BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

ESTÁNDAR ELECTRÓNICO

# FIRMADOR VALIDADOR Y AUTENTICADOR

## SERIE DE NORMAS Y PROCEDIMIENTOS

**Público**

sinpe

# EE-FVA

BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

**E S T Á N D A R  E L E C T R Ó N I C O**

# F I R M A D O R  V A L I D A D O R  Y  A U T E N T I C A D O R

**SERIE DE NORMAS Y PROCEDIMIENTOS**

# Público

sinpe

# EE-FVA

# Tabla de contenido

# Sistema Nacional de Pagos Electrónicos



## 1. Introducción

El contenido de este libro describe el estándar electrónico para el procesamiento de operaciones del servicio Firmador, Validador y Autenticador, provisto por el Banco Central de Costa Rica, por medio del Sistema Nacional de Pagos Electrónicos y Central Directo. El documento se enfoca principalmente en la modalidad de procesamiento de operaciones en tiempo real.

En el caso del servicio Firmador, Validador y Autenticador, el procesamiento de solicitudes en tiempo real se realiza mediante una interacción entre los servidores de la infraestructura del BCCR y de los servidores en las entidades, de forma que no existe un proceso manual para la aplicación de estas.

Para lograr esta comunicación se detalla la tecnología a utilizar para implementar la capa de software encargada de recibir los datos de las solicitudes y el tipo de datos que se transportan en la comunicación entre servidores.

En particular, el objetivo de este documento es permitir a los departamentos de informática de cada entidad verificar el estado de sus sistemas internos e identificar los ajustes necesarios para evitar contratiempos en la participación de la entidad en el servicio.

## 2. Alcance

Este documento explica los elementos técnicos para que una entidad pueda consumir los servicios web de persona física que provee el BCCR para el servicio Firmador BCCR.

Adicionalmente, se explican elementos técnicos requeridos para consumir los servicios web que se proveen para el servicio Firmador BCCR, se definen las interfaces, tipos de datos y de mensajes que se pueden intercambiar entre el BCCR y los sistemas de las entidades para un procesamiento en tiempo real de las solicitudes al servicio.

Este documento incluye los métodos y clases que serán expuestas con el fin de que sean usadas por las entidades para su desarrollo interno y que realicen las pruebas iniciales del servicio.

## 3. Términos empleados

Para los fines del presente documento, se entenderá por:

- Autenticar: Proceso por el cual se verifica que una persona es quien dice ser.
- Autenticidad: La firma se realizó con un certificado válido de la jerarquía nacional.
- BCCR: Banco Central de Costa Rica.
- Binario: Cuando encuentre esta palabra en un tipo de dato, se refiere a un dato binario que debe ser codificado en “Base64”; excepto que específicamente se indique que se utilice otro tipo de codificación.
- BOM: Carácter Unicode que se utiliza para indicar el orden de los bytes en un documento.
- Cofirma: También llamada firma en línea es una firma múltiple donde los firmantes se encuentran en el mismo nivel, por lo cual el orden carece de importancia.

- Contrafirma: También llamada firma en cascada es una firma múltiple tipo mancomunada, ya que el firmante certifica la firma que se realizó con anterioridad.
- Entidad: Persona Jurídica participante de la plataforma SINPE o Central Directo.
- Firma avanzada: Se considera una firma avanzada cuando es integra, autentica y valida en el tiempo. Su vigencia es por siempre. Es recomendable utilizarla cuando se necesita que el documento que respalde la misma sea válido para siempre.
- Firma básica: Se considera una firma básica cuando es integra y autentica. Su vigencia está determinada por la fecha de vencimiento del certificado y la revocación de este. No es recomendable utilizar una firma básica cuando se necesita que el documento que respalde la misma sea válido para siempre.
- Firma válida: Se considera una firma válida si es integra y cumple con la autenticidad.
- Firmador BCCR: Servicio Firmador, Validador y Autenticador.
- FVA: Servicio Firmador, Validador y Autenticador.
- Garantía de validez en el tiempo: Existe evidencia de la validez del certificado con el que se firmó el documento y se puede comprobar en cualquier momento del tiempo. Esto se logra con información contenida en el documento.
- Integra: El documento no tiene modificaciones después de ser firmado.
- Sinpe: Sistema Nacional de Pagos Electrónicos.
- Suscriptor: Persona física que cuenta con un certificado de firma y autenticación, perteneciente a la jerarquía nacional.

## 4. Consideraciones generales

A continuación, se citan algunos aspectos generales concernientes a la comunicación entre los servidores de las entidades participantes en el servicio Firmador BCCR:

La interacción entre los sistemas se hará utilizando tecnología web, específicamente a través de Web Service y WCF seguros (usando TLS1.2 o superior).

Los tipos de datos que se detallan a continuación están basados en el WSDL del servicio, el cual es necesario para que las entidades realicen los ajustes a sus sistemas.

Los servicios serán asegurados con certificados digitales de agente electrónico de la jerarquía de persona jurídica

## 5. Servicios para firmar documentos y autenticar suscriptores

### 5.1. Proceso de solicitud de firma de un documento o autenticación del firmador

El procesamiento de una solicitud de la firma de un documento o autenticación está conformado por los siguientes pasos:

1. Consultar información del suscriptor: Se realiza antes de envíar una solicitud a los servicios del firma y autenticación, permite conocer aspectos importantes del suscriptor como lo son: el suscriptor cuenta con capacidad de firma digital, cuenta con funciones activas de accesibilidad, entre otras. Esto para procesar sus solicitudes.

Para disparar este proceso es necesario invocar el siguiente método:

**ObtengaLaInformacionDelSuscriptor**

2. Solicitud: Se realiza cuando la entidad envía una solicitud (firma o autenticación) a los servicios del firmador.


Para disparar este proceso es necesario invocar los métodos:

- RecibaLaSolicitudDeFirmaXmlEnvelopedCoFirma.
- RecibaLaSolicitudDeFirmaXmlEnvelopedContraFirma.
- RecibaLaSolicitudDeFirmaMSOffice.
- RecibaLaSolicitudDeFirmaODF.
- RecibaLaSolicitudDeFirmaPdf.
- RecibaLaSolicitudDeAutenticacion.

3. Notificación: Se realiza cuando el firmador le notifica a la entidad el resultado de una solicitud (firma o autenticación).


Este proceso invoca el método **NotifiqueLaRespuesta** del servicio de notificación de la entidad.

4. Cancelar una solicitud en proceso: Se realiza cuando el usuario cancela una solicitud de autenticación o firma que no se ha finalizado.


Para disparar este proceso es necesario invocar al método:

**CanceleLaSolicitudDeAutenticacionOFirmaDelSuscriptor**.

## 5.2. Servicios publicados por el BCCR

A continuación, se detallan los servicios publicados por el SINPE y Central Directo para el consumo de las entidades.

## 5.3. Web Service y WCF Firmador

Para solicitar la firma digital de un documento, las entidades participantes harán uso de un servicio desarrollado por el BCCR, que contendrá los métodos descritos a continuación.

### 5.3.1. RecibaLaSolicitudDeFirmaXmlEnvelopedCoFirma

Este método recibe los datos de una solicitud de firma digital que el servicio Firmador BCCR procesará y enviará al suscriptor.

El tamaño máximo permitido para el documento en formato xml de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de la identidad de marca de la entidad que solicita la firma.
- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de firma. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea enviar al suscriptor para firmarlo. Esta propiedad no debe contener caracteres BOM. (ver Remover BOM de un archivo XML).

- ResumenDocumento: Campo alfanumérico (String) obligatorio que se utiliza para identificar el resumen del documento a firmar. Corresponde al texto que se le desplegará al suscriptor en el Firmador BCCR.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (Tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer) que indica la razón por la cual la solicitud no puede ser procesada. (Ver tabla de Códigos de error.).
- CodigoDeVerificacion: Código alfanumérico (String) generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer), que representa el lapso en segundos en el que se espera que una solicitud de firma sea procesada.
- IdDeLaSolicitud: Campo numérico (Integer), que corresponde con el identificador de la solicitud.

#### 5.3.2. RecibaLaSolicitudDeFirmaXmlEnvelopedContraFirma

Este método recibe los datos de una solicitud de firma que el servicio Firmador BCCR procesará y enviará al suscriptor. Donde el tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.

- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de firma Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea enviar al suscriptor para que sea firmado. Esta propiedad no debe contener caracteres BOM. (Ver Remover BOM de un archivo XML).

- ResumenDocumento: Campo alfanumérico (String) obligatorio que se utiliza para identificar el resumen del documento, texto que se le desplegará al suscriptor en el Firmador BCCR.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado al documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver tabla de códigos de algoritmos.
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer), que indica la razón por la cual la solicitud no puede ser procesada. (Ver Tabla de Códigos de error)
- CodigoDeVerificacion: Código alfanumérico (String) generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer), que representa el lapso en segundos en el que se espera que una solicitud de firma sea procesada.
- IdDeLaSolicitud: Campo numérico (Integer), con el identificador de la solicitud.

### 5.3.3. RecibaLaSolicitudDeFirmaMSOffice

Este método recibe los datos de una solicitud de firma de documentos Microsoft Office (formatos soportados .docx, .xlsx y .pptx) que el servicio Firmador BCCR procesará y enviará al suscriptor. Donde el tamaño del documento no debe superar los 20 Mb (20480 Kb). Y en la configuración se debe permitir enviar y recibir hasta 20530 Kb.

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.
- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.

- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de firma. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Documento: Campo binario obligatorio, codificado en formato UTF-8, que identifica el documento que se desea enviar al suscriptor para firmarlo.

- ResumenDocumento: Campo alfanumérico (String) obligatorio que se utiliza para identificar el resumen del documento, texto que se le desplegará al suscriptor en el Firmador BCCR.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado al documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. (Ver Tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer). Que indica la razón por la cual la solicitud no puede ser procesada. (Ver Tabla de Códigos de error).
- CodigoDeVerificacion: Código alfanumérico (String) generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer), que representa el lapso máximo en segundos, en el que se espera que una solicitud de firma sea procesada.
- IdDeLaSolicitud: Campo numérico, con el identificador único de la solicitud.

#### 5.3.4. RecibaLaSolicitudDeFirmaODF

Este método recibe los datos de una solicitud de firma de documentos de Libre Office (formatos soportados .odt, .ods y .odp) que el servicio procesará y enviará al suscriptor. Donde el tamaño máximo permitido para el documento no debe superar los 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.
- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de firma. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Documento: Campo binario obligatorio, codificado en formato UTF-8, que identifica el documento que se desea enviar al suscriptor para ser firmado.

- ResumenDocumento: Campo alfanumérico (String) obligatorio que se utiliza para identificar el resumen del documento, texto que se le desplegará al suscriptor en el Firmador BCCR.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado al documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento a enviar. (Ver Tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer). Que indica la razón por la cual la solicitud no puede ser procesada. (Ver Tabla de Códigos de error).
- CodigoDeVerificacion: Código alfanumérico (String) generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer), con el lapso en segundos en el que se espera que una solicitud de firma sea procesada.
- IdDeLaSolicitud: Campo numérico (Integer) con el identificador de la solicitud.

#### 5.3.5. RecibaLaSolicitudDeFirmaPdf

Este método recibe los datos de una solicitud de firma que el servicio Firmador BCCR procesará y enviará al suscriptor. Donde el tamaño máximo del documento no debe superar los 20 Mb (20480 Kb).

Recibe: SolicitudDeFirmaPdf, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.
- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de firma Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea enviar al suscriptor para ser firmado.

- ResumenDocumento: Campo alfanumérico (String) obligatorio que se utiliza para identificar el resumen del documento a firmar. Corresponde al texto que se le desplegará al suscriptor en el Firmador BCCR.

- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado al documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento a enviar. (Ver Tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.
- Lugar: Campo alfanumérico (String) obligatorio que describe el lugar en donde se realizó la firma.
- Razón: Campo alfanumérico (String) obligatorio que indica La razón de la firma.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer). Que indica la razón por la cual la solicitud no puede ser procesada. (Ver Tabla de Códigos de error).
- CodigoDeVerificacion: Código alfanumérico (String), generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer), que representa el lapso en segundos en el que se espera que una solicitud de firma sea procesada
- IdDeLaSolicitud: Campo numérico (Integer), con el identificador de la solicitud.

#### 5.3.6. ElSuscriptorEstaConectado

Este método debe ser utilizado para consultar si un suscriptor está conectado al agente del Firmador BCCR.

Recibe: laIdentificacion, campo alfanumérico (String) que identifica al suscriptor. Debe tener un formato válido, para nacional 00-0000-0000, para DIDI 500000000000 y para DIMEX 100000000000.

Retorna: Verdadero si está conectado y Falso si no está conectado.

#### 5.3.7. ValideElServicio

Este método deber ser utilizado para verificar si el servicio firmador está disponible.

Recibe: Este método no recibe nada.

Retorna: Verdadero, si el servicio está disponible y Falso si no está disponible.

#### 5.3.8. Consultante de información del suscriptor

Este servicio se recomienda invocar antes de realizar una solicitud de autenticación o firma ya que permite consultar la información de un suscriptor con el fin de poder brindarle una mejor experiencia a la hora de utilizar los servicios de GAUDI.

En el mismo podemos conocer:

El estado de conexión del suscriptor en el agente GAUDI.

- Si el suscriptor activó la opción de accesibilidad y por ende las notificaciones no se muestran automáticamente en el agente GAUDI.
- El suscriptor tiene capacidad de firma móvil.

- El suscriptor cuenta con un certificado de firma digital con tarjeta.

Las entidades participantes podrán hacer uso de un servicio desarrollado por el BCCR, que contendrá el método descrito a continuación:

- ObtengaLaInformacionDelSuscriptor

Este método recibe los datos de un suscriptor para obtener la información del mismo.

Recibe: laIdentificacion: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a revisar el estado de accesibilidad. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Retorna: InformacionDelSuscriptor, esta clase representa la respuesta de la consulta de información del suscriptor y contiene las siguientes propiedades:

- EstaConectadoAlAgenteGaudi: Campo Boolean que indica si el suscriptor se encuentra conectado al Agente Gaudi
- FueExitosa: Campo Boolean que indica si el resultado de la firma se completó sin errores.
- NotificacionesDesactivadasPorAccesibilidad: Campo Boolean que indica si las notificaciones están desactivadas por accesibilidad.
- TieneAlMenosUnaTarjetaParaFirmar: Campo Boolean que indica si el suscriptor tiene al menos una tarjeta para realizar la firma.
- TieneCapacidaDeFirmaMovil: Campo Boolean que indica si el suscriptor tiene registrado un móvil para realizar la firma.
- CodigoDeError: Campo numérico (Integer) que indica la razón por la cual la solicitud no puede ser procesada. (Ver tabla de Códigos de error.)

### 5.3.9. Cancelación de solicitudes en proceso del Suscriptor

Para cancelar el proceso de autenticación de un suscriptor o la firma digital de un documento cualquiera, las entidades participantes podrán hacer uso de un servicio desarrollado por el BCCR, que contendrá el método descrito a continuación:

- CanceleLaSolicitudDeAutenticacionOFirmaDelSuscriptor

Este método recibe los datos de un suscriptor, en este caso su identificación, para poder cancelar una solicitud de firma o de autenticación que se está procesando en tiempo real.

Recibe:

laIdentificacion: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a cancelar la solicitud de autenticación o firma. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Retorna:

RespuestaAlCancelarSolicitud, esta clase representa la respuesta a una solicitud de cancelación de autenticación y/o firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean que indica si el resultado de la firma se completó sin errores.
- CodigoDeError : Campo numérico (Integer) que indica la razón por la cual la solicitud no puede ser procesada. (Ver tabla de Códigos de error.)

#### 5.3.10. Mostrar notificación desactivada por accesibilidad

En el momento que un suscriptor active la configuración de accesibilidad, a este no se le mostrarán las notificaciones en el agente GAUDI, sin embargo, mediante esta funcionalidad se podrá mostrar la notificación cuando el suscriptor lo solicite mediante una implementación por parte de la entidad, con esto podrá visualizar los datos de la solicitud en pantalla y el elegir el código de verificación y finalizar el proceso de autenticación o la firma de un documento. Si se desea conocer si un suscriptor tiene activado o no las notificaciones por accesibilidad se puede utilizar el método antes descrito: ObtengaLaInformacionDelSuscriptor.

Las entidades participantes podrán hacer uso de un servicio desarrollado por el BCCR, que contendrá el método descrito a continuación:

- ConsulteYNotifiqueSolicitudEnProcesoAlAgenteGaudiPorAccesibilidadServicio

Este método recibe los datos de un suscriptor, en este caso su identificación para consultar su configuración de accesibilidad y así poder notificar al agente GAUDI sobre una solicitud de firma o de autenticación en tiempo real.

Recibe: laIdentificacion, campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a revisar el estado de accesibilidad. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Retorna: RespuestaAlNotificar, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean que indica si el resultado de la firma se completó sin errores.
- CodigoDeError: Campo numérico (Integer) que indica la razón por la cual la solicitud no puede ser procesada. (Ver tabla de Códigos de error.)

### 5.4. Web Service y WCF Autenticador

Para solicitar la autenticación de un usuario por medio del Firmador BCCR, las entidades harán uso de un servicio desarrollado por el BCCR, que contendrá los siguientes métodos.

#### 5.4.1. RecibaLaSolicitudDeAutenticacion

Este método recibe los datos de una solicitud de autenticación que el servicio Firmador BCCR procesará y enviará al suscriptor.

Recibe: laSolicitud, esta clase representa la solicitud de autenticación que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.
- IdReferenciaEntidad: Campo numérico (Integer) obligatorio que utiliza la entidad para identificar la solicitud de firma, este número debe ser el resultado del identificador único de una tabla transaccional, en donde se guarden las solicitudes de firma.

- IdentificacionDelSuscriptor: Campo alfanumérico (String) obligatorio que identifica al suscriptor al cual se va a enviar la solicitud de autenticación. Debe tener un formato válido según se especifica en la norma complementaria de codificaciones generales del sistema de pagos.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de autenticación que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodigoDeError: Campo numérico (Integer) que en caso de que la operación sea válida o haya sido rechazada, contiene un código numérico, que indica la razón. Ver (Tabla de Códigos de error).
- CodigoDeVerificacion: Código alfanumérico (String) generado por el servicio Firmador BCCR. Es responsabilidad de la entidad mostrar este valor al suscriptor, para el debido procesamiento de la solicitud.
- IdDeLaSolicitud: Campo numérico (Integer) con el identificador de la solicitud.
- TiempoMaximoDeFirmaEnSegundos: Campo numérico (Integer) con el lapso en segundos en el que se espera que una solicitud de firma sea procesada.
- ResumenDelDocumento: Campo alfanumérico (String) que se utiliza para identificar el resumen del documento.
- InformacionSuscriptorDesconectado: Contiene la información del suscriptor desconectado, este objeto solo viene si el código de error en la respuesta es 9 (suscriptor desconectado), si no, el campo viene nulo. Contiene las siguientes propiedades:

HaIniciadoSesionEnElFirmador: Campo Boolean, puede ser:

"Verdadero" si el suscriptor alguna vez ha iniciado sesión en el Firmador BCCR.

"Falso" si el suscriptor nunca ha iniciado sesión en el Firmador BCCR.

RutaDeDescargaDelFirmador: Ruta de descarga del Firmador BCCR.

ValideElServicio.

Este método deber ser utilizado para verificar si el servicio de autenticación se encuentra disponible.

Recibe: Este servicio no recibe nada.

Retorna: Campo Boolean, su valor es "Verdadero" si el servicio está disponible y "Falso" si no está disponible.

## 5.5. Servicio publicado por la entidad

A continuación, se detalla el servicio que debe ser publicado por la entidad para ejecutar el proceso de firma y autenticación.

## 5.6. Web Service o WCF para la notificación de solicitudes de firma y autenticación

Para la operativa de solicitud de firma digital de un documento o la solicitud de autenticación, las entidades deberán proveer al BCCR un servicio Web Service o WCF seguro que contendrá la siguiente interfaz.

### 5.6.1. NotifiqueLaRespuesta

Este método es ofrecido por una entidad con el fin de recibir el resultado de un proceso de firma o autenticación.

Recibe: ResultadoDeFirma, esta clase representa el resultado de la solicitud de la firma, tiene las siguientes propiedades:

- IdDeLaSolicitud: Campo numérico (Integer) con el identificador de la solicitud que se está notificando. Este dato fue enviado por el servicio Firmador BCCR al iniciar la solicitud.
- DocumentoFirmado: Campo binario codificado en formato UTF-8 que identifica el documento firmado por el suscriptor.
- FueExitosa: Campo Boolean que indica si el resultado de la firma se completó sin errores.
- CodigoDeError: Campo numérico (Integer) con el motivo de error (si lo hubiese). (Ver Tabla de Códigos de error).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver tabla de códigos de algoritmos.
- HashDocumentoFirmado [En desuso]: Campo alfanumérico (String) que se utiliza para identificar el hash calculado al documento firmado.[1]
- HashDelDocumentoFirmadoEnBytes: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

Retorna: Este servicio no retorna nada.

#### 5.6.2. ValideElServicio

Este método es ofrecido por una entidad financiera con el fin de poder realizar una verificación de que el servicio se encuentra funcionando correctamente.

Retorna: Campo Boolean, su valor es "Verdadero" si el servicio está disponible y "Falso" si no lo está.

## 6. Servicios para validar certificados

### 6.1. Web Service y WCF Validador de Certificados

Para solicitar la validación de un certificado digital, las entidades harán uso de un servicio desarrollado por el BCCR, que contendrá los siguientes métodos.

#### 6.1.1. SoliciteLaValidacionDeCetificadoDeAutenticacion

Descripción: Este método se debe utilizar para validar el estado de un certificado de autenticación. Si el certificado enviado pertenece a la jerarquía nacional, se retorna el detalle de este.

Recibe: elCertificadoDeAutenticacion, campo binario que contiene el certificado utilizado durante el proceso de autenticación.

Retorna:

- FueExitosa: Campo Boolean, su valor es "Verdadero" si la validación es correcta, es "Falso" si la validación es incorrecta. Si la validación fue incorrecta el detalle del problema se envía en el campo CodigoDeError.

[1] *Se debe usar el campo "HashDelDocumentoFirmadoEnBytes" en lugar de éste. Se mantiene por compatibilidad hacia atrás con aplicaciones anteriores.*

- CodigoDeError: Campo numérico (Integer) que indica la razón por la cual la validación no fue exitosa. (Ver Tabla de Códigos de error).
- InformacionDelCertificado: Contiene la Información del Certificado. En caso de que no se pueda determinar el estado del certificado, este objeto se retorna nulo. Contiene las siguientes propiedades:

  FechaFinalDeLaVigencia: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos), con la fecha en la cual finaliza la vigencia del certificado.

  FechaInicioDeLaVigencia: Campo tipo fecha (DateTime, Día/Mes/Año Hora:Minutos:Segundos), con la fecha en la cual inicia la vigencia del certificado.

  Identificacion: Campo alfanumérico (String), corresponde a la identificación de la persona a la cual le pertenece el certificado.

  NombreCompleto: Campo alfanumérico (String), corresponde al nombre completo del suscriptor al cual le pertenece el certificado.

  TipoDeIdentificacion: Campo numérico (Integer), es el tipo de identificación del suscriptor. Ver (Tabla de tipos de identificación).

#### 6.1.2. ValideElServicio

Descripción: Este método deber ser utilizado para verificar si el servicio validador de certificados está disponible.

Recibe: este servicio no recibe nada.

Retorna: Campo Boolean, su valor es “Verdadero” si el servicio está disponible y “Falso” si no está disponible.

## 7. Servicios para verificar el uso del firmador

### 7.1. Web Service y WCF Verificador de uso del Firmador

Para solicitar la verificación de uso del Firmador BCCR, las entidades harán uso de un servicio desarrollado por el BCCR, que contará con los siguientes métodos.

#### 7.1.1. ExisteUnaSolicitudDeFirmaCompleta

Descripción: Este método se debe utilizar para verificar si una persona física ha interactuado alguna vez con el firmador y ha realizado al menos una firma digital.

Recibe: laCedulaDelUsuario, campo tipo alfanumérico (String) que corresponde a la identificación de la persona física que se desea consultar.

Retorna: RespuestaDeLaSolicitud, esta clase representa el resultado de la consulta procesada por el servicio que contiene las siguientes propiedades:

- FueExitosa: Campo Boolean. Su valor es “Verdadero” si la operación se ejecutó satisfactoriamente, es “Falso” si la operación se ejecutó con problemas. El detalle del problema se envía en el campo CodigoDeError.
- ExisteUnaFirmaCompleta: Campo Boolean. Su valor es “Verdadero” si la persona ha realizado el proceso de firma completo al menos una vez.

- CodigoDeError: Campo numérico (Integer) que indica la razón por la cual la operación no fue exitosa. (Ver Tabla de Códigos de error).

#### 7.1.2. ValideElServicio

Descripción: Este método deber ser utilizado para verificar si el servicio está disponible.

Recibe: este servicio no recibe nada.

Retorna: Campo Boolean, su valor es "Verdadero" si el servicio está disponible y "Falso" si no está disponible.

## 8. Servicios para completar firmas digitales en documentos firmados

### 8.1. Web Service y WCF Completador de documentos

Para solicitar el servicio completador de Firmas Digitales, las Entidades Bancarias harán uso de un servicio desarrollado por el BCCR, que contendrá los siguientes métodos.

#### 8.1.1. CompleteElDocumentoXmlEnvelopedCoFirma

Descripción: Este método recibe un documento en formato XML que el servicio FVA validará e intentará completar según su estado y enviará el resultado a la entidad solicitante.

Recibe: elDocumentoXml, campo binario que contiene el documento XML firmado no avanzado a completar. El documento puede contener una o varias firmas.

Retorna:

- FueExitosa: Retorna "Verdadero" si las firmas se completaron de manera correcta, "Falso" si existió algún problema al completar las firmas a formato avanzado.
- CodigoDeError: Campo numérico, con el código de error. Ver tabla de Códigos de error.
- Advertencias: Campo de tipo listado alfanumérico (List Of String), con las advertencias que indican las razones por las que no se pueden completar las firmas.
- Documento: Campo binario, codificado en formato UTF-8, que contiene el documento completado en formato avanzado.

#### 8.1.2. CompleteElDocumentoXmlEnvelopedContraFirma

Descripción: Este método recibe un documento en formato XML que el servicio validará e intentara completar todas las firmas básicas, si alguna de las firmas no es válida no se completará ninguna firma.

Recibe: elDocumentoXml: Campo binario que contiene el documento XML firmado no avanzado a completar, puede contener una o varias firmas.

Retorna:

- FueExitosa: Retorna "Verdadero" si las firmas se completaron de manera correcta, "Falso" si existió algún problema al completar las firmas a formato avanzado.
- CodigoDeError: Campo numérico, con el código de error. Ver tabla de Códigos de error.
- Advertencias: Campo de tipo listado alfanumérico (List Of String), con las advertencias que indican las razones por las que no se pueden completar las firmas.
- Documento: Campo binario, codificado en formato UTF-8, que contiene el documento completado en formato avanzado.

#### 8.1.3. CompleteElDocumentoODF

Descripción: Este método recibe un documento en formato ODF que el servicio validará e intentará completar.

Recibe: elDocumentoODF, campo binario que contiene el documento ODF (ODT, ODP, ODS) firmado no avanzado a completar, puede contener una o varias firmas.

Retorna:

- FueExitosa: Retorna "Verdadero" si las firmas se completaron de manera correcta, "Falso" si existió algún problema al completar las firmas a formato avanzado.
- CodigoDeError: Campo numérico, con el código de error. Ver tabla de Códigos de error.
- Advertencias: Campo de tipo listado alfanumérico (List Of String), con las advertencias que indican las razones por las que no se pueden completar las firmas.
- Documento: Campo binario, con el documento que se envió a completar.

#### 8.1.4. CompleteElDocumentoMSOffice

Descripción: Este método recibe un documento en formato OOXML que el servicio FVA validará e intentará completar.

Recibe: elDocumentoOOXML, campo binario que contiene el documento Office (DOCX, XLSX, PPTX) firmado no avanzado a completar, puede contener una o varias firmas.

Retorna:

- FueExitosa: Retorna "Verdadero" si las firmas se completaron de manera correcta, "Falso" si existió algún problema al completar las firmas a formato avanzado.
- CodigoDeError: Campo numérico, con el código de error. Ver tabla de Códigos de error.
- Advertencias: Campo de tipo listado alfanumérico (List Of String), con las advertencias que indican las razones por las que no se pueden completar las firmas.
- Documento: Campo binario, con el documento que se envió a completar.

#### 8.1.5. ValideElServicio

Descripción: Este método deber ser utilizado para verificar si el servicio completador está disponible.

Recibe: Este método no recibe nada.

Retorna: Boolean, retorna "Verdadero" si el servicio está disponible y "Falso" si no está disponible.

## 9. Servicios sellar documentos con certificado de sello electrónico custodiado por el BCCR

### 9.1. Web Service y WCF Sellador Electrónico con control de llave

Para solicitar el sellado electrónico de un documento, las Entidades Participantes harán uso de un servicio desarrollado por el BCCR, que contendrá los siguientes métodos.

#### 9.1.1. RecibaLaSolicitudDeSelladoElectronicoXmlEnvelopedCoFirma

Descripción: Este método recibe los datos de una solicitud de sellado de documento en formato xml que el servicio Firmador BCCR procesará y como resultado retornará un documento firmado digitalmente con el certificado de sello electrónico custodiado de la entidad.

El tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de la identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo DateTime (Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea firmar. Esta propiedad no debe contener caracteres BOM. (ver Remover BOM de un archivo XML).
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean, su valor es “Verdadero” si la firma se ejecutó sin problemas, es “Falso” si existieron problemas al procesar la solicitud el detalle del problema se envía en el campo CodigoDeError.
- DocumentoFirmado: Campo binario codificado en formato UTF-8 que contiene el documento firmado.
- CodigoDeError: Campo numérico con el motivo de error. (Ver tabla de Códigos de error ).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver (tabla de códigos de algoritmos).
- HashDocumentoFirmado: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

#### 9.1.2. RecibaLaSolicitudDeSelladoElectronicoMSOffice

Descripción: Este método recibe los datos de una solicitud de sello de documento en formato Microsoft Office (.docx, .xlsx y .pptx) que el servicio Firmador BCCR procesará y como resultado retornará un documento firmado digitalmente con el certificado de sello electrónico custodiado de la entidad.

El tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio Firmador BCCR y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de la identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo DateTime (Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea firmar.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean, su valor es “Verdadero” si la firma se ejecutó sin problemas, es “Falso” si existieron problemas al procesar la solicitud, el detalle del problema se envía en el campo CodigoDeError.
- DocumentoFirmado: Campo binario codificado en formato UTF-8 que identifica el documento firmado.
- CodigoDeError: Campo numérico con el motivo de error. (Ver tabla de Códigos de error ).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver (tabla de códigos de algoritmos).
- HashDocumentoFirmado: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

#### 9.1.3. RecibaLaSolicitudDeSelladoElectronicoOdf

Descripción: Este método recibe los datos de una solicitud de sello de documentos en formato abierto (.odp, .ods y .odt) que el servicio FVA procesará y como resultado retornará un documento firmado digitalmente con el certificado de sello electrónico custodiado de la entidad.

El tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio FVA y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo DateTime (Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea firmar.

- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean, su valor es "Verdadero" si la firma se ejecutó sin problemas, es "Falso" si existieron problemas al procesar la solicitud, el detalle del problema se envía en el campo CodigoDeError.
- DocumentoFirmado: Campo binario codificado en formato UTF-8 que contiene el Documento Firmado.
- CodigoDeError: Campo numérico con el motivo de error. (Ver tabla de Códigos de error ).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver (tabla de códigos de algoritmos).
- HashDocumentoFirmado: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

#### 9.1.4. RecibaLaSolicitudDeSelladoElectronicoXmlEnvelopedContraFirma

Descripción: Este método recibe los datos de una solicitud de sellado de documento en formato xml que el servicio Firmador BCCR procesará y como resultado retornará un documento firmado digitalmente con el certificado de sello electrónico custodiado de la entidad.

El tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirma, esta clase representa la solicitud de firma que será procesada por el servicio FVA y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de la identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo DateTime (Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea firmar. Esta propiedad no debe contener caracteres BOM. (ver Remover BOM de un archivo XML).
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean, su valor es “Verdadero” si la firma se ejecutó sin problemas, es “Falso” si existieron problemas al procesar la solicitud el detalle del problema se envía en el campo CodigoDeError.
- DocumentoFirmado: Campo binario codificado en formato UTF-8 que contiene el documento firmado.
- CodigoDeError: Campo numérico con el motivo de error. (Ver tabla de Códigos de error ).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver (tabla de códigos de algoritmos).
- HashDocumentoFirmado: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

#### 9.1.5. RecibaLaSolicitudDeSelladoElectronicoPdf

Descripción: Este método recibe los datos de una solicitud de sellado de documentos en formato Pdf que el servicio procesará y como resultado retornará un documento firmado digitalmente con el certificado de sello electrónico custodiado de la entidad.

Las firmas digitales generadas por este método son del tipo certificación, lo que implica que el documento enviado al servicio no debe contener firmas digitales.

El tamaño máximo permitido para el documento de dicha solicitud no debe ser superior a 20 Mb (20480 Kb).

Recibe: SolicitudDeFirmaPdf, esta clase representa la solicitud de firma que será procesada por el servicio FVA y contiene las siguientes propiedades:

- CodNegocio: Campo numérico (Integer) obligatorio que identifica el código de la identidad de marca de la entidad que solicita la firma.
- FechaDeReferenciaDeLaEntidad: Campo tipo DateTime (Día/Mes/Año Hora:Minutos:Segundos) obligatorio para identificar la fecha en la que se envía la solicitud.
- Documento: Campo binario obligatorio, codificado en formato UTF-8, que contiene el documento que se desea firmar.
- HashDocumento: Campo binario obligatorio que se utiliza para identificar el hash calculado del documento.
- IDAlgoritmoHash: Código numérico (Integer) obligatorio que identifica el algoritmo utilizado para calcular el hash del documento. Ver (tabla de códigos de algoritmos).
- IdFuncionalidad: Campo numérico (Integer) no obligatorio que representa la funcionalidad de su identidad de marca, sirve para que la entidad tenga registro de las funcionalidades que envían solicitudes.
- Lugar: Campo alfanumérico obligatorio que describe el lugar en donde se realizó la firma.
- Razon: Campo alfanumérico obligatorio que indica la razón de la firma.

Retorna: RespuestaDeLaSolicitud, esta clase representa la respuesta a una solicitud de firma y contiene las siguientes propiedades:

- FueExitosa: Campo Boolean, su valor es “Verdadero” si la firma se ejecutó sin problemas, es “Falso” si existieron problemas al procesar la solicitud, el detalle del problema se envía en el campo CodigoDeError.
- DocumentoFirmado: Campo binario que contiene el documento Firmado.

- CodigoDeError: Campo numérico con el motivo de error. (Ver tabla de Códigos de error ).
- IDAlgoritmoHashDocumentoFirmado: Campo numérico (Integer) con el algoritmo utilizado para calcular el hash del documento firmado. Ver (tabla de códigos de algoritmos).
- HashDocumentoFirmado: Campo binario que se utiliza para identificar el hash calculado al documento firmado.

#### 9.1.6. ValideElServicio

Descripción: Este método deber ser utilizado para verificar si el servicio de sellado se encuentra disponible.

Recibe: Este servicio no recibe nada.

Retorna: Campo Boolean, su valor es "Verdadero" si el servicio está disponible y "Falso" si no está disponible.

## 10. Servicios para validar documentos firmados

### 10.1. Web Service y WCF Validador de Documentos

Para solicitar el servicio de validación de documentos, las Entidades Participantes harán uso de un servicio Web Service o WCF desarrollado por el BCCR, que contendrá los siguientes métodos.

#### 10.1.1. ValideElDocumentoXmlEnvelopedCoFirma

Este método recibe un documento firmado en formato XML y valida todas las firmas encontradas dentro del documento.

El tamaño máximo permitido para el documento en formato xml de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: El Documento, campo binario que contiene el documento en formato XML a validar.

Retorna: un elemento de tipo ResultadoValidacion, que contiene los siguientes atributos:

- FueExitosa: Verdadero, si se realizó la validación del documento. Falso, si no se realizó la validación del documento, para este escenario, consulte la propiedad ErrorGeneradoAlValidar.
- ErrorGeneradoAlValidar: Campo de tipo alfanumérico con el texto del detalle del error.
- Resumen: un elemento de tipo ResumenDelResultadoDeValidacion que contiene los siguientes atributos:
- ResultadoValidacionDelDocumentoFirmado: Campo numérico que representa el resultado de la validación de todas las firmas del documento, ver Tabla.
- ResumenDeFirmas: Lista de elementos de tipo ResumenDeFirma, cada elemento de tipo ResumenDeFirma contiene los siguientes campos:

  Firmante: Campo alfanumérico con el nombre del firmante, en caso de que no se determine el valor es "Desconocido".

  Identificacion: Campo alfanumérico con la identificación del firmante, en caso de que no se determine el valor es vacío.

  ResultadoValidacion: Campo numérico que representa el estado de respuesta, ver Tabla .

  FechaEstampaDeTiempo: Campo de tipo fecha con la fecha de la estampa de tiempo.

TipoIdentificacion: Campo numérico que representa el estado de respuesta, ver Tabla.

TieneFechaEstampaDeTiempo: Verdadero, cuando contiene una fecha en el campo FechaEstampaDeTiempo. Falso, cuando no contiene una fecha en el campo FechaEstampaDeTiempo.

#### 10.1.2. ValideElDocumentoXmlEnvelopedContraFirma

Este método recibe un documento firmado en formato XML y valida todas las firmas encontradas dentro del documento.

El tamaño máximo permitido para el documento en formato xml de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: El Documento, campo binario que contiene el documento en formato XML a validar.

Retorna: un elemento de tipo ResultadoValidacion, que contiene los siguientes atributos:

- FueExitosa: Verdadero, si se realizó la validación del documento. Falso, si no se realizó la validación del documento, para este escenario, consulte la propiedad ErrorGeneradoAlValidar.
- ErrorGeneradoAlValidar: Campo de tipo alfanumérico con el texto del detalle del error.
- Resumen: un elemento de tipo ResumenDelResultadoDeValidacion que contiene los siguientes atributos:
- ResultadoValidacionDelDocumentoFirmado: Campo numérico que representa el resultado de la validación de todas las firmas del documento, ver Tabla.
- ResumenDeFirmas: Lista de elementos de tipo ResumenDeFirma, cada elemento de tipo ResumenDeFirma contiene los siguientes campos:

  Firmante: Campo alfanumérico con el nombre del firmante, en caso de que no se determine el valor es “Desconocido”.

  Identificacion: Campo alfanumérico con la identificación del firmante, en caso de que no se determine el valor es vacío.

  ResultadoValidacion: Campo numérico que representa el estado de respuesta, ver Tabla .

  FechaEstampaDeTiempo: Campo de tipo fecha con la fecha de la estampa de tiempo.

  TipoIdentificacion: Campo numérico que representa el estado de respuesta, ver Tabla.

  TieneFechaEstampaDeTiempo: Verdadero, cuando contiene una fecha en el campo FechaEstampaDeTiempo. Falso, cuando no contiene una fecha en el campo FechaEstampaDeTiempo.

#### 10.1.3. ValideElDocumentoOdf

Este método recibe un documento firmado en formato (odt, odp, ods) y valida todas las firmas encontradas dentro del documento.

El tamaño máximo permitido para el documento en formato (odt, odp, ods) de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: El Documento, campo binario que contiene el documento en formato (odt, odp, ods) a validar.

Retorna: un elemento de tipo ResultadoValidacion, que contiene los siguientes atributos:

- FueExitosa: Verdadero, si se realizó la validación del documento. Falso, si no se realizó la validación del documento, para este escenario, consulte la propiedad ErrorGeneradoAlValidar.
- ErrorGeneradoAlValidar: Campo de tipo alfanumérico con el texto del detalle del error.
- Resumen: un elemento de tipo ResumenDelResultadoDeValidacion que contiene los siguientes atributos:
- ResultadoValidacionDelDocumentoFirmado: Campo numérico que representa el resultado de la validación de todas las firmas del documento, ver Tabla.
- ResumenDeFirmas: Lista de elementos de tipo ResumenDeFirma, cada elemento de tipo ResumenDeFirma contiene los siguientes campos:

  Firmante: Campo alfanumérico con el nombre del firmante, en caso de que no se determine el valor es “Desconocido”.

  Identificacion: Campo alfanumérico con la identificación del firmante, en caso de que no se determine el valor es vacío.

  ResultadoValidacion: Campo numérico que representa el estado de respuesta, ver Tabla .

  FechaEstampaDeTiempo: Campo de tipo fecha con la fecha de la estampa de tiempo.

  TipoIdentificacion: Campo numérico que representa el estado de respuesta, ver Tabla.

  TieneFechaEstampaDeTiempo: Verdadero, cuando contiene una fecha en el campo FechaEstampaDeTiempo. Falso, cuando no contiene una fecha en el campo FechaEstampaDeTiempo.

#### 10.1.4. ValideElDocumentoMSOffice

Este método recibe un documento firmado en formato (docx, pptx, xlsx) y valida todas las firmas encontradas dentro del documento.

El tamaño máximo permitido para el documento en formato (docx, pptx, xlsx) de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: El Documento, campo binario que contiene el documento en formato (docx, pptx, xlsx) a validar.

Retorna: un elemento de tipo ResultadoValidacion, que contiene los siguientes atributos:

- FueExitosa: Verdadero, si se realizó la validación del documento. Falso, si no se realizó la validación del documento, para este escenario, consulte la propiedad ErrorGeneradoAlValidar.
- ErrorGeneradoAlValidar: Campo de tipo alfanumérico con el texto del detalle del error.
- Resumen: un elemento de tipo ResumenDelResultadoDeValidacion que contiene los siguientes atributos:
- ResultadoValidacionDelDocumentoFirmado: Campo numérico que representa el resultado de la validación de todas las firmas del documento, ver Tabla.
- ResumenDeFirmas: Lista de elementos de tipo ResumenDeFirma, cada elemento de tipo ResumenDeFirma contiene los siguientes campos:

  Firmante: Campo alfanumérico con el nombre del firmante, en caso de que no se determine el valor es “Desconocido”.

Identificacion: Campo alfanumérico con la identificación del firmante, en caso de que no se determine el valor es vacío.

ResultadoValidacion: Campo numérico que representa el estado de respuesta, ver Tabla .

FechaEstampaDeTiempo: Campo de tipo fecha con la fecha de la estampa de tiempo.

TipoIdentificacion: Campo numérico que representa el estado de respuesta, ver Tabla.

TieneFechaEstampaDeTiempo: Verdadero, cuando contiene una fecha en el campo FechaEstampaDeTiempo. Falso, cuando no contiene una fecha en el campo FechaEstampaDeTiempo.

#### 10.1.5. ValideElDocumentoPdf

Este método recibe un documento firmado en formato pdf y valida todas las firmas encontradas dentro del documento.

El tamaño máximo permitido para el documento en formato pdf de dicha solicitud no debe superar los 20 Mb (20480 Kb).

Recibe: El Documento, campo binario que contiene el documento en formato pdf a validar.

Retorna: un elemento de tipo ResultadoValidacion, que contiene los siguientes atributos:

- FueExitosa: Verdadero, si se realizó la validación del documento. Falso, si no se realizó la validación del documento, para este escenario, consulte la propiedad ErrorGeneradoAlValidar.
- ErrorGeneradoAlValidar: Campo de tipo alfanumérico con el texto del detalle del error.
- Resumen: un elemento de tipo ResumenDelResultadoDeValidacion que contiene los siguientes atributos:
- ResultadoValidacionDelDocumentoFirmado: Campo numérico que representa el resultado de la validación de todas las firmas del documento, ver Tabla.
- ResumenDeFirmas: Lista de elementos de tipo ResumenDeFirma, cada elemento de tipo ResumenDeFirma contiene los siguientes campos:

  Firmante: Campo alfanumérico con el nombre del firmante, en caso de que no se determine el valor es “Desconocido”.

  Identificacion: Campo alfanumérico con la identificación del firmante, en caso de que no se determine el valor es vacío.

  ResultadoValidacion: Campo numérico que representa el estado de respuesta, ver Tabla .

  FechaEstampaDeTiempo: Campo de tipo fecha con la fecha de la estampa de tiempo.

  TipoIdentificacion: Campo numérico que representa el estado de respuesta, ver Tabla.

  TieneFechaEstampaDeTiempo: Verdadero, cuando contiene una fecha en el campo FechaEstampaDeTiempo. Falso, cuando no contiene una fecha en el campo FechaEstampaDeTiempo.

#### 10.1.6. ValideElServicio

Descripción: Este método deber ser utilizado para verificar si el servicio de sellado se encuentra disponible.

Recibe: Este servicio no recibe nada.

Retorna: Campo Boolean, su valor es “Verdadero” si el servicio está disponible y “Falso” si no está disponible.

#### 10.1.7. Interpretación del resultado de la validación de Documentos

El servicio de validación de documento intenta validar todas las firmas digitales que contiene un documento, para interpretar correctamente el resultado se deben considerar los siguientes detalles:

**a)** ¿El servicio realizó la validación satisfactoriamente?

Para esto es necesario que la propiedad FueExitosa sea Verdadera.

**b)** ¿Cuál es el tipo de firma digital mínimo aceptado por su flujo de negocio, firma digital básica o avanzada?

El negocio debe tener claro cuál es el tipo de firma digital aceptado, firma básica o firma avanzada. La firma básica asegura la integridad y autenticidad de un documento, pero no asegura la validez en el tiempo (por la vigencia de los certificados y por la revocación), la firma digital avanzada asegura integridad, autenticidad y validez en el tiempo.

En la clase resumen, en la propiedad ResultadoValidacionDelDocumentoFirmado, se especifican los resultados de las validaciones de todas las firmas.

**c)** ¿Quiénes firmaron el documento?

En la clase ResumenDeFirma, se encuentra una lista con la información de las personas que firmaron el documento. La información más relevante es la siguiente:

- Firmante
- Tipo de identificación
- Identificación
- Fecha oficial de la firma (FechaEstampaDeTiempo)
- Resultado de validación. Si es básica o avanzada.

## 11. Referencia técnica para consumir los servicios

### 11.1. Prerrequisitos para implementar un cliente que consuma los servicios.

Los servicios publicados en este estándar están asegurados mediante un canal seguro, asegurado con el certificado de agente electrónico del Banco Central de Costa Rica. Además, están configurados para que todas las solicitudes gestionen autenticación mutua con certificados de agente electrónico.

Esto implica que un servidor de una entidad que hospede un servicio que quiera hacer uso directo de la plataforma centralizada, deberá contar con un certificado de agente electrónico de la jerarquía nacional vigente. Para cada invocación a los servicios de servicios del Firmador BCCR, se deberá agregar el certificado de agente electrónico respectivo.

A continuación, mostramos un ejemplo de un cliente que consume los servicios expuestos por WCF o por Web Service.

### 11.2. Ejemplo de consumo del servicio utilizando WCF

```
Dim elCertificadoDeLaEntidad As X509Certificate
```

```
Dim elServicio As Wcf.ServicioFirmador.FirmadorClient = Nothing
Dim laSolicitudDeFirma As SolicitudDeFirma
Dim laRespuestaDelServicio As RespuestaDeLaSolicitud
Try
    elCertificadoDeLaEntidad = ObtengaElCertificadoDeAgenteElectronico()
    laSolicitudDeFirma = CreeLaSolicitudDeFirma()
    elServicio = New Wcf.ServicioFirmador.FirmadorClient
    Dim elUrl = elServicio.Endpoint.Address.Uri
    elServicio.Endpoint.Address = New EndpointAddress(elUrl)
    elServicio.ClientCredentials.ClientCertificate.Certificate = elCertificadoDeLaEntidad
    laRespuestaDelServicio = elServicio.RecibaLaSolicitudDeFirmaXmlEnvelopedCoFirma(laSolicitudDeFirma)
Catch laExcepcion As Exception
    RegistreElErrorEnBitacora(laExcepcion)
Finally
    If elServicio IsNot Nothing Then
        Try
            If elServicio.State <> CommunicationState.Faulted Then
                elServicio.Close()
            Else
                elServicio.Abort()
            End If
        Catch ex As Exception
            System.Diagnostics.EventLog.WriteEntry("Application", String.Format("Error al cerrar el canal: {0}", ex), EventLogEntryType.Error)
        End Try
    End If
End Try
```

### 11.3.Ejemplo de consumo del servicio utilizando Web Service

A continuación un ejemplo para consumir unos de los métodos del Web Service en forma segura:

```
Dim elCertificadoDeLaEntidad As X509Certificate
```

```
Dim laSolicitudDeFirma As SolicitudDeFirma
Dim laRespuestaDelServicio As RespuestaDeLaSolicitud
Try
    elCertificadoDeLaEntidad = ObtengaElCertificadoDeAgenteElectronico()
    laSolicitudDeFirma = CreeLaSolicitudDeFirma()
    Using elServicio As New Ws.ServicioFirmador.Firmador
        elServicio.Url = ObtengaLaUrlDelServicioFirmador()
        elServicio.ClientCertificates.Add(elCertificadoDeLaEntidad)
         laRespuestaDelServicio                                                    =
elServicio.RecibaLaSolicitudDeFirmaXmlEnvelopedCoFirma(laSolicitudDeFirma)
    End Using
Catch laExcepcion As Exception
    RegistreElErrorEnBitacora(laExcepcion)
End
Try
```

## 12. Tablas de referencia

### 12.1. Códigos de algoritmos

| Código | Algoritmo |
|---|---|
| 1 | Sha256 |
| 2 | Sha384 |
| 3 | Sha512 |

### 12.2. Códigos de error del firmador al solicitar una firma o autenticación

| Código numérico | Descripción |
|---|---|
| 0 | Solicitud recibida correctamente. |
| 1 | Ha ocurrido algún problema al solicitar la firma o autenticación. |

| Código numérico | Descripción |
|---|---|
| 2 | Solicitud con campos incompletos. |
| 3 | Existe una diferencia no permitida entre la fecha y hora del cliente y la del servidor. La fecha/hora de la solicitud no debe tener una diferencia de más de 60 segundos de la fecha/hora del servidor. |
| 4 | La entidad no se encuentra registrada. |
| 5 | La entidad se encuentra en estado inactiva. |
| 6 | La identidad de marca no pertenece a la entidad solicitante. |
| 7 | El tamaño del resumen de la solicitud de firma es no valido, este debe ser mayor a 1 y menor a 250 caracteres. |
| 8 | El tamaño de la razón de firma de la solicitud de firma PAdES es inválida, este debe ser mayor a 1 y menor a 125 caracteres. |
| 9 | El suscriptor se encuentra desconectado para recibir una solicitud. |
| 10 | El formato de la identificación enviado no es válido, este debe tener un formato para un nacional 0#-####-#### para un DIDI 5########### para un DIMEX 1########### |
| 11 | La identidad de marca no se encuentra configurado para persona física. |
| 12 | La identidad de marca cuenta con una configuración de persona física deshabilitada. |
| 13 | La entidad no está habilitada para el uso del firmador por parte del representante legal. |
| 14 | No se han completado los escenarios en el ambiente de pruebas. |

### 12.3.Códigos de error del firmador al notificar una firma

| Código numérico | Descripción |
|---|---|
| 0 | Solicitud completada sin errores. |
| 1 | Ha ocurrido algún problema al firmar. |
| 2 | Solicitud de firma rechazada por el suscriptor. |
| 3 | El suscriptor ha excedido el tiempo máximo permitido para firmar la solicitud. |
| 4 | El suscriptor se encuentra desconectado para recibir una solicitud de firma. |
| 5 | El documento XML de la solicitud contiene una marca de bytes (BOM) no permitido. |

| Código numérico | Descripción |
|---|---|
| 6 | El documento de la solicitud es inválido. |
| 8 | El hash de la solicitud es incorrecto. |
| 9 | El certificado del suscriptor está revocado. |
| 10 | El certificado del suscriptor está vencido. |
| 11 | Existe una solicitud de firma en proceso para el cliente. |
| 12 | No se pudo notificar a la entidad. |
| 13 | El código de verificación es incorrecto |
| 14 | El suscriptor bloqueo el pin de la tarjeta |
| 15 | El documento no es válido para ser contrafirmado. |

### 12.4.Códigos de error del validador de certificados

| Código numérico | Descripción |
|---|---|
| 0 | Certificado válido. |
| 1 | Error interno al validar el certificado. |
| 2 | Los bytes enviados no corresponden a un certificado. |
| 3 | El certificado del suscriptor está vencido. |
| 4 | El certificado del suscriptor está revocado. |
| 5 | El Certificado enviado no es de confianza porque no es emitido por la CA Raíz Nacional. |
| 6 | El certificado enviado no es de autenticación. |
| 7 | El certificado tiene un problema de estructura, no cuenta con el OID de OCSP en el que se encuentra la dirección del servicio. |
| 8 | El certificado tiene un problema de estructura, no cuenta con los usos de la clave necesarios para un certificado de autenticación. |
| 9 | El certificado tiene un problema de estructura, el campo CN del sujeto tiene una estructura inválida. |
| 10 | El certificado tiene un problema de estructura, el campo SERIALNUMBER del sujeto tiene una estructura inválida. |
| 11 | La entidad no se encuentra registrada. |
| 12 | La entidad no se encuentra en estado inactiva. |

### 12.5.Tipo de identificación

| Código | Tipo de identificación |
|---|---|
| 1 | Identificación Nacional |
| 2 | DIMEX |
| 3 | DIDI |
| 4 | Jurídica (Solo aplica para el validador de documentos) |

### 12.6.Códigos de error del Servicio verificador

| Código numérico | Descripción |
|---|---|
| 0 | Verificación recibida correctamente. |
| 1 | Ha ocurrido algún problema al verificar el estado de la firma |
| 2 | La entidad no se encuentra registrada |
| 3 | La entidad se encuentra en estado inactiva. |

### 12.7.Códigos de error del Servicio completador de documentos

| Código numérico | Descripción |
|---|---|
| 0 | Las firmas digitales se completaron correctamente. |
| 1 | Error al completar el documento. |
| 2 | La entidad enviada no se encuentra registrada. |
| 3 | La entidad enviada se encuentra en estado inactiva. |
| 4 | El documento no tiene un formato válido. |
| 5 | El documento no contiene firmas. |
| 6 | Algunas de las firmas no pudieron ser completadas. |
| 7 | No se completó ninguna de las firmas. |

### 12.8.Códigos de error del Servicio sellado electrónico

| Código numérico | Descripción |
|---|---|
| 0 | Solicitud recibida correctamente. |
| 1 | Ha ocurrido algún problema al solicitar la firma. |
| 2 | Solicitud con campos incompletos. |
| 3 | Existe una diferencia no permitida entre la fecha y hora del cliente y la del servidor. |
| 4 | La entidad no se encuentra registrada. |
| 5 | La entidad se encuentra en estado inactiva. |
| 6 | La identidad de marca no pertenece a la entidad solicitante. |
| 7 | La identidad de marca no cuenta con un sello electrónico configurado. |
| 8 | La identidad de marca cuenta con una configuración de sello electrónico deshabilitada. |
| 9 | Documento no válido. |
| 10 | El Hash enviado del documento no coincide con el hash calculado. |
| 11 | El documento XML no es válido para ser contrafirmado. |
| 12 | La longitud de la razón no es válida. |
| 13 | El documento PDF posee firmas, para este tipo de documento, la firma de Certificación debe ser la primera. |
| 14 | La entidad no está habilitada para el uso del firmador por parte del representante legal. |
| 15 | El certificado de sello electrónico está vencido. |
| 16 | No se han completado los escenarios en el ambiente de pruebas. |

### 12.9.Estados de respuesta del Servicio Validador de Documentos

| Código numérico | Descripción |
|---|---|
| 0 | No válido. |
| 1 | Válido con advertencias. |
| 2 | Válido. |

### 12.10. Códigos de respuesta del Servicio Validador de Documentos

| Código numérico | Descripción |
|---|---|
| 1 | El contenido del documento no ha sido modificado después de realizada la firma. |
| 2 | La integridad del documento ha sido comprometida después de la firma. |
| 3 | La integridad del documento no puede ser comprobada porque el algoritmo de firma utilizado no es soportado. |
| 4 | El documento fue firmado con un certificado oficial. Certificados de la jerarquía contenidos en el documento. |
| 5 | El documento fue firmado con un certificado no oficial. |
| 6 | El certificado digital estaba vigente al momento de la firma. |
| 7 | El certificado digital está vigente. |
| 8 | El certificado digital no estaba vigente al momento de la firma. |
| 9 | El tipo de certificado utilizado es válido para firmar. |
| 10 | El tipo de certificado utilizado no es válido para firmar. Para persona física el tipo de certificado permitido es el de Firma Digital y para persona jurídica es el de Sello Electrónico. |
| 11 | En la firma se utilizó un certificado de Autenticación, el cual no es el recomendado para firmar. Para persona física el tipo de certificado permitido es el de Firma Digital. |
| 12 | El certificado no estaba revocado al momento de la firma. La información de revocación está contenida en el documento. |
| 13 | El certificado no estaba revocado al momento de la firma, pero la información necesaria para la validación de la revocación no está contenida en el documento. |
| 14 | El certificado está revocado. |
| 15 | No se puede validar en línea el estado de revocación del certificado firmante debido a que ya venció. |
| 16 | El documento cuenta con una estampa de tiempo en el momento de la firma. |
| 17 | El documento no cuenta con una estampa de tiempo oficial. |
| 18 | El documento no cuenta con una estampa de tiempo válida. |
| 19 | El documento no cuenta con una estampa de tiempo. |

| Código numérico | Descripción |
|---|---|
| 20 | El documento cuenta con una estampa de tiempo en el momento de la firma. Pero no incluye información de revocación o los certificados de la jerarquía correspondiente. |
| 21 | El documento fue firmado con un certificado oficial pero los certificados de la jerarquía no están contenidos en el documento. |
| 22 | El documento contiene una estampa de tiempo de una autoridad desconocida, sin embargo, no se utilizó para determinar la validez de la firma. |
| 23 | El documento contiene una estampa de tiempo de una autoridad desconocida, sin embargo, no se utilizó para determinar la validez de la firma. Además, cuenta con otra estampa de tiempo en el momento de la firma, pero no se incluye información de revocación o los certificados de la jerarquía correspondiente. |
| 24 | El certificado digital no está vigente. |
| 25 | El certificado no estaba revocado en el momento de la firma. El documento cuenta con información de revocación, pero fue descartada porque posee una validez fuera del rango de tolerancia. |
| 26 | No se puede validar en línea el estado de revocación del certificado firmante debido a que ya venció. El documento cuenta con información de revocación, pero fue descartada porque posee una validez fuera del rango de tolerancia. |

### 12.11. Resultado de validación de una firma digital

| Código numérico | Descripción |
|---|---|
| 0 | No válido. |
| 1 | Firma digital Básica. |
| 2 | Firma digital Avanzado. |

### 12.12. Resultado de la Validación del Documento Firmado

| Código numérico | Descripción | Escenarios de uso |
|---|---|---|
| 0 | Todas las firmas del documento no son válidas.<br>Al menos una firma del documento no es válida. | No hay escenarios de uso, porque el documento contiene firmas no válidas. Es un riesgo aceptar este documento. |
| 1 | Todas las firmas son válidas.<br>Al menos una firma del documento es básica o todas las firmas son básicas. | Cuando se aceptan firmas básicas y avanzadas |
| 2 | Cuando todas las firmas son avanzadas. | Cuando se aceptan solo firmas avanzadas |

### 12.13. Resultados de Garantía de Validez en el Tiempo

| Código numérico | Descripción |
|---|---|
| 0 | Cuando no cumple con jerarquía, ni vigencia, ni revocación o fecha oficial de la firma. |
| 1 | Cuando se cumple la jerarquía, la vigencia y la revocación, pero no cumple la fecha oficial de la firma. |
| 2 | Cuando cumple con jerarquía, vigencia, revocación y fecha oficial de la firma |

### 12.14. Remover BOM de un archivo XML

El siguiente es un ejemplo programado en vb.net, que permite remover el carácter BOM de un archivo XML.

```
Dim laCadenaXml As String

Dim laCadenaXmlSinBom As String

Dim elOrdenDeBytes As String

Dim elDocumentoEnArregloDeBytesOriginal As Byte()

Dim elDocumentoEnArregloDeBytesSinBom As Byte()

elDocumentoEnArregloDeBytesOriginal = ObtengaElDocumentoXmlAFirmar()

laCadenaXml = Encoding.UTF8.GetString(elDocumentoEnArregloDeBytesOriginal)

elOrdenDeBytes = Encoding.UTF8.GetString(Encoding.UTF8.GetPreamble())

laCadenaXmlSinBom = laCadenaXml.Remove(0, elOrdenDeBytes.Length)

elDocumentoEnArregloDeBytesSinBom = Encoding.UTF8.GetBytes(laCadenaXmlSinBom).
```

### 12.15. Código de error del servicio: Cancelación de solicitudes en proceso del Suscriptor

| Código numérico | Descripción |
|---|---|
| 0 | Solicitud recibida correctamente. |
| 1 | Ha ocurrido algún problema al cancelar la firma o autenticación. |
| 2 | El formato de la identificación enviado no es válido, este debe tener un formato para un nacional 0#-####-#### para un DIDI 5########### para un DIMEX 1########### |

| | |
|---|---|
| 3 | La entidad no se encuentra registrada. |
| 4 | La entidad se encuentra en estado inactiva. |

### 12.16. Código de error del servicio: Mostrar notificación desactivada por accesibilidad

| Código numérico | Descripción |
|---|---|
| 0 | Solicitud recibida correctamente. |
| 1 | Ha ocurrido algún problema al consultar. |
| 2 | La identificación debe incluirse. |
| 3 | El formato de la identificación enviado no es válido, este debe tener un formato para un nacional 0#-####-#### para un DIDI 5########### para un DIMEX 1########### |
| 4 | La entidad no se encuentra registrada. |
| 5 | La entidad se encuentra en estado inactiva. |
| 6 | No existe una solicitud en proceso |
| 7 | El suscriptor ha excedido el tiempo máximo permitido para firmar la solicitud |
| 9 | El suscriptor se encuentra desconectado para recibir una solicitud de firma. |

### 12.17. Código de error del servicio: Consultante de información del suscriptor

| Código numérico | Descripción |
|---|---|
| 0 | Consulta realizada correctamente. |
| 1 | Ha ocurrido algún problema al consultar. |
| 2 | El formato de la identificación enviado no es válido, este debe tener un formato para un nacional 0#-####-#### para un DIDI 5########### para un DIMEX 1########### |

| | |
|---|---|
| 3 | La entidad no se encuentra registrada. |
| 4 | La entidad se encuentra en estado inactiva. |