BANCO CENTRAL DE COSTA RICA

FIRMADOR, VALIDADOR Y AUTENTICADOR

NORMA TÉCNICA

CONFIGURACIÓN DE GAUDI PARA EL SERVICIO FIRMADOR PARA PERSONA FÍSICA CANAL PÚBLICO

Público

NT-FVA

Tabla de Contenido

1. Introducción 2
2. Prerequisitos 2
3. Términos empleados 2
4. Paso 1: ¿Qué necesito antes de iniciar la configuración de las funcionalidades del servicio Firmador? 3
5. Paso 2: Cree la identidad de marca 4
6. Paso 3: Configure la identidad de marca para el ambiente de pruebas 6
7. Paso 4: Ejecute los escenarios de PRUEBAS 8
8. Paso 5: Configure la identidad de marca para el ambiente de producción 10
9. Paso 6: Verifique los requisitos para utilizar las funcionalidades del firmador 12
10. Paso 7: Consuma las funcionalidades del servicio Firmador en Producción 13
11. Anexos 15

Configuración de los servidores 15

Publicar el servicio de notificaciones 15

Instalar certificado de agente electrónico de su entidad 18

1. Introducción

El propósito de este documento es facilitar la puesta en marcha en el **AMBIENTE DE PRODUCCIÓN**, de los servicios web que consumen las funcionalidades de GAUDI, provisto por el Banco Central de Costa Rica por medio de INTERNET.

Este documento permite a los departamentos de informática de cada Suscriptor, verificar el estado de sus sistemas internos e identificar los ajustes necesarios para evitar contratiempos en la implementación del firmador GAUDI en personas físicas.

2. Prerequisitos

- Validar la funcionalidad a usar. Las funcionalidades están disponibles en la página Funcionalidades Disponibles GAUDI
- Tener conocimientos básicos de certificados digitales e infraestructura de llave pública.
- Tener conocimientos de programación y consumo de servicios Web como WFCs, WebServices y servicios tipo API REST.
- Conocimiento en la Norma Técnica - Estándar Electrónico GAUDI, pues acá se describen los posibles métodos a usar en el servicio.

3. Términos empleados

- Para los fines del presente documento, se entenderá por:
  - ⊡ BCCR: Banco Central de Costa Rica.
  - ⊡ GAUDI: Gestor de Autenticaciones y Firmas Digitales del Banco Central.
  - ⊡ Suscriptor: Entidad que desea implementar el uso de los servicios de firma digital GAUDI.
  - ⊡ Identidad de marca: Se entiende por identidad de marca un portal web 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 al sitio “Central Directo” y los portales de las superintendencias (SUGEF, SUGESE y SUGEVAL). Otro ejemplo: la empresa “Banco Alianza de Costa Rica S.A.” podría tener una identidad de marca para su sitio https://www.bancoalianza.fi.cr/ que se llame “Portal Banco Alianza” y otra identidad de marca para gestionar las firmas de su APP llamada “Banca Móvil Alianza”, si es que dicho APP también va a usar los servicios de Firma Digital. Bajo este escenario, así se vería la identidad de marca (marcada “en amarillo”) para las solicitudes de firma que dicha entidad haga hacia sus usuarios finales:



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

a. **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. El certificado de agente electrónico solo puede ser gestionado por el representante legal de la entidad, si desea ver más detalles sobre este requerimiento puede revisarlo en este enlace.
   Para consumir los servicios de GAUDI tanto en el ambiente de pruebas como en Producción, es necesario asegurar la comunicación con el certificado de PRODUCCIÓN de Agente Electrónico de la entidad. **Con el mismo certificado se consumen los servicios en los dos ambientes, NO se necesita un certificado de Agente Electrónico del ambiente de pruebas**.

b. **Solicitud de habilitación de accesos hacia los servicios de notificación de la entidad:** Posterior a disponer de un certificado de agente electrónico y con el fin de que la plataforma del BCCR pueda comunicarse correctamente con los servicios de notificación de la entidad, deberá gestionarse la habilitación de los accesos de red requeridos desde el BCCR hacia los servidores de la entidad que hospedan dichos servicios.
   Para esta gestión, la entidad deberá proporcionar el o los nombres de dominio completos (FQDN - Fully Qualified Domain Name) asociados a los servicios de notificación que serán utilizados para la integración.
   Consideraciones importantes:
   - Los nombres de dominio suministrados deben corresponder a un **FQDN completo y específico**.

- No se aceptarán solicitudes que incluyan **comodines (wildcards)** en los nombres de dominio, por ejemplo:
  - No se acepta: ***.entidad.com** o ***.qa.entidad.com**
  - Se acepta: **notificaciongaudi1.entidad.com** o **api.entidad.com**
- En caso de requerirse acceso a múltiples servicios o ambientes, deberá suministrarse cada FQDN de forma individual.
- La habilitación de estos accesos deberá ser solicitada mediante la apertura de un caso formal ante los canales definidos por el BCCR en el sitio de atención al ciudadano para el servicio de firma digital.
- La aprobación y configuración de los accesos estará sujeta a la validación de las políticas de seguridad vigentes.

c. **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 el 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.

d. **Un sitio público configurado en donde el servicio de la entidad va a consumir las funcionalidades del servicio Firmador y además se le van a hacer notificaciones**: Este sitio público va a ser el encargado de solicitar las firmas y autenticaciones; además el servicio Firmador GAUDI 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".

5. Paso 2: Cree la identidad de marca

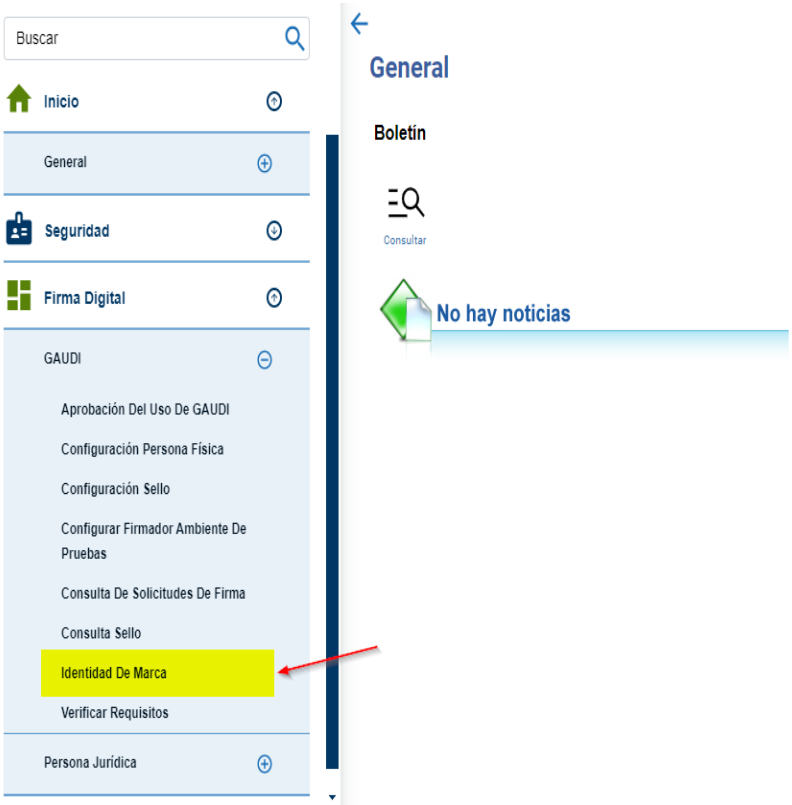
Para crear la identidad de marca realice los siguientes pasos:

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:
   a. Ingrese en la entidad donde es usuario: Seleccione la entidad que representa.
   b. 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.

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



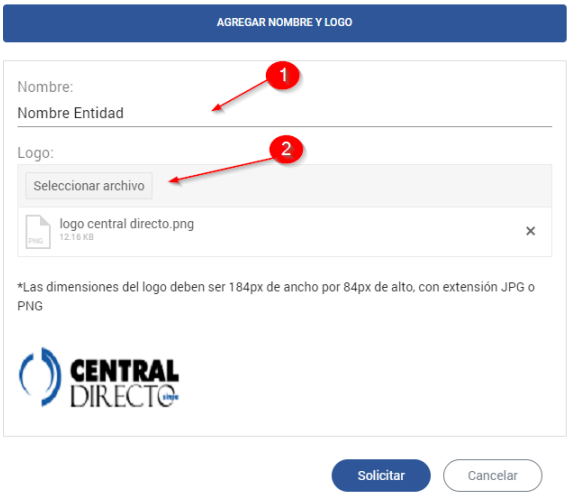
3. Cree la identidad de marca: Para hacerlo seleccione:
   a. Ir al menú "**Firma Digital**" -> "**GAUDI**" -> "**Identidad de Marca**"



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



Solicitar identidad de marca

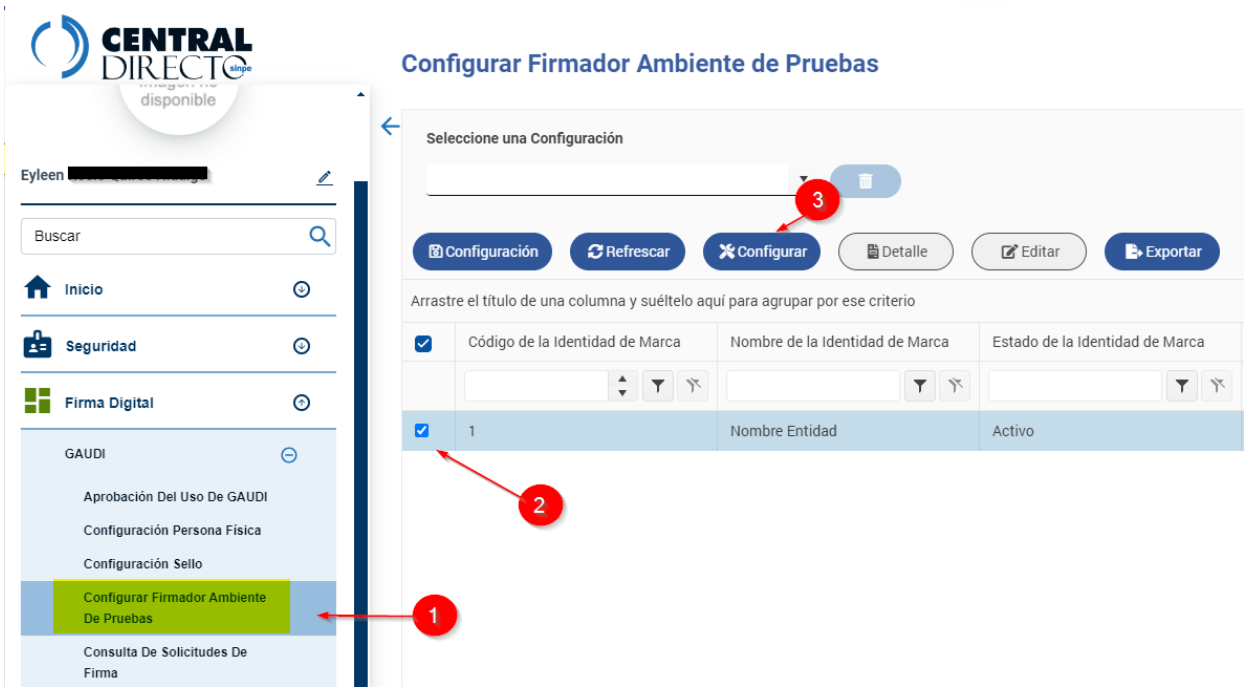


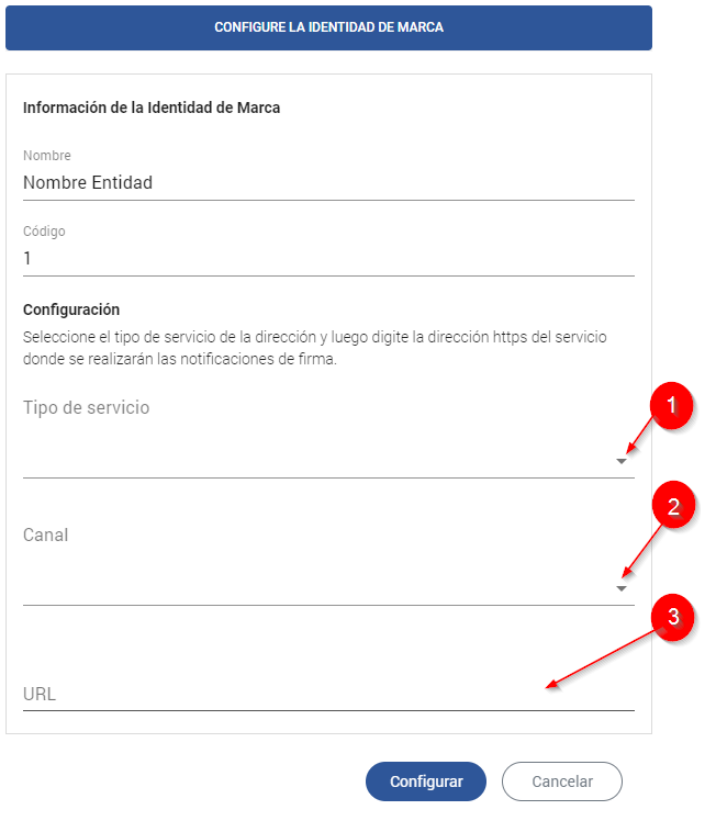
6. Paso 3: Configure la identidad de marca para el ambiente de pruebas

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 público y la URL de notificación del ambiente de pruebas, este URL debe ser en el puerto 8443. Favor verifique que el URL funcione en un navegador cargando una página a través del protocolo http “GET”. **Se aclara que, para poder incluir el URL de esta identidad de marca, se debe tener listo el servicio de notificaciones asegurado con el certificado de Agente Electrónico de su entidad.** (Paso 1.d). Este paso va a intentar validar el acceso a dicho URL y si no estuviera listo no se va a poder configurar.

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





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

7. Paso 4: Ejecute los escenarios de PRUEBAS

Para poder iniciar con las pruebas, se debe de tener configurado el sitio que hace las peticiones, el servicio que recibe las notificaciones y adicionalmente configurada la identidad de marca de pruebas en Central Directo. El ambiente de pruebas de su entidad debe estar desarrollado respetando las interfaces, tipos de datos y mensajes especificados en el estándar electrónico, según sea su tipo de consumo (**Web Service, WCF Autenticador y API REST**).

La funcionalidad de **FIRMA DIGITAL** de documentos se publica en los siguientes servicios, cuya documentación detallada sobre como consumir se puede encontrar en este sitio Documentos complementarios :

WCF:

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Firmador.svc

WS:

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Firmador.asmx

API: (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.AmbienteDePruebas.Entidades.FirmarDocumento.API

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

- **WCF**:

  https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Autenticador.svc

- **WS**:

  https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Autenticador.asmx

- **API:** (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

  https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.AmbienteDePruebas.Entidades.Autenticar.API

La funcionalidad de **ADMINISTRACIÓN DE SOLICITUDES** se publica en estos servicios:

- **WCF**:

  https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/ConsultanteAccesibilidad.svc

  https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/ConsultanteInformacionSuscriptor.svc

  https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/CanceladorSolicitudSuscriptor.svc

- **WS**:

  https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/ConsultanteAccesibilidad.asmx

  https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/ConsultanteInformacionSuscriptor.asmx

  https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/CanceladorSolicitudSuscriptor.asmx

- **API:** (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

  https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.AmbienteDePruebas.Entidades.AdminSolicitudes.API

Escenarios de pruebas

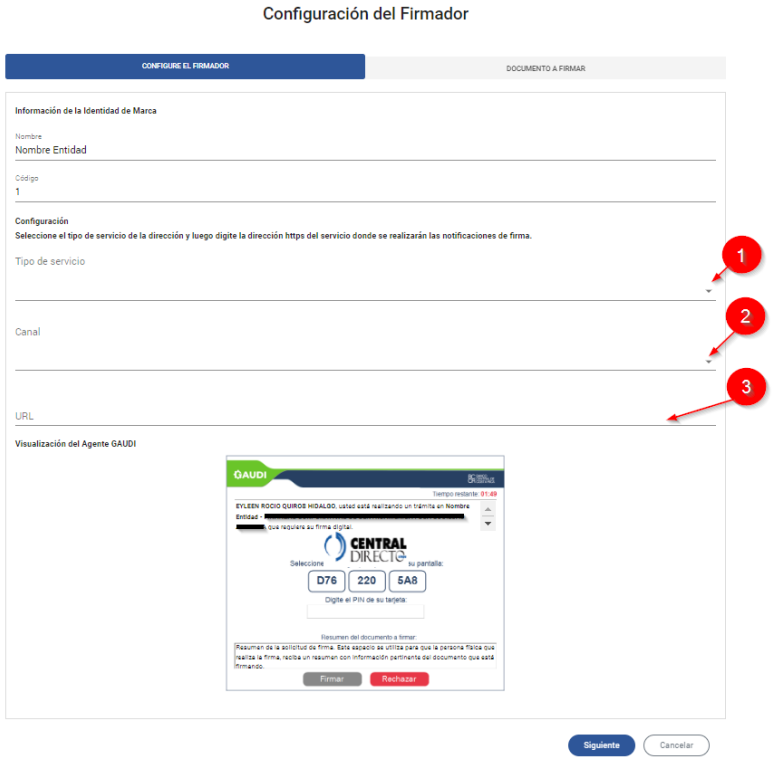
- La documentación respectiva de los escenarios de pruebas que se deben realizar se encuentra publicada en la sección Documentos complementarios en el archivo Escenarios del ambiente de pruebas para la funcionalidad de firma y autenticación**.**

8. Paso 5: 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:

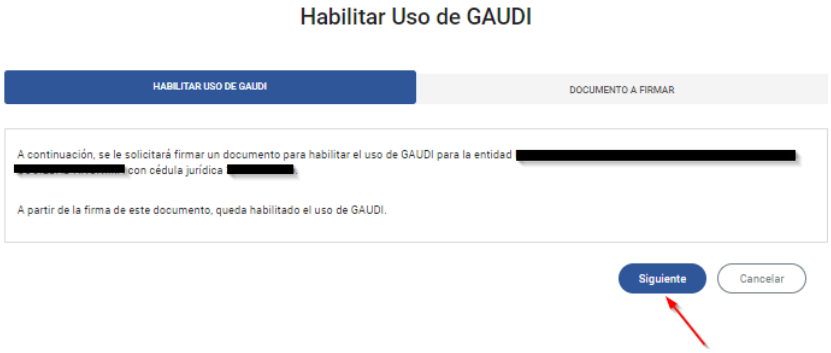
a. Configure la identidad de marca creada: Seleccione: “Firma Digital” -> “GAUDI” -> “**Configuración Persona Física**” y configure la identidad de marca con el canal público y la URL de notificación del ambiente de producción, este URL debe ser en el puerto 8443. Favor verifique que el URL funcione en un navegador cargando una página a través del protocolo http “GET”.

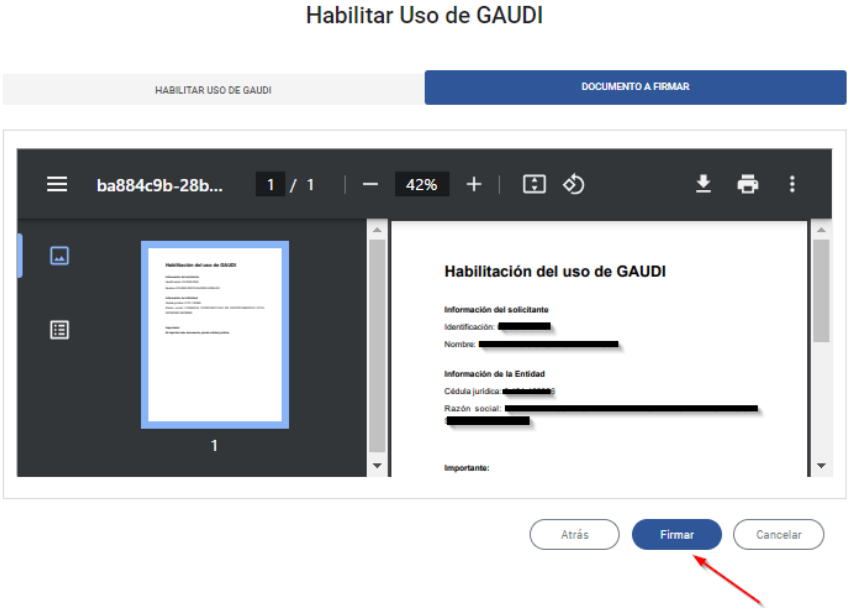




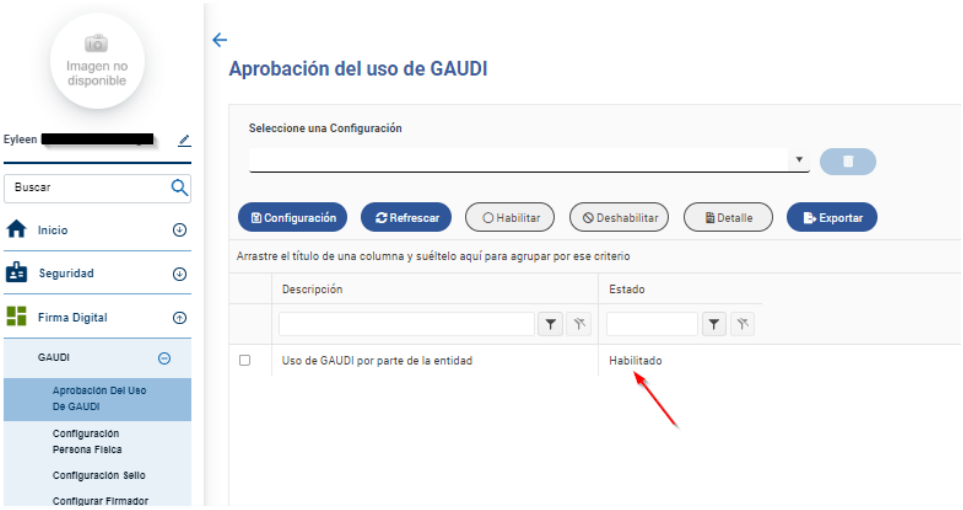
b. Apruebe (habilite) el uso de GAUDI**.** Seleccione: “Firma Digital” -> “GAUDI” -> “**Aprobación del uso de GAUDI**” y habilitar el Uso de GAUDI por parte de la entidad. Esta acción solo la puede llevar a cabo el apoderado legal de la institución nombrado en el sistema.







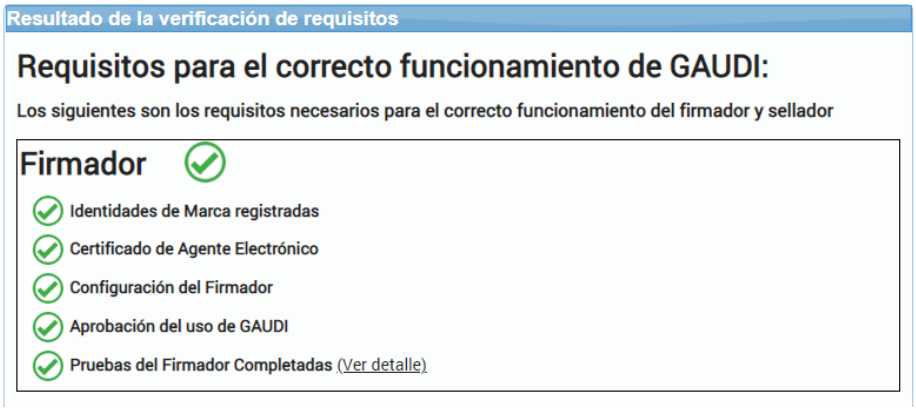
Verificar que el estado de "**Uso de GAUDI por parte de la entidad**" se encuentra en estado "**Habilitado**".



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

9. Paso 6: 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:



10. Paso 7: Consuma las funcionalidades del servicio Firmador en Producción

Los servicios con los que cuenta el Firmador se encuentran desarrollados utilizando tecnologías Web Service o WCF o API REST. El ambiente de **PRODUCCION** de su entidad debe estar desarrollado respetando las interfaces, tipos de datos y mensajes especificados en el estándar electrónico, según sea su tipo de consumo (**Web Service, WCF Autenticador y API REST**).

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

- **WCF**:

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Firmador.svc

- **WS**:

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Firmador.asmx

- **API:** (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.Entidades.FirmarDocumento.API/

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

- **WCF**:

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Autenticador.svc

- **WS**:

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Autenticador.asmx

API: (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

- https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.Entidades.Autenticar.API/

La funcionalidad de **ADMINISTRACIÓN DE SOLICITUDES** se publica en estos servicios:

- **WCF**:

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/ConsultanteAccesibilidad.svc

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/ConsultanteInformacionSuscriptor.svc

https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/CanceladorSolicitudSuscriptor.svc

- **WS**:

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/ConsultanteAccesibilidad.asmx

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/ConsultanteInformacionSuscriptor.asmx

https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/CanceladorSolicitudSuscriptor.asmx

- **API**: (En el caso del servicio API para visualizar la documentación de los métodos descargar el archivo)

https://servicios-rest-firmador.gaudi.sinpe.fi.cr/FVA/Bccr.Firma.Fva.Entidades.AdminSolicitudes.API/

11. 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 del 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. Para consumir los servicios de GAUDI, consulte los Archivos WSDL (Firmador, Autenticador, Verificador y ResultadoDeSolicitud) tipo WCF para entregar a las entidades externas, o Archivos OpenAPI-JSON(Servicio GAUDI Persona Física) tipo API para entregar a las entidades externas, estos archivos se encuentran publicados en la sección Documentos complementarios.
3. Instale los certificados descargados en los servidores de su entidad en el almacén de certificados correspondiente para cada certificado.
4. 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.

Publicar el servicio de notificaciones

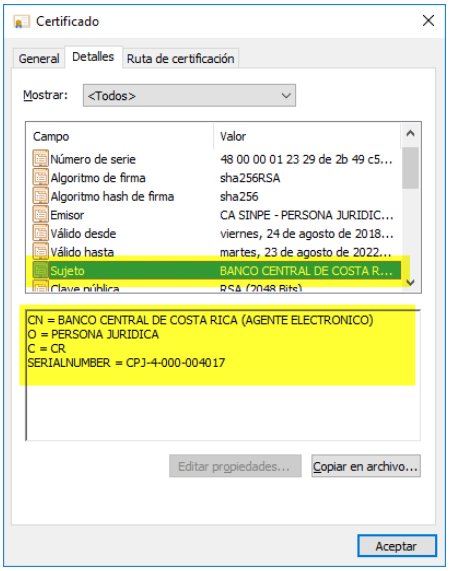
1. La implementación de este servicio es indispensable para que la entidad pueda recibir los resultados de las solicitudes de firma de documentos y de autenticación de personas físicas.
    - El servicio de notificación **debe** estar asegurado con el certificado de agente electrónico de la entidad.
    - El servicio debe ser publicado por el puerto 8443.
    - Por cada "**Identidad de Marca**" usted debe tener un servicio de notificación.
    - 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/
    - 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/
        - …

- 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.
- 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, o Archivos OpenAPI-JSON(Servicio GAUDI Persona Física) tipo API 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).

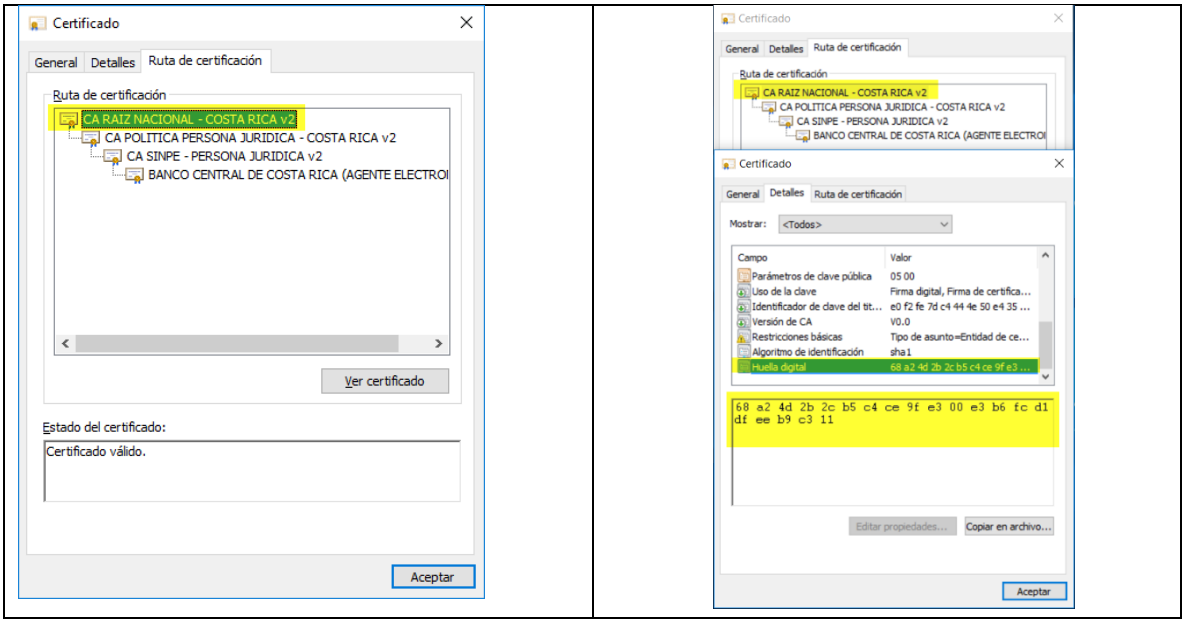
```
<ServiceContract()>
0 references
Public Class ResultadoDeSolicitud
    <OperationContract()>
    0 references
    Public Sub NotifiqueLaRespuesta(elResultado As ResultadoDeFirma)
```

- El servicio de notificación **puede** ser utilizado para notificar a una o varias identidades de marca.
- Recomendamos revisar el documento Base de datos de conocimiento de la configuración de los servicios que se encuentra publicado en la sección Documentos complementarios.
  - Si el servicio de notificación va a ser publicado en un servidor web IIS es necesario verificar el punto: "Solución al error The remote server returned an unexpected response: (413) Request Entity Too Large", cuando aparece en el trace del WCF o en la bitácora central del Sinpe, en el servicio de notificación" en dicho documento de la base de conocimiento.
  - Si requiere habilitar el uso de TLS 1.2 es necesario verificar el punto "Configuración para que la aplicación utilice TLS 1.2" de dicho documento.

- 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, sea 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 personal de certificados o en HSM (dependiendo del proveedor criptográfico utilizado) que se visualiza **el ícono de la llave privada** del certificado de agente electrónico.

