BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

FIRMADOR, VALIDADOR Y AUTENTICADOR

GUIA TÉCNICA DE CONFIGURACIÓN DEL SERVICIO FIRMADOR

CANAL PRIVADO

VERSION 1.2

sinpe

EE-FVA

Contenido

Introducción

El propósito de este documento es facilitar la puesta en marcha en el ambiente de producción que utilizan un canal privado, de los servicios web que consuman las funcionalidades de GAUDI, provisto por el Banco Central de Costa Rica por medio de una red privada.

Este documento permite a los departamentos de informática de cada entidad asociada al SINPE, verificar el estado de sus sistemas internos e identificar los ajustes necesarios para evitar contratiempos en la participación de la entidad en el servicio.

Términos empleados

- Para los fines del presente documento, se entenderá por:
    - **SINPE**: Sistema Nacional de Pagos Electrónicos.
    - **COS**: Centro de Operaciones del SINPE.
    - **BCCR**: Banco Central de Costa Rica.
    - **GAUDI**: Gestor de Firmas y Autenticaciones Digitales del Banco Central.
    - **Identidad de marca**: Se entiende por identidad de marca un portal web transaccional en donde se brindan servicios que requieren el uso de funcionalidades del Firmador GAUDI. Por ejemplo, para el caso del BCCR, se tiene registrado como identidad de marca a Central Directo y los portales de las superintendencias (SUGEF, SUGESE y SUGEVAL).

Paso 1: ¿Qué necesito antes de iniciar la configuración de las funcionalidades del servicio Firmador?

- **Un certificado de agente electrónico de la jerarquía nacional**: Le permitirá asegurar los servicios que va a exponer para que el BCCR los consuma, además este certificado le permitirá al BCCR identificar a la entidad que se encuentra realizando solicitudes de firma o autenticación.
- **Identificar la identidad de marca que va a consumir el servicio**: En el proceso es necesario crear una identidad de marca, para esto es necesario definir el nombre y el logo de dicha identidad. El logo deberá tener un tamaño de 184 px de ancho x 84 px de alto, las extensiones permitidas son .jpg y .png.
- **Un sitio privado configurado en donde el servicio de su entidad va a consumir las funcionalidades del servicio Firmador y además se le van a hacer notificaciones**: Este sitio privado de su entidad va a ser el encargado de solicitar las firmas y autenticaciones; además el servicio Firmador le va a notificar el resultado de dichas solicitudes al sitio que se indique en la configuración, no necesariamente el sitio que solicita y recibe las notificaciones debe ser el mismo. Consulte el Anexo "Configuración de los servidores".

Es necesario que el servicio de notificación cumpla con el estándar electrónico. Consulte el Anexo "Publicar el servicio de notificaciones".

Paso 2: Solicite el acceso, a nivel de telecomunicaciones, a las funcionalidades del servicio Firmador GAUDI Persona Fisica

Solicitud

La solicitud de acceso al ambiente para pruebas y producción (actualmente es el mismo a nivel de telecomunicaciones) se debe realizar por medio del envío de un caso al **COS**, registrado por el Responsable de Servicios de la entidad. Se debe especificar los datos que se describen a continuación:

- Dirección **IP** de los **servidores**, desde donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el servicio **Firmador**.
    - Si el servicio que realiza las invocaciones está instalado en un clúster de servidores, se debe proporcionar la dirección IP de cada uno de los nodos que conforman el clúster.
- Dirección **IP** del **servidor** (o clúster) donde se encuentra publicado el (los) **servicio**(s) de **notificación** perteneciente(s) a la entidad. Sólo puede existir un único servicio de notificación por identidad de marca de cada entidad.

Resultado

- La IP del servidor donde se encuentran alojados los servicios web que la entidad deberá consumir del BCCR, además se incluirá la IP de los servidores desde donde el BCCR se comunicará con la entidad para realizar la notificación correspondiente. Esta información es distinta para cada entidad:
    - La IP del servidor **orosi.fdi.cr.**
    - La IP del servidor **tenorio.fdi.cr.**

Paso 3: Cree la identidad de marca

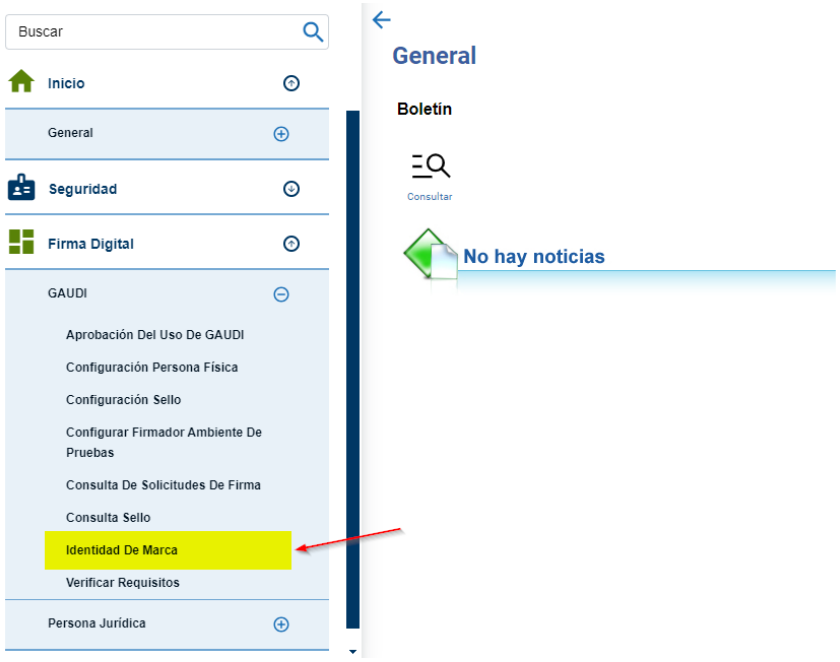
Para crear la identidad de marca realice los siguientes pasos:

1. Ingrese al sitio de Central Directo y autentíquese[1].
2. Ingrese a la pestaña de Entidades Jurídicas, de clic en el bloque de "Firma Digital" y seleccione una de las siguientes opciones según corresponda:
    - Ingrese en la entidad donde es usuario: Seleccione la entidad que representa.

[1] La persona por autenticarse debe ser el representante legal de la institución o un asistente técnico nombrado por él.

- Suscriba una entidad donde usted es Representante Legal Principal o Autorizado: Si la entidad que representa no se muestra en la opción anterior, ingrese la cédula jurídica de la entidad y siga las indicaciones del asistente.

3. Cree la identidad de marca: Para hacerlo seleccione:
    a. Ir al menú “Firma Digital” -> “GAUDI” -> “Identidad de Marca”



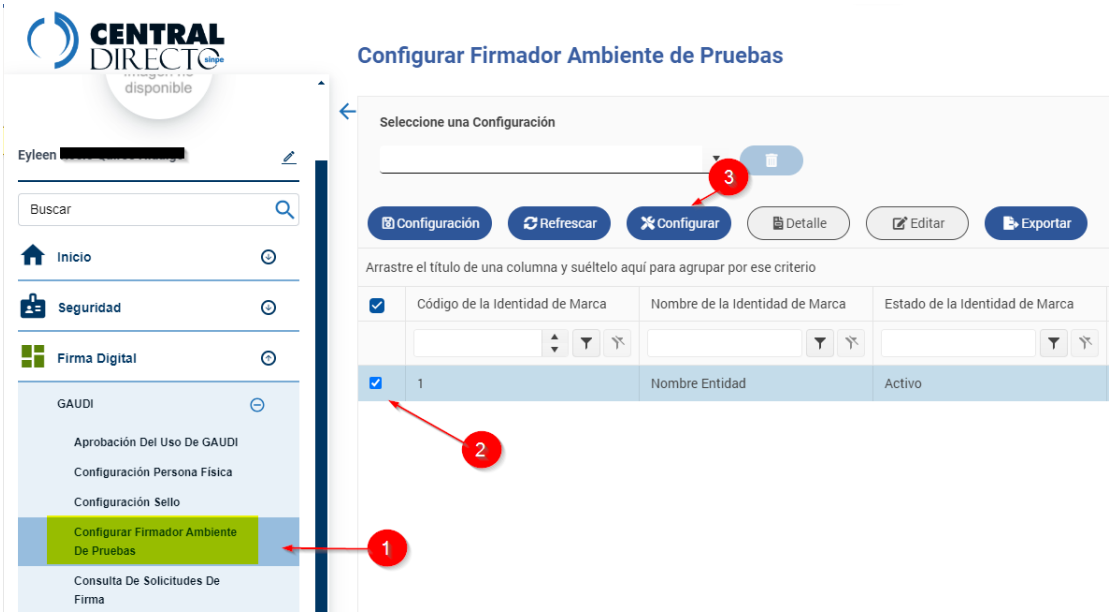
    b. Clic en la acción “Solicitar”, en la ventana siguiente ingrese el nombre y logo[2] deseado

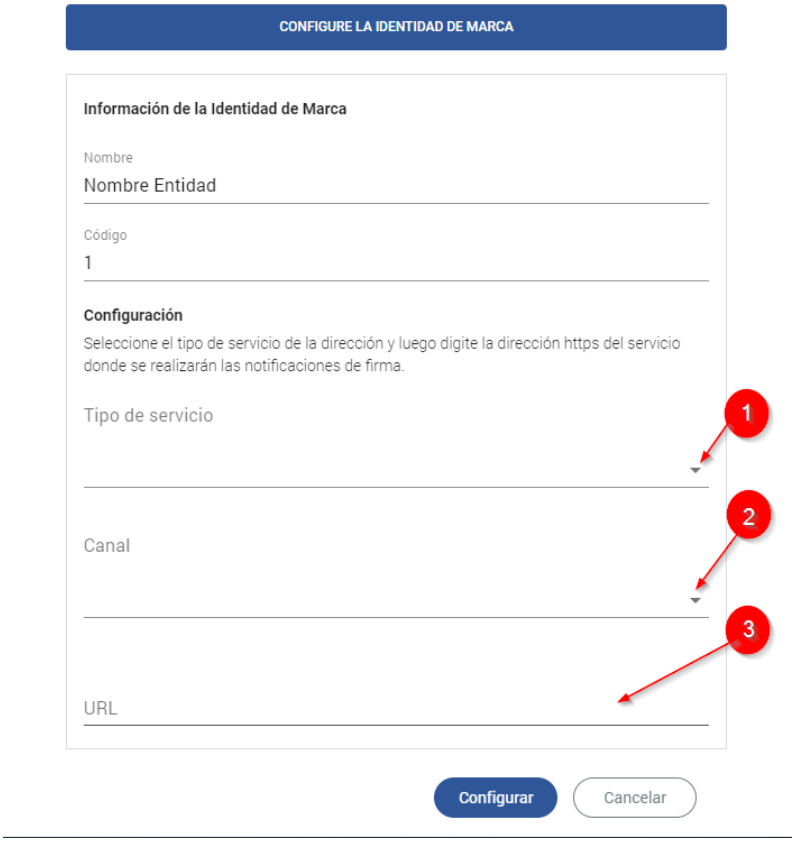
[2] Se permiten logos únicamente de 184 x 84 px

Paso 4: Configure la identidad de marca para el ambiente de pruebas

Para poder consumir los servicios en el ambiente de producción es necesario valorar el desarrollo realizado contra un ambiente de pruebas. Para configurar la identidad de marca realice los siguientes pasos:

a. Configure la identidad de marca creada: Seleccione: “Firma Digital” -> “GAUDI” -> “**Configurar Firmador Ambiente De Pruebas”** y configure la identidad de marca con el canal privado y la URL de notificación del ambiente de pruebas, este URL debe ser en el puerto 443 (https). Favor verifique que el URL funcione en un navegador cargando una página a través del protocolo http “GET”.





Para más información acerca de cómo realizar las firmas en Central Directo, consulte la ayuda en línea de Firma Digital.

Paso 5: Ejecute los escenarios de pruebas

El ambiente de pruebas publica los servicios para firmar **(Web Service y WCF Firmador)** y autenticar **(Web Service y WCF Autenticador)** respetando las interfaces, tipos de datos y mensajes especificados en el estándar electrónico.

La funcionalidad de **FIRMA DIGITAL** de documentos se publica en estos servicios:

- **WCF:**
  https://firmador.fdi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Firmador.svc

- **WS:**
  https://firmador.fdi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Firmador.asmx

La funcionalidad de **AUTENTICACIÓN** con firma digital se publica en estos servicios:

- **WCF:** https://firmador.fdi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Autenticador.svc

- **WS:** https://firmador.fdi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Autenticador.asmx

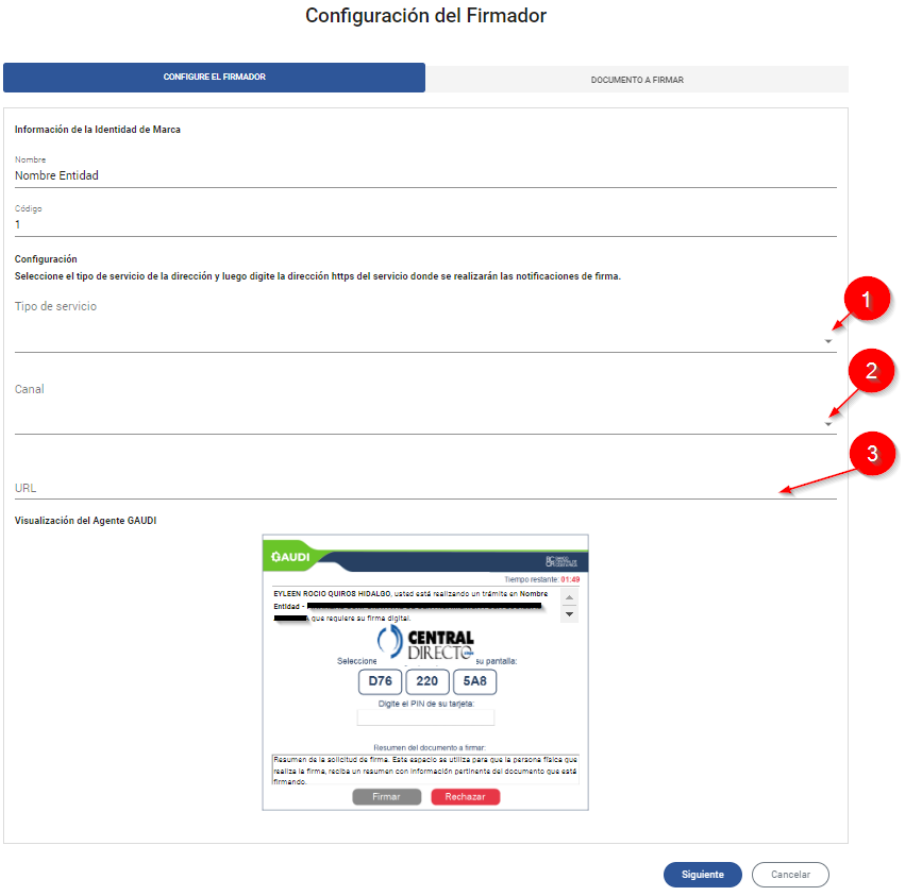
Escenarios de pruebas

La documentación respectiva de los escenarios de pruebas que se deben realizar se encuentra publicada en la sección Documentos complementarios en el archivo **Escenarios del ambiente de pruebas para la funcionalidad de firma y autenticación.**

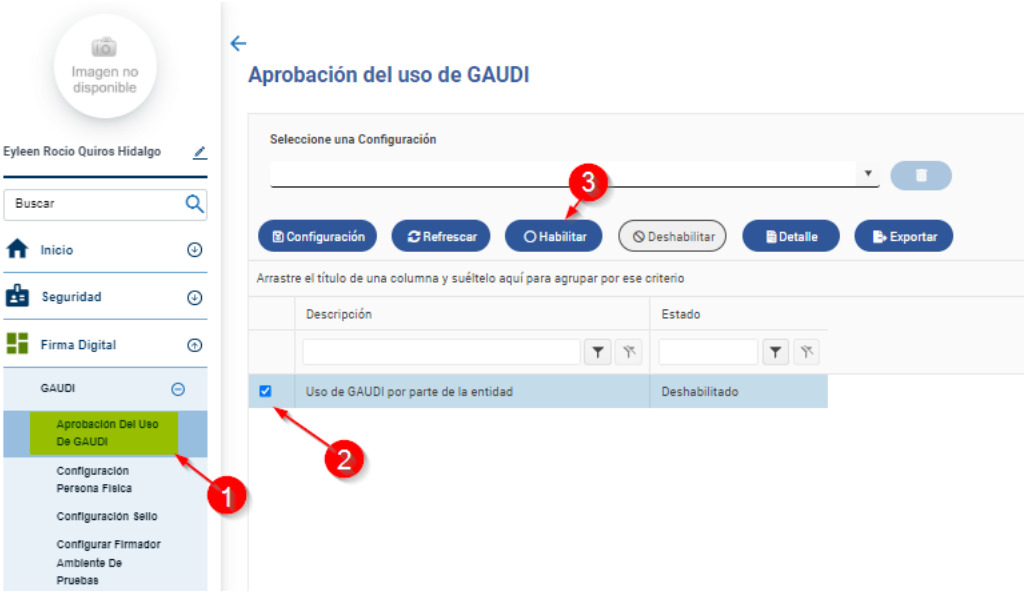
Paso 6: Configure la identidad de marca para el ambiente de producción

Para poder consumir los servicios en el ambiente de producción es necesario configurar la identidad de marca, para eso realice los siguientes pasos:

a. Configure la identidad de marca creada: Seleccione: "Firma Digital" -> "GAUDI" -> "**Configuración Persona Física**" y configure la identidad de marca con el canal privado y la URL de notificación del ambiente de producción, este URL debe ser en el puerto 443 (https). Favor verifique que el URL funcione en un navegador cargando una página a través del protocolo http "GET".

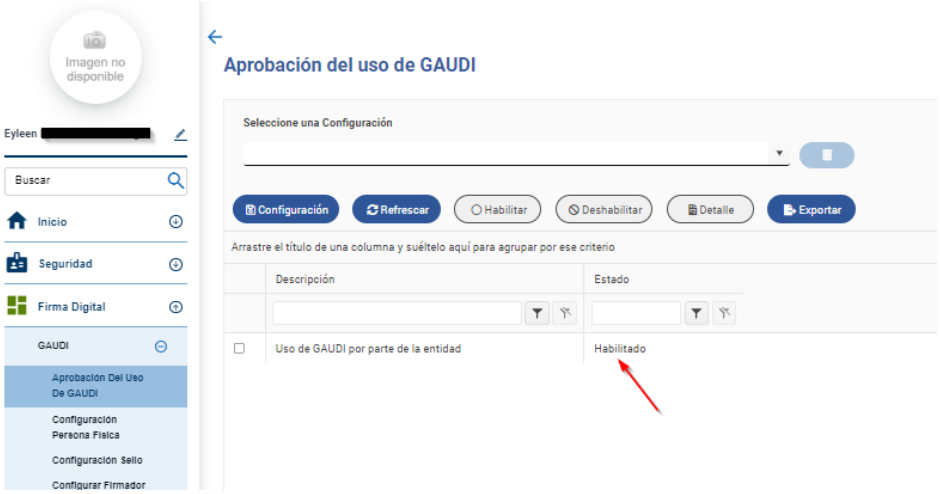


b. Apruebe (habilite) el uso de GAUDI**.** Seleccione: “Firma Digital” -> “GAUDI” -> “**Aprobación del uso de GAUDI**” y habilitar el Uso de GAUDI por parte de la entidad. Esta acción solo la puede llevar a cabo el apoderado legal de la institución nombrado en el sistema.



Fecha de última modificación: 10/Octubre/2024

Verificar que el estado de "**Uso de GAUDI por parte de la entidad**" se encuentra en estado "**Habilitado**".

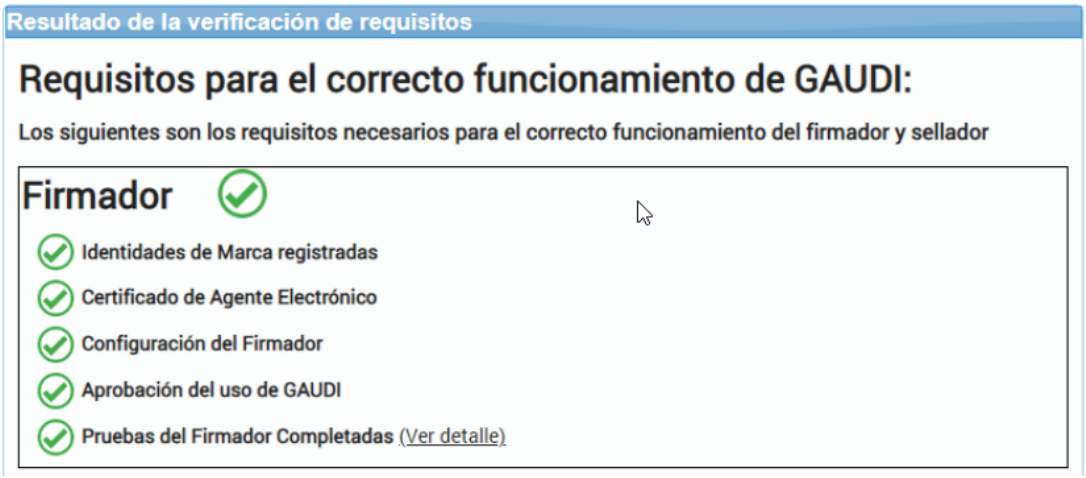


Para más información acerca de cómo realizar las firmas en Central Directo, consulte la [ayuda en línea de Firma Digital].

Fecha de última modificación: 10/Octubre/2024

Paso 7: Verifique los requisitos para utilizar las funcionalidades del firmador

En Central Directo en las opciones de GAUDI se encuentra una opción para verificar los requisitos. Cuando se finalicen las pruebas de manera exitosa es necesario verificar que todos los requisitos se cumplen, una vez que esté todo correcto (en verde) se podrán utilizar las funcionalidades del servicio Firmador en producción. En caso de que usted quiera verificar que requisitos o pruebas que le faltan por cumplir, lo puede realizar en esta sección. Los requisitos que cumplir son los siguientes:



Paso 8: Consuma las funcionalidades del servicio Firmador en Producción

Estos son los servicios de PRODUCCION publicados para firmar **(Web Service y WCF Firmador)** y autenticar **(Web Service y WCF Autenticador).** Se deben respetar las interfaces, tipos de datos y mensajes especificados en el Estándar Electrónico.

Servicio firmador

- **WCF**: https://firmador.fdi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Firmador.svc
- **WS**: https://firmador.fdi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Firmador.asmx

Servicio autenticador

- **WCF**: https://firmador.fdi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Autenticador.svc
- **WS**: https://firmador.fdi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Autenticador.asmx

Anexos

Configuración de los servidores

Se deberán realizar las configuraciones descritas en esta sección, en los servidores de la entidad que publican y consumen las funcionalidades del servicio firmador:

1. Descargue los archivos necesarios para la configuración, estos archivos se encuentran publicados en la sección Documentos complementarios en el archivo **Jerarquía Persona Jurídica Producción para entregar a las entidades externas.**
2. Instale los certificados descargados en los servidores de su entidad en el almacén de certificados correspondiente para cada certificado.
3. Ejecute la **Guía para validar los CRLs de certificados de la jerarquía del ambiente de producción del firmador** que se encuentra publicada en la sección Documentos complementarios. La ejecución de esta guía garantiza que se tiene acceso a los CRLs en el ambiente de producción.
4. En el archivo **hosts** del servidor o los servidores desde donde se interactuará con el servicio Firmador, se debe registrar:
    - ✓ El nombre **firmador.fdi.cr** asociada a la IP de la cual fue entregada por el área de atención al cliente de Banco Central.
5. En el archivo host del servidor o los servidores desde donde recibirán las notificaciones, se debe registrar los datos brindados por el área de atención al cliente de Banco Central:
    - ✓ El nombre **ocsp.sinpe.fi.cr** asociada a la IP de la cual fue entregada.
    - ✓ El nombre **fdi.sinpe.fi.cr** asociada a la IP de la cual fue entregada.
    - ✓ El nombre **www.firmadigital.go.cr** asociada a la IP de la cual fue entregada.
6. Habilitar los accesos de telecomunicaciones, como se describe en la siguiente tabla:

Desde	Hacia	Puerto
Entidad	firmador.fdi.cr (#.#.#.38)	443
orosi.fdi.cr (#.#.#.36)	Entidad	443
tenorio.fdi.cr (#.#.#.37)	Entidad	443
Entidad	ocsp.sinpe.fi.cr (#.#.#.28)	80
Entidad	fdi.sinpe.fi.cr (#.#.#.28)	80
Entidad	www.firmadigital.go.cr (#.#.#.8)	80

7. Verificar los accesos que se abrieron en el paso anterior.
    a. Esta verificación se debe realizar desde los servidores donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el **Firmador.** Se debe abrir una consola del

sistema y ejecutar un "**telnet**" a las siguientes IP´s y puertos para garantizar que el acceso se encuentre abierto.

Desde	Hacia	Puerto
Entidad	firmador.fdi.cr (#.#.#.38)	443
Entidad	ocsp.sinpe.fi.cr (#.#.#.28)	80
Entidad	fdi.sinpe.fi.cr (#.#.#.28)	80
Entidad	www.firmadigital.go.cr (#.#.#.8)	80

b. Verificar que se puede validar el estado de revocación de un certificado, para esto ejecutar la "**Guía para validar los CRLs de certificados de la jerarquía del ambiente de producción del firmador**", la ejecución de esta guía garantiza que se tiene acceso a los CRLs en el ambiente de producción.

Publicar el servicio de notificaciones

1. La implementación de este servicio es indispensable para que la entidad pueda recibir los resultados de las solicitudes de firma de documentos y de autenticación de personas físicas.
    1. El servicio de notificación **debe** estar asegurado con el certificado de agente electrónico de la entidad.
    2. Por cada "**Identidad de Marca**" usted debe tener un servicio de notificación.
    3. El servicio de notificación debe estar publicado en un sitio que respete el siguiente formato:
        - https://notificacionserviciogaudi[consecutivo].[dominiodelaentidad]/[rutadelservicio]
        - Por ejemplo:
            - https://notificacionserviciogaudi1.bancodummy.com/Servicio/Resultado.svc/
    4. En caso de que tenga varios sitios de notificación para diferentes identidades de marca, también estos sitios deben tener el mismo formato a nivel del nombre del host, pero con diferente consecutivo. Por ejemplo:
        - https://notificacionserviciogaudi2.bancodummy.com/
        - https://notificacionserviciogaudi3.bancodummy.com/
        - https://notificacionserviciogaudi4.bancodummy.com/
        - …

5. El servidor o clúster de servidores que hospeda el servicio de notificaciones no precisamente tiene que llamarse: **notificacionserviciogaudi1**, sin embargo, si debe existir una entrada en el DNS interno para que resuelva a la dirección IP del servidor o del clúster respectivo.

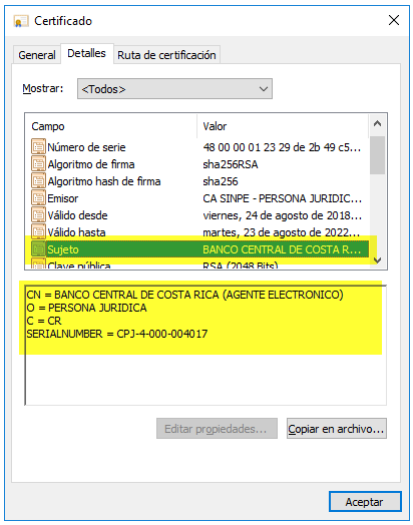
6. El servicio de notificación **deberá** implementarse siguiendo las interfaces, tipos de datos y mensajes especificados en el estándar electrónico en la sección **Servicios Publicados por las Entidades**, consulte los **Archivos WSDL (Firmador, Autenticador, Verificador y ResultadoDeSolicitud) tipo WCF para entregar a las entidades externas**, que se encuentran publicados en la sección Documentos complementarios.
    - Debe estar preparado para manejar archivos de hasta 20 megas.
    - Particularmente la clase "**ResultadoDeFirma**" debe tener el NameSpace "**Bccr.Firma.Fva.Entidad.Contenedores**".
    - Además, el método "**NotifiqueLaRespuesta**", debe recibir un parámetro llamado "**elResultado**" de tipo "**ResultadoDeFirma**" (se debe respetar el nombre del parámetro).

```
<ServiceContract()>
0 references
Public Class ResultadoDeSolicitud
    <OperationContract()>
    0 references
    Public Sub NotifiqueLaRespuesta(elResultado As ResultadoDeFirma)
```

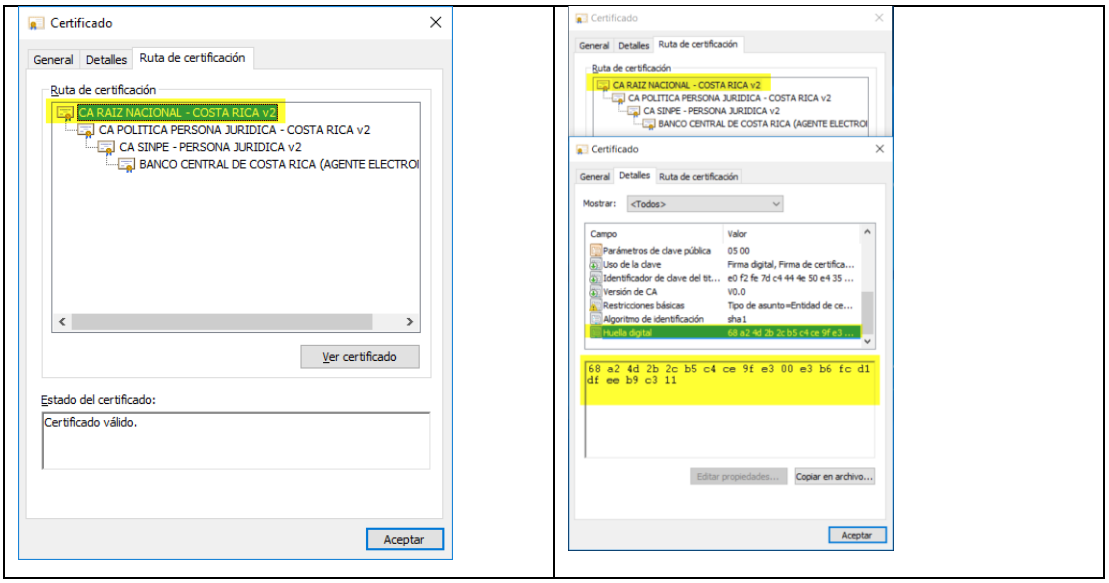
7. El servicio de notificación **puede** ser utilizado para notificar a una o varias identidades de marca.
8. Recomendamos revisar el documento **Base de datos de conocimiento de la configuración de los servicios** que se encuentra publicado en la sección Documentos complementarios. Este documento contiene información que hemos recolectado de la experiencia de otras instituciones conectándose a las funcionalidades del servicio firmador
    - Si el servicio de notificación va a ser publicado en un servidor web IIS es necesario verificar el punto #14 del documento de base de datos.
    - Si requiere habilitar el uso de TLS 1.2 es necesario verificar el punto #14 del documento de base de datos.

9. El servicio de notificación de la entidad **debe** garantizar que sólo puede ser consumido con el certificado de agente electrónico que el Banco Central de Costa Rica tiene para ese efecto. En particular, dicho certificado debe:

   - Tener el sujeto: “CN=BANCO CENTRAL DE COSTA RICA (AGENTE ELECTRONICO), O=PERSONA JURIDICA, C=CR, SERIALNUMBER=CPJ-4-000-004017”. Al realizar la validación, respetar las mayúsculas y el espacio después de cada coma (,).



   - La huella del **certificado raíz de la jerarquía** a la que pertenece el certificado de agente del BCCR, debe ser la siguiente “68A24D2B2CB5C4CE9FE300E3B6FCD1DFEEB9C311”. Al realizar la validación la huella debe ir en mayúsculas y sin espacios.



   - Debe validarse que sea vigente y no haya sido revocado.

Instalar certificado de agente electrónico de su entidad

El certificado de agente electrónico que se generó para asegurar el sitio de su entidad debe instalarse en los servidores, puede seguir los siguientes pasos:

1. Cargue una consola del sistema y diríjase a la carpeta donde se encuentra la llave pública del certificado de agente electrónico, este archivo tiene extensión ".cer".
2. Ejecute el comando "C:\WINDOWS\System32\certreq –accept *{nombreDelCertificado}*.cer"
3. Verifique en el store de certificados (personal o de maquina) o en HSM (dependiendo del proveedor criptográfico utilizado) que se generó la llave privada del certificado de agente electrónico.