta": 0
  },
  "signature": {
    "signedInfo": {
      "canonicalizationMethod": { "algorithm": "http://www.w3.org/TR/2001/REC-xml-c14n-20010315" },
      "signatureMethod": { "algorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" },
      "reference": {
        "digestMethod": { "algorithm": "http://www.w3.org/2001/04/xmldsig-more#sha256" },
        "digestValue": "7xvDnM22K4jupFHUdNFEVW7dolq/Nu6IRDFhNm+u2KE=",
        "uri": "#DATA"
      }
    },
    "signatureValue":
    "SFJkbhjhoASDQ/9b22SKxLBC7ENRgVHIjnp8GqFvKz3n2TMtebLThjQQ8hNqpcat73TT2e/B0x\\nMRPAsGLHmbCKJ6tAz
    +W7ipj/FkLLEoU4Wka3GHvtXRRTKbNVDpgNRbeeDiedupmKzGHyoF+EpkXwAyD\\npQt3pv3ntEqE4FQhB6nEU3QdfBOv
    uBMZmG72LwqNXojGILcd35igggdiSpmij0QrKeTeo8onFzFp1NG\\nrgTH6UcCiYPM61ehwNZh478pm6q75U8N7vIAVwcE
    l+YSSwMg04i9NJ3ZSjojRS3mvDmLtiophNHc\\n2jSMU1Um1ulH2YjEhPPZHwJ+rMpnamsIURliOxeCasQIVwV9ljeFJq7Acq
    6YodkWAaPLF5W3V5vW\\n8tez0t22euiRTftPW8KWrbhgqEi2rUZ4RFUvpLN4Y2Puzv6R2IbNbcSnZMVb3fmNh1Md6nbE7
    N7Dn7NAsgqXdAkWDCpiYUW3HGMXYeLikcwfmuu+ugObooz1wpn3X1JEAXv+LR2YiJBBC5Ne4QJwYSHf8\\nQRtPKL
    RexWTNdVsOaH51DUiDm5cQDh7Bp/o/txVqnw8nMs5Y38dhuyQKaj7ytax9mKDWAmoxmVW\\nVUCFP7biugxw4Q5ZyWt
    ZLqpjBDVNdCrUnWvt/8ke3n0eIDgEYiRFB09bJ1UVGeVKSihCrt/ZK1A=",
    "keyInfo": { "x509Data": { "x509SerialNumber": "SERIALNumber" } }
  }
}
```

},

```
"timestamp": {  
  "momento": "20170712214756.161Z",  
  "indice": "2f0000000020170512000000000000000000000000097739141481428",  
  "numeroSerie": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c"  
}  
}
```

NOTA: Los atributos “canonicalizationMethod”, “signatureMethod”, “reference” y “digestMethod” se incluyen en la respuesta JSON para conservar compatibilidad con XML.

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

4 – Generación de certificados para comunicación HTTPS

La transferencia de información entre la Institución y el INE se realiza mediante el protocolo HTTP y TLS de dos vías. Para llevarlo a cabo, es necesario que la Institución genere por cada uno de sus servidores (empleados para tal fin) un certificado x509, que será enviado al INE para su firma por parte de la Autoridad Certificadora (CA) establecida.

El proceso de generación puede variar, sin embargo se considera obligatorio:


- La llave privada debe ser RSA 2048
- Nombre de país (código 2 letras): MX
- Estado o provincia (nombre completo): Estado de la Institución
- Localidad (ciudad): Ciudad de la Institución
- Nombre de la organización: Nombre de la Institución
- Nombre común (FQDN): nombre-del-servidor.dominio-institucion
- Correo electrónico: correo del responsable del certificado

Estos datos se emplean para generar el Certificate Signing Request (.csr) que será enviado a la CA del INE; éste regresará el certificado firmado y, opcionalmente, una copia del certificado raíz de la CA (ambos en formato .cer), mismo que deberá ser usado para confirmar la identidad del servidor del INE. El certificado firmado tendrá una vigencia de 3 años.

El certificado firmado por la CA del INE también será empleado para autenticar al servidor.

El procedimiento se explica a detalle en el documento *Estándar del Servicio de Certificación DERFE*, incluido dentro del *paquete técnico de certificación*.

NOTA: Por parte del INE se envía el paquete técnico de certificación. Los formatos de solicitud serán enviados al correo **ssi.derfe@ine.mx**

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

5 Anexo

5.2 Códigos de Respuesta.


La descripción del catálogo de códigos de respuesta para los servicios es:

Código	Descripción	Servicio
0	OK	Central
100	Licencia no vigente.	Central
101	Licencia no encontrada.	Central
102	Error inesperado en la validación de licencia.	Central
103	Sin aviso de privacidad.	Central
104	Error de comunicación con el servicio de biométricos.	Central
105	Error de comunicación con el servicio consulta datos.	Central
106	Error en parámetros de entrada para biométricos.	Central
107	Error inesperado en el servicio de consulta externa.	Central
108	Error al realizar la petición del servicio de biométricos.	Central
109	Error al realizar la petición del servicio de datos.	Central
110	Parámetros no válidos.	Central
111	Error al descifrar los datos	Central
112	Error al verificar la firma.	Central
113	Firma inválida.	Central
114	Error al convertir los datos cifrados.	Central
115	Error al firmar la respuesta.	Central
116	Error inesperado al guardar la bitácora	Central
117	error inesperado al obtener la estampa de tiempo	Central

		Instituto Nacional Electoral
		Dirección de Infraestructura y Tecnología Aplicada
		Especificaciones Técnicas
200	Error en la búsqueda del ciudadano.	Datos
201	Error inesperado en la consulta del ciudadano.	Datos
202	Parámetros erróneos de entrada en la búsqueda del ciudadano.	Datos
205	Parámetros incompletos de entrada de búsqueda del ciudadano	Datos
300	Error inesperado en el servicio de biométricos.	Biométricos
301	No se encontraron archivos de huellas en el sistema.	Biométricos
302	Imagen de huella candidata no válida.	Biométricos
303	El formato de imagen que enviaron como muestra no es soportado.	Biométricos
304	Error al comparar las imágenes.	Biométricos
305	El formato de imagen que se solicita para file system no es soportado.	Biométricos
306	La petición es inválida para biométricos.	Biométricos
307	El id de la transacción es inválido o nulo.	Biométricos
308	El id del ciudadano es inválido o nulo.	Biométricos
309	El tipo de imagen no fue indicado.	Biométricos
310	Los parámetros de altura y longitud son requeridos.	Biométricos
311	La petición contiene más/menos huellas de las posibles.	Biométricos
312	El tipo de imagen es incorrecto.	Biométricos


	Instituto Nacional Electoral	
	Dirección de Infraestructura y Tecnología Aplicada	
	Especificaciones Técnicas	
313	Demasiados archivos abiertos.	Biométricos
314	La imagen tiene baja calidad o no es una huella.	Biométricos
315	La imagen tiene baja calidad, muy pocas minucias identificables.	Biométricos
316	La imagen tiene una resolución incorrecta.	Biométricos
317	Las librerías están desactivadas.	Biométricos
318	Las librerías no están cargadas correctamente.	Biométricos
320	Error al convertir la imagen	Biométricos
321	El formato de imagen que enviaron para convertir no está soportada	Biométricos
322	No hay Imágenes en la petición de conversión.	Biométricos
323	Formato de argumento invalido	Biométricos

Tabla 27 Descripción de los códigos de respuesta obtenidos del Servicio de Verificación

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

5.3 Catálogo de Entidades Federativas.

Código estandarizado	Entidad Federativa
1	AGUASCALIENTES
2	BAJA CALIFORNIA
3	BAJA CALIFORNIA SUR
4	CAMPECHE
5	COAHUILA
6	COLIMA
7	CHIAPAS
8	CHIHUAHUA
9	CIUDAD DE MEXICO
10	DURANGO
11	GUANAJUATO
12	GUERRERO
13	HIDALGO
14	JALISCO
15	MEXICO
16	MICHOACAN
17	MORELOS
18	NAYARIT
19	NUEVO LEON
20	OAXACA
21	PUEBLA
22	QUERETARO
23	QUINTANA ROO
24	SAN LUIS POTOSI
25	SINALOA
26	SONORA
27	TABASCO
28	TAMAULIPAS
29	TLAXCALA
30	VERACRUZ
31	YUCATAN
32	ZACATECAS

	Instituto Nacional Electoral
	Dirección de Infraestructura y Tecnología Aplicada
	Especificaciones Técnicas

5.4 Resultados de comparación

Los datos del ciudadano enviados al servicio de verificación pueden presentar los siguientes casos.

1. Si el dato a verificar se manda como null, en el response será null.
2. Si el dato a verificar se manda vacío, la respuesta podrá ser false o true dependiendo de lo que se tenga en base de datos; ejemplo:

“apellidoMaterno”: “”, o “apellidoPaterno”:””,

Exclusivamente se presenta en los datos del apellido paterno o apellido materno.

3. Para el punto anterior, es altamente recomendable, en caso de que el ciudadano no cuente con algún apellido mandar el dato en null.
4. Si algún dato a verificar no coincide con lo que se tenga en la base de datos el response será false.
5. Las llaves de búsqueda son:
 - 5.1. CIC.
 - 5.2. OCR, Clave de elector y Número de emisión de Credencial.