

Sandbox Tecnológico ATENA

Sistema de Finanzas Abiertas

Esta guía tiene por objetivo acompañar a las entidades participantes del Sistema de Finanzas Abiertas (SFA) durante su proceso de habilitación en el Sandbox Tecnológico ATENA, proporcionando una ruta práctica para preparar su ingreso, configurar los componentes necesarios y ejecutar pruebas correspondientes.

A través de los siguientes pasos podrá identificar los principales componentes del proceso de onboarding, conocer las acciones que debe realizar su institución para operar en el ambiente de pruebas y acceder directamente a la documentación y material de apoyo necesarios para cada etapa, disponibles en el Portal del Desarrollador de Finanzas Abiertas¹.

Flujo de incorporación y uso del Sandbox

- 1 Conocer el ecosistema y las especificaciones del SFA
- 2 Marco técnico de seguridad
- 3 Solicitar la habilitación de su institución en el Sandbox
- 4 Configurar la información de su institución en el directorio de pruebas
- 5 Ejecutar las pruebas
- 6 Registrar evidencias, incidencias y resultados

1 Conocer el ecosistema y las especificaciones del SFA

Previo a comenzar la configuración técnica, es recomendable que cada participante identifique el rol que desempeñará dentro del SFA y revise las especificaciones aplicables para implementar los distintos componentes e interacciones con el Sandbox ATENA.

La sección “Especificaciones de Integración y Operación” del Portal de Desarrollador, describe las pautas técnicas y operativas necesarias para la integración de los participantes del SFA de acuerdo al rol con el que participa en el SFA:

Institución Proveedora de Información (IPI)	Institución Proveedora de Cuentas (IPC)	Prestador de Servicios Basados en Información (PSBI)	Prestador de Servicios de Iniciación de Pagos (PSIP)
Bancos y emisores de tarjetas de crédito, tarjetas de pago con provisión de fondos o de cualquier otro sistema similar que se encuentren autorizados por la CMF.	Banco o institución financiera proveedora de cuentas corrientes, cuentas vista o cuentas de provisión de fondos.	Proveedores de servicios habilitados por información financiera, con el fin de consultar, acceder y recibir datos para efectos de proveer servicios a los clientes.	Entidades que pueden instruir, a nombre de un cliente, la ejecución de órdenes de pago o transferencias electrónicas de fondos, incluyendo pagos recurrentes, con cargo a sus respectivas cuentas y medios de pago.

1/ Portal del Desarrollador: <https://openfinancechile.atlassian.net/wiki/spaces/OFAC/overview?homepageId=12222466>

Link:  [Especificaciones de Integración y Operación](#)

2 Marco técnico de seguridad

La seguridad es uno de los pilares fundamentales del SFA. Para garantizar un intercambio de información confiable, interoperable y seguro, la NCG514 y el Portal del Desarrollador establecen un conjunto de especificaciones técnicas que definen los principales mecanismos y estándares que deben considerar los participantes del ecosistema, incluyendo autenticación, autorización, identificación y protección de las comunicaciones. Las pruebas deben considerar tanto flujos exitosos como escenarios de error, permitiendo verificar que las solicitudes válidas sean procesadas correctamente y que aquellas que no cumplan con las condiciones establecidas sean rechazadas de acuerdo con las especificaciones del SFA.

Para orientar la configuración y ejecución de estos flujos, se establece un conjunto de especificaciones que conforman el marco técnico de seguridad del SFA. Estas definen los estándares, mecanismos y requisitos que deben considerar los participantes durante sus pruebas, permitiendo validar su correcta implementación e interoperabilidad dentro del ecosistema.

Entre las principales especificaciones que deberán considerarse según los flujos, se encuentran:
• Perfil de seguridad del SFA • Rich Authorization Request (RAR) • Grant Management • Dynamic Client Registration (DCR) • Directrices para firma digital de mensajes y payloads • Especificaciones de Webhooks • Gestión de certificados en el SFA

Estas especificaciones permiten que todas las instituciones implementen un modelo de seguridad común, facilitando una integración consistente y la correcta ejecución de las pruebas en el Sandbox Tecnológico ATENA.

Link:  [Especificaciones de Seguridad](#)

3 Solicitar la habilitación en el Sandbox Tecnológico ATENA

Para participar en el Sandbox ATENA, la institución debe encontrarse habilitada para operar dentro del entorno de pruebas.

La solicitud se realiza a través del siguiente link, el cual además estará disponible en la página web de la CMF:

Link:  [Link a formulario](#)

4 Configurar la información de su institución en el directorio de pruebas

Una vez habilitado el acceso al Sandbox ATENA, el usuario administrador de la institución deberá completar la información correspondiente a su organización, incorporando los antecedentes necesarios para su correcta habilitación y operación. Además, podrá crear y gestionar nuevos usuarios para su institución, permitiendo que accedan y participen en las actividades requeridas para la ejecución de las pruebas.

Antecedentes que completar por la institución en el Sandbox, previo a las pruebas:
• URL de Webhook para notificaciones en el sistema • Certificado digital para firma y encriptación. En el caso del sandbox ATENA, estos certificados serán autofirmados • Declaraciones de software (en el caso de las PSBI y PSIP) • Servidores de autorización y declaración de APIs (en el caso de las IPI e IPC)

Link:  [Generación de certificados](#)

5 Ejecutar las pruebas

5.1 Pruebas de integración al Directorio mediante APIs

Una vez configurada la institución y sus componentes en el Directorio de pruebas, los participantes deberán validar su correcta integración mediante las APIs y herramientas disponibles para este ambiente.

Para facilitar este proceso, el Portal del Desarrollador dispone de una colección Postman del Directorio de Participantes, que permite ejecutar los flujos necesario para validar la autenticación y obtener los elementos técnicos requeridos para continuar con las pruebas.

La colección Postman permite ejecutar las pruebas de integración en tres pasos principales:	
Prueba	Lo que permite validar
1. Crear Token del Participante	Permite obtener un access_token mediante el flujo Client Credentials y validar la autenticación del participante para acceder a las APIs del Directorio.
2. Obtener el JWKS	Permite obtener las claves públicas asociadas a la Declaración de Software y validar su disponibilidad para la verificación de firmas y los flujos de confianza entre participantes.
3. Obtener el SSA	Permite obtener el Software Statement Assertion (SSA) emitido y firmado por el Directorio, insumo necesario para procesos como Dynamic Client Registration (DCR) y el establecimiento de relaciones de confianza entre participantes.

Adicionalmente, el Directorio dispone de APIs públicas que permiten realizar pruebas de descubrimiento y consultar la información necesaria para la interoperabilidad entre los participantes, incluyendo organizaciones, servidores de autorización, recursos API y sus respectivos endpoints.

Link:  [Uso de colección Postman Directorio Participantes](#)

5.2 Pruebas de consumo de APIs de la Entidad Financiera Simulada (EFS)

En el Sandbox ATENA se dispone de una Entidad Financiera Simulada (EFS) que emula el comportamiento de un participante del SFA, permitiendo la ejecución controlada de pruebas de integración, autenticación y consumo de APIs, conforme a los estándares y lineamientos definidos por CMF.

El Sandbox ATENA dispone de las siguientes APIs:		
APIs de Open Data	APIs de Productos y Transacciones	APIs de Iniciación de Pagos
Información pública sobre productos y servicios financieros	Información financiera custodiada por las instituciones participantes	Permiten iniciar órdenes de pago desde las cuentas de los clientes
Información pública de productos y servicios financieros (sin consentimiento): • Términos y condiciones generales • Canales de atención	Información financiera del cliente y servicios asociados (con consentimiento): • API Cuentas • Enrolamiento • Tarjetas de Crédito • Operaciones de Crédito • Servicio de Operación de Tarjetas de Pago • Recursos • Instrumentos de Inversión • Pólizas de Seguros	Servicios asociados a la iniciación de pagos (con consentimiento): • Pago único inmediato • Pago único programado • Pago recurrente con Monto Fijo • Pago recurrente con Monto Variable • Confirmación de Fondos

Link:  [Especificaciones APIs Open Finance](#)

Y permite ejecutar pruebas controladas de:

- [Integración](#)
- [Autenticación](#)
- [Autorización](#)
- [Certificados](#)
- [Consumo de APIs](#)
- [Flujos funcionales y técnicos](#)

La documentación disponible en el Portal del Desarrollador incluye:

- Manual de consumo de APIs
- Recursos para generación de certificados
- Ambiente Postman
- Colecciones Postman de Open Data
- Colecciones de Productos y Transacciones
- Colecciones de Iniciación de Pagos
- Validación de firma x-jws-signature
- Dynamic Client Registration (DCR)
- Pushed Authorization Requests (PAR)
- Set de pruebas

Link:  [Documentación Entidad Financiera Simulada](#)

6 Registrar evidencias, incidencias y resultados

Durante la ejecución de las pruebas es importante mantener trazabilidad de los resultados, observaciones e incidencias detectadas.

CMF ha dispuesto un canal oficial que permite:
• Realizar consultas técnicas o funcionales • Reportar incidencias • Solicitar apoyo • Coordinar observaciones y aclaraciones • Realizar seguimiento de hallazgos y resultado

Link:  [Canal Oficial de Soporte](#)