Riesgos en los Servicios de Valores según ISSA – 2025

April 2025

DESCARGO DE RESPONSABILIDAD

La intención de ISSA es que este informe se actualice periódicamente. Este documento no constituye asesoramiento profesional ni legal, y está sujeto a posibles cambios en la normativa, interpretación o prácticas del mercado. Ninguno de los productos, servicios, prácticas o estándares mencionados o descritos en este informe tiene carácter prescriptivo para los Participantes del Mercado. Por lo tanto, no deben interpretarse como prácticas de mercado requeridas, ya sea de forma expresa o implícita. En cambio, su objetivo es servir como puntos de referencia informativos que puedan ayudar a los Participantes del Mercado a gestionar los desafíos del entorno actual de los servicios de valores. Ni ISSA ni los miembros del Grupo de Trabajo de ISSA

Tabla de Contenido

Sección 1: Resumen Ejecutivo

Introducción

La Asociación Internacional de Servicios de Valores (ISSA) es una asociación global que respalda a la industria de Servicios de Valores. Los miembros de ISSA incluyen Depósitos Centrales de Valores (CSDs), custodios, empresas tecnológicas y otras entidades que participan activamente en todos los aspectos de la cadena de valor de los Servicios de Valores. Al conectar a sus miembros y facilitar la colaboración, ISSA brinda el liderazgo necesario para impulsar el cambio en esta industria. El enfoque está en encontrar soluciones progresivas para reducir riesgos y mejorar la eficiencia y eficacia — desde el emisor hasta el inversor — así como en proporcionar liderazgo intelectual más amplio para ayudar a definir el futuro de la industria.

La capacidad para comprender y mitigar riesgos es clave para todos los participantes en la cadena de valor de los Servicios de Valores. La mitigación de riesgos puede evitar que las organizaciones se vean afectadas por eventos inesperados y sufran pérdidas financieras, operativas y/o reputacionales. Por ello, ISSA ha creado el informe "Riesgos en los Servicios de Valores 2025", con el objetivo de ofrecer a quienes participan activamente en esta industria la información necesaria para identificar riesgos potenciales e implementar acciones para mitigarlos. Sin embargo, al identificar los riesgos clave inherentes a los Servicios de Valores, debe tenerse en cuenta que no todos los riesgos pueden mitigarse, siendo parte inherente de la actividad comercial. Es responsabilidad de cada organización llevar a cabo su propia investigación y evaluación para asegurar que comprendan tanto los riesgos asumidos como las mejores formas de gestionarlos.

Antecedentes

En 2017, ISSA publicó un “Informe sobre Riesgos Inherentes en la Cadena de Custodia Global” que actualizó la publicación original de 1992 “Informe sobre Riesgos en la Custodia Global”. Ambos informes fueron diseñados como textos informativos con el objetivo de mejorar la comprensión de los Servicios de Valores, lo que a su vez llevó a una mayor apreciación de los riesgos y, por tanto, a una mejor mitigación de riesgos a lo largo de la cadena de valor, minimizando pérdidas y resultados adversos.

Desde la publicación anterior, la industria de Servicios de Valores ha experimentado cambios continuos:

- Nuevas clases de activos ganando popularidad entre los inversores
- Avances significativos en tecnología
- Cambios fundamentales en los modelos operativos
- Evolución continua de las regulaciones
- Materialización del impacto de eventos geopolíticos

Dado este contexto, ISSA considera adecuado producir un informe actualizado sobre los riesgos en los Servicios de Valores.

Riesgos en los Servicios de Valores según ISSA – 2025

El nuevo informe de ISSA comienza con una sección que proporciona el contexto necesario, definiendo los Servicios de Valores, explicando su papel dentro del ciclo de vida del activo y describiendo el rol de los distintos participantes y funciones dentro de la cadena de valor de los Servicios de Valores.

La siguiente sección está estructurada en torno a los principales tipos de riesgos inherentes a la prestación de Servicios de Valores y ofrece información sobre enfoques comunes para su mitigación.

Estos riesgos incluyen:

Categorías de Riesgo Operacional:

- Riesgo Regulatorio, Legal y de Cumplimiento
- Riesgo del Cliente
- Riesgo de Proveedores Terceros
- Riesgo de Protección de Activos
- Riesgo de Ejecución, Entrega y Gestión de Procesos
- Riesgo de Seguridad de la Información
- Riesgo Tecnológico
- Riesgo relacionado con Activos Digitales

Otras categorías clave de riesgo:

- Riesgo de Crédito
- Riesgo de Liquidez
- Riesgo Sistémico
- Riesgo Geopolítico

Puntos Clave para Tener en Cuenta

Se deben considerar los siguientes puntos clave al leer este documento:

- Este informe abarca riesgos específicos de la cadena de valor de los Servicios de Valores, lo cual incluye la captura de operaciones, compensación y liquidación, custodia, servicios sobre activos y servicios relacionados. No aborda riesgos ajenos a los Servicios de Valores, como los vinculados a la emisión o a decisiones de inversión.
- Si bien el informe se enfoca principalmente en las funciones de los Servicios de Valores y los riesgos para sus participantes, también se incluyen perspectivas de otras partes involucradas en la cadena de valor, cuando es pertinente.
- En los Apéndices se proporciona un glosario con los términos clave y sus definiciones a alto nivel

Público Objetivo

Este informe tiene como propósito presentar los procesos y riesgos inherentes a la cadena de valor de los Servicios de Valores. Su objetivo es ofrecer una visión general completa con fines educativos, proporcionando una buena introducción a la terminología de los Servicios de Valores, los participantes, las funciones y, por supuesto, los riesgos. Será de interés para:

- Participantes del ciclo de vida del activo, incluyendo emisores, gestores de activos, proveedores de Servicios de Valores (como custodios e infraestructuras de mercado financiero), proveedores externos (como proveedores de tecnología y empresas de outsourcing) y — potencialmente — asociaciones del sector y organismos reguladores.
- Personas que se están incorporando al sector de Servicios de Valores, así como empleados actuales de la industria que buscan ampliar su comprensión del entorno de estos servicios.

Agradecimientos

Este informe es el resultado del esfuerzo de un equipo de expertos de ISSA que participaron en el Grupo de Trabajo sobre Riesgos en los Servicios de Valores 2025 (GT). Este grupo incluyó a miembros del Comité Operativo y otras empresas miembro de ISSA. Los nombres de las empresas que colaboraron en la elaboración de este informe se incluyen en los Apéndices.

La Junta Ejecutiva de ISSA desea agradecer a los miembros del GT por sus contribuciones, así como a sus respectivas empresas por haber permitido su participación.

Sección 2: Contexto

1. Introducción a los Servicios de Valores

1.1 Introducción

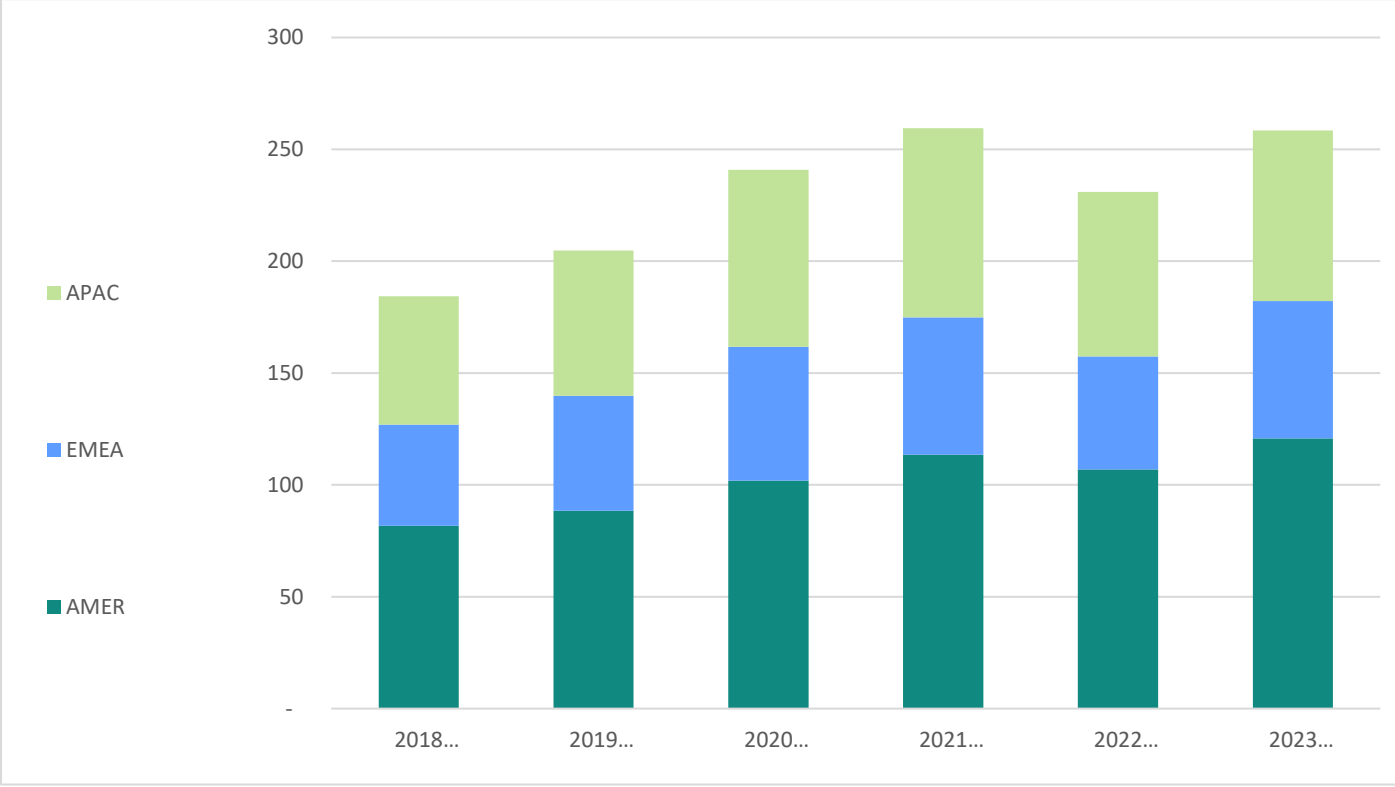
En este capítulo se define el término *Servicios de Valores*. Se presenta el ciclo de vida del activo y se destacan los componentes correspondientes a los Servicios de Valores. Además, se proporciona el significado del término *activo*.

1.2 Definición

Los Servicios de Valores son un componente clave dentro del ciclo de vida completo de un activo. En su forma más básica, los Servicios de Valores (también conocidos como servicios post-ejecución o post-negociación) comprenden la captura de operaciones, la compensación y liquidación, así como la custodia y administración de activos en nombre de los clientes. Los Servicios de Valores han experimentado un crecimiento significativo tanto en tamaño como en complejidad, al igual que los propios mercados financieros. El siguiente gráfico ilustra el crecimiento de los Activos Bajo Custodia (*Assets under Custody*, AUC) entre 2018 y 2023.

Ilustración 1.2 Gráfico del Crecimiento de los Activos Bajo Custodia

Crecimiento de los Activos Bajo Custodia 2018 a 2023 (en billones de USD)



Fuente: Federación Mundial de Bolsas (WFE), Banco de Pagos Internacionales (BIS) y análisis de McKinsey

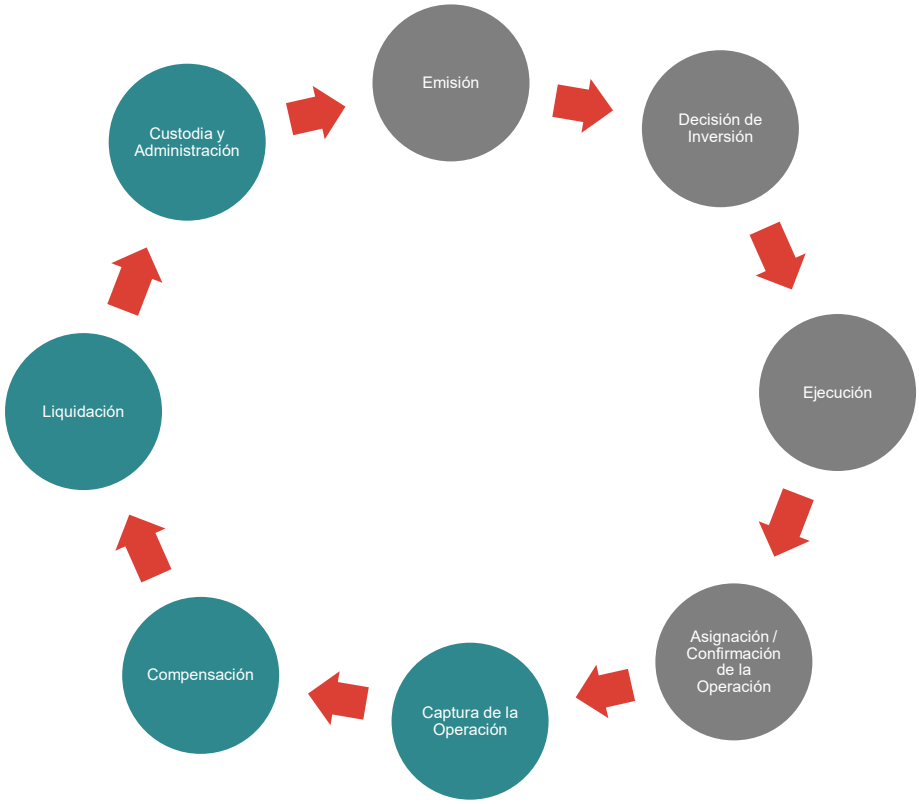
1.3 El Ciclo de Vida del Activo

El siguiente diagrama ilustra, a un nivel general, el ciclo de vida de un activo.

Este documento se centra en los riesgos inherentes dentro de la cadena de valor de los Servicios de Valores. Los componentes de los Servicios de Valores dentro del ciclo de vida comprenden las funciones que están resaltadas en verde en la ilustración. Estas funciones incluyen la captura de operaciones, la compensación, la liquidación y la custodia y administración de los activos.

También existen otros componentes del ciclo de vida del activo — resaltados en gris en la ilustración — que están conectados y proporcionan la información y el soporte necesarios para que los componentes de los Servicios de Valores puedan operar, pero que no son, en sí mismos, funciones propias de los Servicios de Valores.

Ilustración 1.3 Ciclo de Vida de un Activo



1.4 Activos

Un activo en el mundo financiero (también conocido como activo financiero o instrumento financiero) es un bien que tiene valor derivado de un derecho contractual o de propiedad. Existen muchos tipos diferentes de activos financieros y pueden mantenerse en diversas formas.

1.4.1 Tipos de Activos

A lo largo de este documento se hace referencia a múltiples tipos de activos. Las categorías principales, según lo definido por la Directiva sobre Mercados de Instrumentos Financieros (MiFID), incluyen:

- Valores negociables (como acciones, recibos de depósito y bonos)
- Instrumentos del mercado monetario (como certificados de depósito, pagarés comerciales, letras del tesoro)
- Participaciones en instituciones de inversión colectiva
- Derivados (como futuros, opciones, swaps, contratos a plazo)

Nota: Esta lista no es exhaustiva. Puede encontrarse más información sobre activos financieros, tal como se definen en MiFID II, en el siguiente enlace: Anexo I Autoridad de Títulos Valores y Mercados Europeos (europa.eu).

1.4.2 Formas de los Activos

Los activos se mantienen predominantemente en forma electrónica, aunque también pueden conservarse en otras formas, como certificados físicos. Las principales formas son:

- **Activos desmaterializados**
  Son activos que se emiten y mantienen únicamente en formato electrónico mediante anotaciones en cuenta.
- **Activos inmovilizados**
  Son activos emitidos en forma de certificados en papel, pero que han sido inmovilizados (en un CSD), y por lo tanto están disponibles en formato electrónico mediante anotaciones en cuenta.
- **Activos mantenidos como certificados**
  Son activos que se emiten y permanecen en circulación en forma de certificados físicos. Normalmente, estos activos son mantenidos por inversores individuales o por clientes que designan a un proveedor de Servicios de Valores para que los custodie de forma segura en la bóveda de un subcustodio.
- **Activos tokenizados**
  Son una representación digital de los activos mencionados anteriormente o activos que se emiten exclusivamente en forma tokenizada (véase el capítulo sobre Activos Digitales para más información).

En muchos mercados, los activos están ahora completamente desmaterializados o inmovilizados. La desmaterialización e inmovilización mejoran la eficiencia y el control, reduciendo el riesgo de pérdida, fallos en la liquidación y fraude.

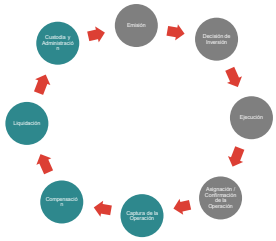
1.4.3 Propiedad de los Activos

La propiedad de los activos se ve afectada según si los valores son nominativos o al portador:

- **Valores nominativos**
  El derecho de propiedad o titularidad de los activos se registra en el libro de acciones o de bonos de la empresa emisora. Dependiendo del mercado, el registro puede realizarse a nombre del titular nominal (nominee) o directamente a nombre del inversor final.
- **Valores al portador**
  No existe registro en los libros de la empresa emisora; el propietario es quien tenga en su posesión los valores al portador.

2. Participantes en el Ciclo de Vida del Activo

2.1 Introducción



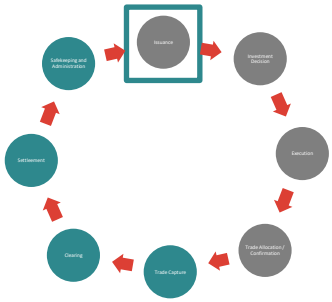
Como se muestra en la ilustración del Capítulo 1, el ciclo de vida de un activo consta de varios componentes. En este capítulo, se presentan los participantes clave en cada etapa del ciclo de vida del activo, y se resumen sus funciones y responsabilidades.

2.2 Definición

Los participantes en el ciclo de vida del activo son organizaciones o individuos que proporcionan o utilizan cualquiera de los componentes definidos en el ciclo de vida del activo, tal como se muestra en la ilustración del Capítulo 1. Estos incluyen tanto a los participantes que forman parte de la cadena de valor de los Servicios de Valores como a aquellos que se conectan e interactúan con ellos.

Las siguientes secciones describen los distintos participantes en el ciclo de vida del activo que aparecen en el diagrama anterior, en orden secuencial. Las secciones 2.3, 2.4, 2.5 y 2.7 cubren a los participantes que se conectan e interactúan con los participantes de los Servicios de Valores, mientras que la sección 2.6 se enfoca en los participantes directos de los Servicios de Valores.

2.3 Participantes en los Servicios del Emisor



La primera etapa del ciclo de vida del activo es aquella en la que se crea el activo, conocida como emisión. Esta creación puede corresponder a un nuevo activo o a una ampliación de un activo ya existente. Los participantes en la etapa de emisión incluyen al emisor, al agente de transferencias y al registrador.

2.3.1 Emisor

El creador de un activo se conoce como emisor. Los emisores pueden ser gobiernos, empresas u otras entidades que necesitan obtener financiación. El emisor buscará vender el activo a los clientes con el fin de recaudar los fondos necesarios. Además, el emisor es responsable, de forma continua, de asegurar el cumplimiento de las normas de divulgación para los inversores.

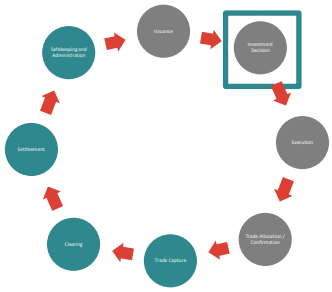
2.3.2 Agente de Transferencias

Un agente de transferencias es una entidad designada por un fondo o por el emisor de un activo para emitir y cancelar participaciones de fondos y valores en formato físico o desmaterializado, reflejar los cambios en la titularidad del activo, actuar como intermediario del emisor y gestionar la interacción con los inversores en relación con consultas como la pérdida o robo de valores, así como procesar distribuciones.

2.3.3 Agente de Registro

El agente de registro es responsable de mantener un registro de los inversores y del número de valores que poseen en el caso de emisiones de fondos, bonos o acciones, y de asegurar que la cantidad de valores en circulación coincida con la cantidad emitida. Las funciones de registro y de agencia de transferencias suelen ser ofrecidas por la misma entidad.

2.4 Participantes en la Toma de Decisiones de Inversión



La siguiente etapa en el ciclo de vida del activo es la toma de decisiones de inversión. Estas decisiones pueden ser tomadas directamente por un inversor o por un gestor de activos, que puede actuar en nombre propio o en representación de uno o varios inversores. Para los fines de este informe, cuando un inversor o gestor de activos designa a un proveedor de ejecución de operaciones y/o de servicios de valores, se le denomina cliente.

2.4.1 Inversor

Un inversor es una persona física u organización que invierte en activos. Puede ser el propietario real de los activos o un intermediario que los mantiene en nombre de otros inversores.

Un inversor puede ser institucional (por ejemplo, un fondo de pensiones, un fondo soberano, un fondo de cobertura, un fondo o sociedad de capital privado, un banco —a menudo en nombre de sus propios clientes— o una compañía de seguros), o puede ser un inversor minorista. Cuando el inversor es el propietario real de los activos, se le conoce como el beneficiario final (*Ultimate Beneficial Owner*, UBO). El término UBO puede tener distintas definiciones según la jurisdicción; por ejemplo, en ciertos mercados puede considerarse UBO a la parte que posee derechos de voto.

Un inversor puede tomar decisiones de inversión por sí mismo o designar a un gestor de activos para que gestione dichas decisiones, convirtiéndose así en el cliente del gestor de activos.

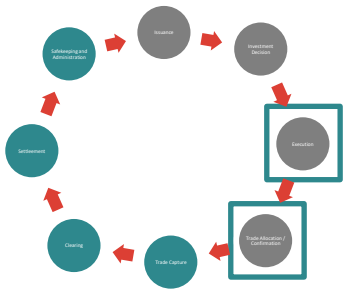
2.4.2 Gestor de Activos

Un gestor de activos es una entidad o individuo que toma decisiones de inversión en nombre de uno o varios inversores. Los gestores de activos pueden gestionar inversiones de distintos tipos de clientes, incluyendo fondos institucionales, clientes privados, fondos de inversión y otros vehículos colectivos.

El gestor de activos actúa bajo un mandato de inversión acordado con el cliente, que establece directrices sobre la estrategia de inversión, los tipos de activos permitidos, la tolerancia al riesgo y otros parámetros relevantes.

En algunos casos, el gestor de activos también puede seleccionar y designar proveedores de ejecución de operaciones y/o servicios de valores para realizar operaciones y administrar los activos del cliente. En este contexto, el gestor de activos actúa como cliente de esos proveedores.

2.5 Participantes en la Ejecución de Operaciones



La siguiente etapa en el ciclo de vida del activo es la **negociación** de este. Los activos pueden negociarse tanto en mercados organizados como fuera de ellos (*on-exchange* u *off-exchange, conocido también como OTC – over the counter*), y por diferentes participantes encargados de la ejecución de operaciones.

2.5.1 Broker Dealer

Un Broker Dealer ejecuta transacciones financieras en nombre de sus clientes (como *Broker*) o por cuenta propia (como *Dealer*). Puede formar parte de una firma especializada en servicios de corretaje o de una organización más grande, como un banco o un custodio. El Broker puede proporcionar a sus clientes acceso a plataformas de negociación y, en algunos

casos, a servicios de préstamo de valores. Los Broker Dealers están autorizados y supervisados por los organismos reguladores locales.

2.5.2 Broker de Valores o Prime Broker

Los brokers de valores o Prime Brokers ofrecen servicios a fondos de cobertura y otros clientes profesionales, incluyendo préstamo de valores, ejecución apalancada de operaciones y gestión de dinero. Un Prime Broker también puede custodiar activos en nombre de sus clientes y actuar como custodio. Además, puede ofrecer acceso a plataformas de negociación.

2.5.3 Bolsa de Valores

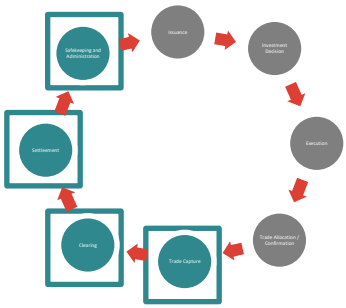
Una bolsa de valores es un lugar físico o electrónico donde los Broker Dealers pueden comprar y vender valores como acciones, bonos y otros instrumentos financieros. La mayoría de los países tienen una bolsa de valores (en algunos mercados existen varias). Estas bolsas están reguladas por las autoridades locales competentes.

2.5.4 Otras Infraestructuras de Mercado

Existen múltiples infraestructuras de mercado adicionales, incluidas aquellas que proporcionan plataformas de negociación y ejecución para la industria. También existen entidades que suministran datos bursátiles, conectividad y datos de referencia y precios de valores. Algunos ejemplos incluyen:

- Redes de Comunicación Electrónica (ECNs)
- Sistemas Alternativos de Negociación (ATSs)
- Instalaciones Multilaterales de Negociación (MTFs)

2.6 Participantes en los Servicios de Valores



En la siguiente etapa del ciclo de vida del activo, conocida como Servicios de Valores —también llamados servicios *post-ejecución* o *post-negociación*— participan múltiples entidades. Estas incluyen custodios, infraestructuras del mercado financiero (FMIs, por sus siglas en inglés), así como otros participantes que pueden ser necesarios según los servicios requeridos por el cliente. A lo largo de este documento, estos participantes se denominan proveedores de Servicios de Valores.

2.6.1 Custodio

Aunque existen varias formas en que un inversor o gestor de activos puede mantener sus activos, uno de los modelos más comunes es la designación de un custodio. En ese caso, el inversor o gestor de activos se convierte en cliente del custodio, término que se utiliza consistentemente en este informe.

Un custodio es una institución financiera autorizada y supervisada por la autoridad reguladora de servicios financieros o de supervisión bancaria en su jurisdicción de establecimiento y/o donde presta sus servicios. Es responsable de salvaguardar los activos financieros del cliente, manteniéndolos de forma segura y, en la medida en que esté bajo su control, protegiéndolos contra pérdidas mientras estén bajo custodia. También se encarga de procesar y liquidar las operaciones con valores en todas las clases de instrumentos financieros que puedan mantenerse en custodia, así como de prestar los servicios asociados a esos portafolios mientras estén bajo su responsabilidad.

En muchos sentidos, el custodio puede considerarse un intermediario de información**,** que facilita la comunicación entre emisores e inversores.

La relación entre un custodio y un cliente se rige por un contrato de custodia. Esta relación puede ser tan simple como la designación de un banco a otro como custodio en un país determinado, o tan compleja como la participación de varios gestores de fondos que actúan en nombre de un cliente y que requieren servicios más allá de los tradicionales Servicios de Valores. Un custodio puede interactuar directamente con el cliente o recibir instrucciones en nombre del cliente por parte de un gestor de activos. La función y el alcance de los servicios del custodio dependerán de los clientes y los mercados que cubra.

Para custodiar valores en un mercado o jurisdicción determinados en nombre de sus clientes, el custodio debe tener una cuenta en el Depósito Central de Valores (CSD) o en un CSD internacional (ICSD). Esta cuenta puede estar mantenida directamente por un custodio global, si tiene la capacidad para ello, o por un subcustodio designado. A efectos de este informe, el término custodio se refiere tanto al custodio global como al subcustodio.

2.6.1.1 Custodio Global

Un custodio global presta servicios en relación con valores negociados en múltiples mercados o jurisdicciones. Proporciona acceso a diversos mercados a instituciones financieras como bancos, brokers y *prime brokers*, así como a gestores de activos, gestores de fondos, fondos de pensiones y otros clientes. Los custodios globales pueden ofrecer estos servicios directamente, manteniendo una cuenta en un (I)CSD, o indirectamente a través del uso de varios subcustodios.

Cuando los portafolios son grandes o están diversificados geográfica o sectorialmente, un cliente puede designar a un custodio global como agente, beneficiándose así de contar con un único punto de contacto y experiencia especializada, en lugar de tener que coordinarse con múltiples partes (como subcustodios, CSDs, agentes fiscales, registradores, etc.). Al designar un custodio global, el cliente puede aprovechar su experiencia y, en última instancia, reducir su riesgo en Servicios de Valores.

2.6.1.2 Subcustodio

Un subcustodio presta servicios relacionados con valores negociados en un mercado o jurisdicción específicos. Además de proporcionar acceso a mercados concretos a instituciones financieras como bancos, brokers y *prime brokers*, el subcustodio también puede prestar servicios a un custodio global cuando este no tiene presencia operativa en dicha jurisdicción. En estos casos, el subcustodio se denomina a veces banco agente, y su relación con el custodio global se rige mediante un contrato de subcustodia. En algunas ocasiones, el subcustodio forma parte del mismo grupo empresarial que el custodio global.

2.6.2 Infraestructura del Mercado Financiero (*Financial Market Infrastructure*, también denominada Utilidad del Mercado Financiero)

En la industria de los Servicios de Valores, una Infraestructura del Mercado Financiero (FMI) es un proveedor u operador que compensa o liquida valores entre los participantes de los Servicios de Valores. Como intermediario, un custodio puede acceder a las FMIs directamente, a través de su propia membresía, o indirectamente, mediante su red de subcustodios. Puede encontrarse más información sobre las FMIs en el sitio web del Banco de Pagos Internacionales: Principles for Financial Market Infrastructures (PFMI) (bis.org)

Ejemplos de FMIs incluyen las contrapartes centrales (CCPs), los depósitos centrales de valores (CSDs) (véase la definición más abajo) y los sistemas de pago.

2.6.2.1 Contraparte Central

Una Contraparte Central (CCP) —también conocida como cámara de compensación— existe en ciertos mercados y puede operar de manera transfronteriza en otros. Las CCPs suelen utilizarse para transacciones en bolsas de valores, mientras que las operaciones extrabursátiles (*over the counter*, OTC) tienden a dirigirse directamente a los (I)CSDs a través de los custodios.

La CCP actúa como contraparte central para todos los miembros compensadores. Mediante el proceso de novación, la CCP sustituye el contrato entre dos partes por uno nuevo, en el cual se convierte en el comprador frente a cada vendedor y en el vendedor frente a cada comprador. La CCP es responsable de la compensación (después de la negociación y antes de la liquidación), de definir las obligaciones de liquidación neta (cuando sea aplicable) y de asignar la responsabilidad para llevar a cabo la liquidación.

La liquidación se realiza en el CSD correspondiente, una vez completado el proceso de compensación en la CCP. En caso de que un miembro compensador incumpla sus obligaciones, la CCP proporciona una garantía de cumplimiento de todas las obligaciones de los miembros que no han incumplido, actuando en lugar de la parte en incumplimiento.

2.6.2.2 Depósito Central de Valores (Central Securities Depository)

Un Depósito Central de Valores (CSD) es una infraestructura de mercado que custodia valores y permite que las transacciones con dichos valores se procesen mediante anotaciones electrónicas en cuenta. El CSD normalmente opera un sistema de liquidación de valores y proporciona mantenimiento centralizado de cuentas de valores y/o funciones de notaría. Dependiendo del mercado, un CSD puede ser de propiedad privada o estar listado en bolsa. Algunos son operados por el Banco Central nacional, mientras que otros forman parte de un grupo de FMIs más amplio que puede incluir bolsas de valores y/o CCPs.

Un CSD también proporciona custodia centralizada y servicios sobre activos (lo que puede incluir la administración de eventos corporativos y amortizaciones), y desempeña un papel clave en la integridad de las emisiones de valores a través de reconciliaciones y otros controles similares, que en algunos casos son obligatorios según normativas locales o regionales, como el Reglamento sobre los Depósitos Centrales de Valores (CSDR**)** en el EEE.

Los valores pueden mantenerse en el CSD ya sea en forma física (pero inmovilizada) o en forma desmaterializada.

A un nivel general, y dejando de lado las diferencias regionales, un CSD puede actuar en distintas capacidades:

- Un CSD nacional (Domestic CSD) forma parte de la infraestructura de mercado del país en el que está establecido y, dependiendo del mercado, puede actuar tanto como CSD emisor como CSD inversor**.**
- Un CSD emisor (Issuer CSD) es el CSD en el que se emiten (o inmovilizan) los valores.
- Un CSD inversor (Investor CSD) es un participante directo o indirecto en el sistema de liquidación de valores operado por otro CSD, con el fin de facilitar la transferencia de valores entre los participantes de ambos CSDs.
- Un CSD internacional (ICSD) cumple una doble función, ya que puede actuar como CSD emisor para activos internacionales (por ejemplo, *eurobonos*), pero también puede liquidar instrumentos nacionales elegibles, actuando así como CSD inversor**.**

Como infraestructuras del mercado financiero, los CSD operan en un entorno altamente regulado. Están sujetos a leyes nacionales sobre la emisión, liquidación y custodia de valores, y son supervisados por las autoridades competentes, que suelen ser el regulador de valores, el regulador bancario o la autoridad nacional correspondiente. Generalmente, también están sujetos a la supervisión del banco central pertinente.

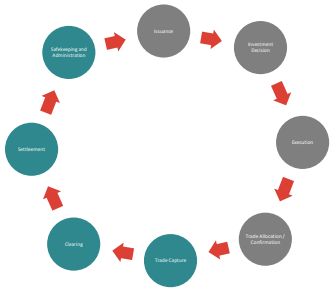
No obstante, los CSD están expuestos a pérdidas asociadas a sus propios errores u omisiones, fraudes y a los costos derivados de interrupciones operativas. Por ello, un CSD debe contar con normas, políticas y procedimientos claros y completos, así como con un marco de gobernanza y gestión de riesgos igualmente integral y transparente, que garantice que los valores mantenidos en nombre de sus participantes y de los clientes de estos estén debidamente registrados en sus libros y protegidos frente a los riesgos asociados a otros servicios que el propio CSD pueda ofrecer.

2.6.2.3 Banco Central

El banco central es el proveedor de dinero del banco central (Central Bank Money, CBM) para la liquidación en el CSD. Los participantes del CSD deben tener una cuenta, ya sea directamente con el banco central o con un banco liquidador que mantenga dicha cuenta. En ciertos países, el banco central también puede actuar como, o directamente operar, el CSD nacional para determinados segmentos del mercado (normalmente para valores de renta fija emitidos por el gobierno), y mantener el registro de propiedad de estos valores.

2.7 Otros Participantes en el Ciclo de Vida del Activo

Otros participantes que forman parte del ciclo de vida del activo incluyen al regulador, los proveedores externos y los participantes en servicios de fondos.



2.7.1 Regulador

Un regulador supervisa el funcionamiento del mercado financiero en la jurisdicción bajo su responsabilidad. Aunque el mandato y el alcance de un regulador varían de un mercado a otro, a menudo cumple funciones relacionadas con el monitoreo de las condiciones del mercado, su estabilidad y la supervisión general.

Dentro del componente de Servicios de Valores del ciclo de vida del activo, los reguladores establecen las reglas bajo las cuales deben operar los participantes del mercado y pueden ejercer sus funciones de supervisión, por ejemplo, obteniendo datos de los CSD y custodios.

En algunos mercados, la entidad que actúa como regulador —como un banco central— también desempeña un papel directo en el funcionamiento de las infraestructuras del mercado financiero, como las CCP y los CSD.

2.7.2 Proveedor Externo

Un proveedor externo es una empresa especializada que ofrece servicios a los proveedores de Servicios de Valores. Aunque los proveedores externos son una parte importante del ecosistema de Servicios de Valores, es fundamental que existan acuerdos contractuales y niveles de servicio definidos para garantizar que la prestación del servicio sea clara y que los riesgos se gestionen de forma eficaz.

Más adelante en este informe se proporciona información adicional sobre los riesgos asociados a los proveedores externos.

Un ejemplo específico de proveedor externo en Europa es la plataforma Target2-Securities (T2S) del Banco Central Europeo. Esta plataforma se encuentra por encima de varios CSD y bancos centrales, y proporciona una capa armonizada que permite la liquidación transfronteriza en dinero del banco central.

2.7.3 Participantes en Servicios para Fondos

Los servicios para fondos se refieren a los participantes que prestan servicios a un fondo, lo cual incluye al administrador del fondo, al depositario o banco depositario y al agente de transferencias (véase la sección de participantes del emisor).

2.7.3.1 Administrador del fondo

Un administrador del fondo es responsable de verificar de forma independiente los activos de un fondo y de valorar el fondo en nombre del cliente (en el caso de un fondo, el gestor del fondo). Sus responsabilidades incluyen:

- Contabilidad del fondo
- Informes financieros
- Cálculo del valor neto del activo (NAV) del fondo
- Llamadas de capital y distribuciones
- Funciones de supervisión de ciertas operaciones para garantizar que el fondo actúe conforme a la legislación nacional aplicable y a las normas del propio fondo

2.7.3.2 Depositario / Banco depositario

Un depositario, o banco depositario, es designado por ciertos tipos de fondos domiciliados en la UE para supervisar las inversiones realizadas en el fondo. Los fondos que requieren un banco depositario son los Organismos de Inversión Colectiva en Valores Mobiliarios (UCITS) o los Fondos de Inversión Alternativa (AIFs). El banco depositario tiene una responsabilidad estricta de restitución por los activos perdidos, sujeta a ciertas excepciones derivadas de eventos externos.

Sus responsabilidades incluyen, pero no se limitan a:

- Funciones de custodia y registro
- Monitoreo de flujos de dinero
- Funciones de supervisión de ciertas operaciones para garantizar que el fondo actúe conforme a la legislación nacional aplicable y a las normas del fondo

3. Funciones de los Servicios de Valores

3.1 Introducción

Para proporcionar contexto y facilitar la comprensión del componente de Servicios de Valores dentro del ciclo de vida del activo descrito en el Capítulo 1, este capítulo presenta las funciones y utilidades principales —así como otros servicios adicionales— que constituyen funciones propias de los Servicios de Valores.
Más adelante, en la sección de Riesgos, se ofrece información detallada sobre los riesgos asociados a estas funciones.

3.2 Definición

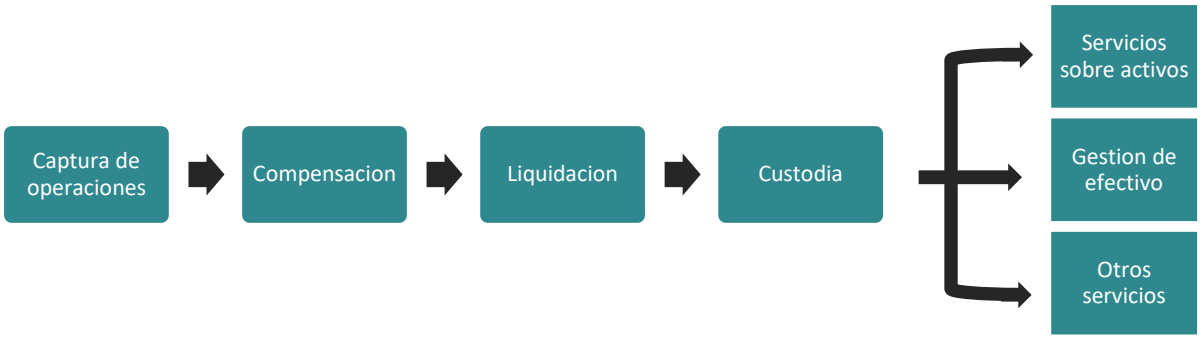
Las funciones de los Servicios de Valores son las distintas áreas operativas de un custodio, o de otro proveedor de Servicios de Valores, que prestan servicios a un cliente. Estas funciones incluyen tanto las funciones principales —que son utilizadas por la mayoría de los clientes que recurren a un proveedor de Servicios de Valores— como servicios adicionales, que son opcionales pero que también pueden ser de interés para el cliente. Asimismo, existen una serie de utilidades necesarias para respaldar la oferta general de servicios.

3.3 Funciones de los Servicios de Valores

Como se muestra en el ciclo de vida del activo, este comprende múltiples componentes, varios de los cuales están relacionados con los Servicios de Valores. El siguiente diagrama ilustra, a un nivel general, las funciones principales de los Servicios de Valores. Este diagrama será citado a lo largo de este informe.

Las funciones de los Servicios de Valores proporcionan múltiples capas de intermediación entre el emisor y el inversor final. Cada capa representa un participante cuyos servicios y perfil de riesgo dependerán en gran medida de su base de clientes. El diagrama debe interpretarse tanto desde la perspectiva de la compra como de la venta de activos.

Ilustración 3.3 Diagrama de las funciones principales de los Servicios de Valores



3.4 Funciones principales de los Servicios de Valores

A continuación, se describen las funciones principales que conforman la oferta de servicios en los Servicios de Valores.

3.4.1 Captura de operaciones

La captura de operaciones, o de instrucciones, es la primera función en el diagrama de los Servicios de Valores y consiste en el proceso mediante el cual el proveedor de Servicios de Valores recibe una instrucción de su cliente (o del participante en la ejecución de operaciones) para "liquidar la operación" en su nombre.

Como se explicó antes, un cliente normalmente accede a los mercados a través de un broker, quien ayuda a encontrar un vendedor para un comprador y viceversa. En las operaciones entre un cliente y un participante en la ejecución de operaciones, una sola transacción puede ser asignada a varias cuentas diferentes. Esto da lugar, en efecto, a múltiples transacciones distintas que deben liquidarse entre ambas partes negociadoras, quienes instruirán las órdenes de liquidación a través del proveedor de Servicios de Valores hacia el CSD correspondiente.

La generación y transmisión de las instrucciones de liquidación es un primer paso crucial en el proceso de liquidación, ya que introduce la operación en el sistema del proveedor de Servicios de Valores para su conciliación y, finalmente, su liquidación.

3.4.2 Compensación

La compensación es un paso opcional —entre la negociación y la liquidación— mediante el cual ciertas transacciones se procesan de forma conjunta, normalmente en una plataforma de compensación (aunque los flujos extrabursátiles u OTC también pueden someterse a compensación). La compensación se realiza en una CCP, que se convierte en el comprador frente a cada vendedor y en el vendedor frente a cada comprador.

La compensación agrupa múltiples operaciones —proceso conocido como "neteo"— para formar una de las siguientes:

- Una única operación neteada, es decir, el resultado neto de todas las compras y ventas de un mismo valor
- Un agregado de todas las compras y un agregado de todas las ventas de un mismo valor

El neteo es un proceso económico y eficiente, pero requiere una gestión de riesgos sólida.

Las organizaciones que participan en el proceso de compensación se conocen como miembros compensadores. Estos actúan como contraparte en las operaciones que compensan y pueden desempeñar dos funciones diferentes:

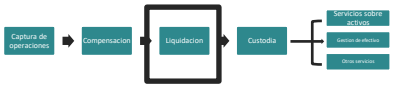
- En nombre propio, para operaciones propias, como miembro compensador directo (Direct Clearing Member, DCM)
- En nombre de un cliente, como miembro compensador general (General Clearing Member, GCM)

En ambos casos, los miembros compensadores actúan como la contraparte en la operación. Por lo tanto, cuando un proveedor de Servicios de Valores es miembro compensador y actúa en calidad de GCM, asume el riesgo principal de la operación de su cliente. En este sentido, el proveedor de Servicios de Valores está expuesto a múltiples riesgos asociados a la compensación, incluidos el riesgo de crédito, riesgo de mercado, riesgo operativo y, en última instancia, riesgo de insolvencia en caso de incumplimiento del cliente. Los gestores de redes de subcustodios deben mantener una supervisión continua de su red de CCP.

La CCP se protege reteniendo un margen inicial tanto del comprador como del vendedor, para asegurarse de que cualquier disminución en el valor esté cubierta. Realiza una valoración diaria (*mark to market*) para garantizar que ambas partes puedan cumplir con sus obligaciones. Además, la CCP puede iniciar un proceso de recompra (*buy-in*), que es un mecanismo para cubrir fallos en la liquidación. En este caso, la CCP adquiere el valor que no se ha entregado de otra fuente, cancela la operación original y liquida con el nuevo valor. Cualquier costo asociado a esta recompra se deduce del colateral proporcionado por el GCM. Cuando la CCP mantiene valores como colateral, designará a un custodio para que preste los servicios de gestión de colateral.

3.4.3 Liquidación

La liquidación es el movimiento de valores entre la parte receptora y la parte entregadora. Aunque comúnmente se asocia con la conclusión de una operación (es decir, la compra y venta de valores), la liquidación también puede implicar un movimiento entre dos cuentas distintas del mismo titular, lo que se conoce habitualmente como gestión de inventario.



Si bien muchos proveedores de Servicios de Valores facilitan el proceso de liquidación, esta generalmente tiene lugar en el sistema de liquidación de valores del (I)CSD, donde la transferencia de la titularidad —y el registro posterior de la propiedad— se realiza a través de la liquidación central de valores, ya sea contra pago o sin pago.

La liquidación se refiere al proceso de transferencia de la propiedad de los valores del vendedor al comprador. Puede realizarse “en mercado” (*on exchange*) o “fuera de mercado” (*off exchange u OTC*). Normalmente, la liquidación se efectúa contra dinero, lo que se denomina Entrega contra Pago (DVP) o Recepción contra Pago (RVP). No obstante, la liquidación también puede realizarse sin contraprestación monetaria (*free of payment*).

3.4.3.1 Liquidación de operaciones en mercado

La liquidación en mercado (*on-exchange*) se beneficia de la supervisión y las normas de la bolsa de valores, así como de la transparencia del mercado, y con frecuencia se apoya en la liquidación a través de una CCP. Para las operaciones canalizadas a través de una CCP, la bolsa de valores envía todas las órdenes para su verificación al cliente a través de un miembro compensador (normalmente un broker dealer o un custodio). El miembro compensador está obligado a liquidar todas las operaciones al final de cada día sobre una base neta con la CCP y respalda esta obligación con niveles adecuados de colateral elegible.

Las organizaciones que no son miembros compensadores deben encontrar un proveedor externo que les proporcione servicios de compensación (normalmente un custodio). Este proveedor externo es responsable de la compensación de todas las operaciones en mercado de sus clientes y solicitará a estos el colateral adecuado para respaldar sus obligaciones de liquidación.

3.4.3.2 Liquidación de operaciones fuera de mercado

Algunos valores no son adecuados para ser liquidados en mercados organizados (*on-exchange*) debido a su falta de liquidez o al nivel de riesgo de crédito que representan, por lo que se liquidan fuera de mercado (*off-exchange u OTC*). Ejemplos de ello incluyen acciones ilíquidas, transacciones difíciles de valorar y ciertos valores específicos de un emisor que pueden no ser elegibles debido a su aparente falta de liquidez en el mercado en caso de fallo en la operación.

La liquidación de una operación fuera de mercado suele realizarse entre dos proveedores de Servicios de Valores utilizando sus cuentas en el (I)CSD. Esto puede hacerse bajo un esquema de entrega contra pago (DVP), recepción contra pago (RVP), o sin pago alguno (*free of payment*), por ejemplo, cuando la moneda utilizada no es admitida por el (I)CSD.

3.4.3.3 Operaciones de entrega contra pago

El Banco de Pagos Internacionales (BIS) publicó un documento sobre los modelos de liquidación DVP que describe los tres modelos utilizados por los proveedores de Servicios de Valores. Delivery versus payment in securities settlement systems - Oct 1992.

Los tres modelos se describen a continuación:

- Modelo 1: Se refiere a un sistema que liquida las transacciones de valores y dinero sobre una base bruta, operación por operación, donde la transferencia final (incondicional) de los valores del vendedor al comprador (entrega) ocurre al mismo tiempo que la transferencia final del dinero del comprador al vendedor (pago).
- Modelo 2: Es un sistema que liquida las transacciones de valores sobre una base bruta, con la transferencia final de valores del vendedor al comprador (entrega) ocurriendo a lo largo del ciclo de procesamiento, pero liquida las transacciones en dinero sobre una base neta, con la transferencia final de dinero del comprador al vendedor (pago) al final del ciclo de procesamiento.
- Modelo 3: Es un sistema que liquida tanto las transacciones de valores como de fondos sobre una base neta, con las transferencias finales de ambos —valores y dinero— ocurriendo al final del ciclo de procesamiento.

El modelo 1 es el preferido, tanto desde la perspectiva del inversor como en los mercados europeos, ya que reduce el riesgo de que un incumplimiento afecte la liquidación de una operación. Sin embargo, los tres modelos están presentes en los mercados desarrollados.

3.4.3.4 Operaciones sin pago

El tipo de liquidación con mayor nivel de riesgo es aquella en la que los valores se entregan a una contraparte “sin pago”. Se trata de una transferencia de titularidad sin contraprestación. Este tipo de liquidación se utiliza al mínimo, por razones evidentes, pero puede aplicarse en la emisión de nuevos valores cuando el pago se realiza antes de la entrega, o cuando es necesario ejecutar una transferencia de cuenta entre dos proveedores.

Debe actuarse con especial precaución, ya que cualquier entrega incorrecta puede ser difícil de recuperar y generará responsabilidad total si la operación resulta inválida. Una entrega sin pago conlleva un riesgo inherente más elevado de fraude, ya que no se intercambia valor alguno a cambio de los valores entregados.

3.4.4 Custodia

La tenencia de valores propiedad de un cliente se denomina custodia. Los activos suelen custodiarse —aunque aún existen excepciones— en forma electrónica desmaterializada o inmovilizada. Se mantienen en el CSD del emisor (Issuer CSD o ICSD) como anotaciones en cuenta a nombre del cliente o de su titular nominal (nominee), registradas en el libro del emisor. Este servicio puede prestarse en un solo mercado o en múltiples mercados.

Los activos se mantienen, gestionan y supervisan conforme a los regímenes de protección de activos de la jurisdicción del proveedor de Servicios de Valores que firmó el contrato inicial, de la ubicación de la custodia o del lugar de emisión, y también cumpliendo con los requisitos normativos regionales y globales.

3.4.5 Servicios sobre activos

La administración de los activos de un cliente, comúnmente conocida como servicios sobre activos o también conocido como eventos corporativos, típicamente incluye:

- Acciones corporativas (por ejemplo, emisiones de derechos, desdoblamientos de acciones)
- Votación por poder
- Demandas colectivas (class actions)
- Procesamiento de ingresos (por ejemplo, dividendos, intereses / amortizaciones)
- Servicios fiscales (por ejemplo, retención de impuestos y solicitudes de reembolso)

3.4.5.1 Acciones corporativas

Una acción corporativa es un evento iniciado por el emisor de un valor que genera un derecho a favor del cliente. Para el proveedor de Servicios de Valores, la administración de las acciones corporativas sobre los activos de un cliente suele considerarse uno de los procesos de mayor riesgo, debido a la posibilidad de errores y al impacto que estos pueden tener, considerando las variaciones de precio en el mercado que suelen acompañar estos eventos.

Como consecuencia, el modelo operativo suele estar diseñado para asegurar la automatización y el procesamiento directo (*Straight Through Processing*, STP), con el fin de garantizar la precisión y reducir el riesgo de malinterpretaciones o de no cumplir con los plazos establecidos.

Una acción corporativa puede ser obligatoria (por ejemplo, desdoblamientos de acciones, fusiones y adquisiciones, dividendos en dinero) o voluntaria (por ejemplo, ofertas públicas de adquisición, emisiones de derechos, recompras y conversiones). El proveedor de Servicios de Valores está expuesto a un mayor riesgo operativo cuando la acción corporativa es voluntaria, ya que se requiere una instrucción por parte del cliente.

- Evento obligatorio
- En una acción corporativa obligatoria, el cliente no necesita realizar ninguna acción y no tiene la opción de decidir si desea participar cuando el emisor inicia el evento.
- Evento voluntario
- Los eventos voluntarios se ejercen a discreción del cliente, quien puede optar por participar enviando una instrucción, o no tomar ninguna medida, en cuyo caso sus valores no se verán afectados. También existen eventos obligatorios con opciones, en los que el inversor puede enviar una instrucción para elegir entre varias alternativas, aunque se aplicará una opción predeterminada si no se recibe ninguna elección.

3.4.5.2 Votación por poder

Los servicios de votación a través de un poder proporcionan a los inversores notificaciones sobre situaciones comunicadas por el emisor en las que se solicita al inversor que emita un voto. A continuación, un proveedor de Servicios de Valores —ya sea directamente o a través de un agente— se encargará de asegurar que las intenciones de voto del inversor se comuniquen según lo requerido.

3.4.5.3 Demandas colectivas

El servicio de demandas colectivas de un proveedor de Servicios de Valores incluye la recolección de los ingresos resultantes de demandas colectivas específicas y su posterior transferencia al cliente. Dado que la resolución de estas demandas puede extenderse por períodos prolongados, es importante que el proveedor de Servicios de Valores mantenga registros de las instrucciones de liquidación estándar (Standard Settlement Instructions o *SSIs*) del cliente, incluso si el contrato de custodia ha finalizado.

El cliente debe asegurarse de que dicha información esté actualizada, ya que es probable que cambie durante el largo período que suele tomar el proceso de resolución de una demanda colectiva.

3.4.5.4 Procesamiento de ingresos

Un proveedor de Servicios de Valores puede ofrecer un servicio fiscal que facilite al cliente la recepción de una reducción de impuestos sobre acciones corporativas e ingresos recibidos, de acuerdo con los tratados fiscales aplicables y su situación tributaria. Dependiendo del mercado, este servicio fiscal puede prestarse a través de un modelo de reducción en origen o mediante un proceso de solicitud de reembolso de impuestos.

3.4.6 Gestión de dinero

Un proveedor de Servicios de Valores suele ofrecer facilidades de cuenta de dinero para respaldar los movimientos relacionados con la liquidación de valores y los servicios sobre activos. Estos servicios pueden incluir líneas de crédito para apoyar la liquidez intradía y servicios de cambio de divisas (FX).

Los servicios de FX suelen ser necesarios para repatriar ingresos en moneda extranjera (relacionados con la venta de valores, vencimientos, ingresos por dividendos o cupones, y solicitudes de reembolso de impuestos) a la moneda base del cliente, o para financiar la liquidación de transacciones o acciones corporativas. El acceso a divisas puede estar restringido (controles de cambio) según las normativas del mercado y, en ocasiones, como resultado de acciones gubernamentales.

La inteligencia de mercado del proveedor de Servicios de Valores puede proporcionar al cliente información detallada sobre estas restricciones a medida que se hagan conocidas.

3.5 Servicios adicionales

Además de las funciones principales de los Servicios de Valores, un cliente también puede requerir servicios adicionales como préstamo de valores, gestión de colateral, contabilidad de inversiones y/o administración de fondos. Estos servicios suelen ofrecerse como parte de un catálogo de opciones por parte del proveedor de Servicios de Valores, o por una entidad relacionada, y se valoran de forma específica según el servicio.

3.5.1 Préstamo de Valores

Es la transferencia – con objeto temporario – the activos de un beneficiario a otro. A cambio, el tomador de los activos da una garantía, que pueden ser otros activos o dinero, y además paga un arancel.

3.5.2 Gestión de colateral

La gestión de colateral consiste en la entrega de garantías de una contraparte a otra como respaldo frente a una exposición crediticia.

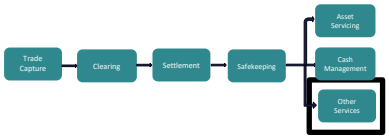
3.5.3 Contabilidad de inversiones

La contabilidad de inversiones implica el registro, la valoración y la elaboración de informes sobre los activos mantenidos por un cliente, de acuerdo con las normativas contables y los principios establecidos.

3.5.4 Administración de fondos

La administración de fondos abarca una variedad de servicios administrativos prestados a un fondo, incluyendo la contabilidad del fondo, el cálculo del valor neto del activo (NAV), la elaboración de informes financieros, y el cumplimiento de requisitos normativos y operativos.

3.6 Servicios de Utilidad en los Servicios de Valores



Además de las funciones principales de los Servicios de Valores y los servicios adicionales que se ofrecen a un cliente, el proveedor de Servicios de Valores también puede necesitar proporcionar algunos servicios de utilidad para respaldar las distintas funciones. Estas incluyen los servicios que se describen a continuación.

3.6.1 Debida Diligencia

La debida diligencia es esencial para el funcionamiento seguro y eficiente del ciclo de vida de los Servicios de Valores. Por lo tanto, sustenta todas las funciones desde el inicio y es fundamental para garantizar la transparencia y la protección de los activos. Se ofrece información adicional sobre la debida diligencia en la Sección de Riesgos, en los capítulos sobre Riesgo del Cliente y Riesgo de Proveedores Externos.

3.6.2 Conciliación e informes

Requerida en todas las etapas del ciclo de vida de los Servicios de Valores, la conciliación es un control fundamental y actúa, en efecto, como un "acuerdo" entre los diferentes participantes. La conciliación se realiza en múltiples fases del ciclo de vida, tanto antes como después de la liquidación, incluyendo la conciliación a nivel de posiciones y transacciones.

El proveedor de Servicios de Valores también proporcionará informes para garantizar que el cliente disponga de información actualizada sobre sus transacciones y posiciones. En última instancia, el proveedor de Servicios de Valores debe asegurar que los activos bajo custodia (AUC) coincidan con los registros requeridos por las infraestructuras del mercado financiero (FMI) como parte de la operación estándar. Esto se verifica, en primer lugar, a nivel de posición para cada valor y luego, dependiendo de las estructuras de cuenta aplicables a las tenencias específicas, a nivel del inversor.

3.6.3 Tecnología, soluciones e interfaces

Un proveedor de Servicios de Valores suele ofrecer acceso técnico a múltiples infraestructuras del mercado financiero (FMIs), incluyendo CCPs y (I)CSDs. También suele proporcionar acceso a participantes en la ejecución de operaciones (por ejemplo, brokers) cuando se ofrecen servicios de ejecución.

Al conectarse con un único proveedor de Servicios de Valores, un cliente puede reducir sus necesidades de interfaces de sistema y de desarrollo, aprovechando la red y la conectividad del proveedor.

4. Estructuras de cuenta

4.1 Introducción

Las estructuras de cuenta para la custodia de activos —tanto de valores como de dinero— varían a lo largo de la cadena de valor de los Servicios de Valores. Estas estructuras están determinadas por factores como los requisitos obligatorios del mercado y decisiones comerciales o estratégicas de incorporación de clientes. En este capítulo se ofrece una explicación de las estructuras de cuentas de valores y de dinero que puede adoptar un proveedor de Servicios de Valores. Se describen las distintas opciones disponibles, junto con los aspectos clave que tanto el proveedor como, potencialmente, el cliente deberá considerar al establecer una estructura de cuenta.

4.2 Definición

Una estructura de cuenta es la forma en que un proveedor de Servicios de Valores configura una cuenta. Las estructuras clave de cuentas de valores incluyen las cuentas ómnibus y las cuentas segregadas (ya sea a nivel de subcustodio y/o de CSD). Además, existen diferentes convenciones de denominación para las cuentas, incluyendo el uso de cuentas a nombre de titulares nominales (*nominees*).

4.3 Estructuras de cuentas de valores

Las estructuras de cuentas de valores varían a nivel mundial y a lo largo de la cadena de Servicios de Valores. Esta variación puede deberse a varios factores, como:

- Regulaciones y/o legislación
- Prácticas de mercado
- Preferencias comerciales u operativas de los intermediarios en la cadena
- Mercados de inversión
- Tipo de valores
- Domicilio del inversor

Las estructuras de cuenta de valores más comunes ofrecidas por los custodios incluyen:

- Cuenta ómnibus (donde se agrupan los activos de varios inversores)
- Cuenta segregada (donde los activos se separan, ya sea a nivel de subcustodio o de CSD)
- Cuenta a nombre de un titular nominal (nominee) (donde los activos pueden mantenerse en una cuenta ómnibus o segregada, pero están registrados a nombre de un nominee)

A continuación se proporciona información más detallada sobre las diferentes estructuras de cuentas de valores.

4.3.1 Estructura de cuenta ómnibus

Una cuenta ómnibus es una cuenta abierta a nombre de un custodio, ya sea a nivel de subcustodio o de CSD. Las posiciones mantenidas en esta cuenta pertenecen a múltiples clientes del custodio. En algunas jurisdicciones, aunque se permiten las cuentas ómnibus, las regulaciones exigen la segregación entre los activos de los clientes y los activos propios del custodio en el subcustodio y en el CSD. Incluso en jurisdicciones donde se permite la mezcla de activos de clientes y propios, la mejor práctica consiste en asegurarse de que estén segregados.

Para garantizar la seguridad de los activos, el custodio suele estar obligado a mantener registros en sus propios libros que reflejen la propiedad individual de cada cliente respecto de los valores mantenidos en la cuenta ómnibus. Las convenciones de denominación de cuentas ómnibus también están diseñadas para garantizar que se mantenga una protección adecuada de los activos de los clientes.

4.3.2 Estructura de cuenta segregada

En algunos mercados, la regulación —o la práctica local del mercado— determina el uso de estructuras de cuentas segregadas. Existen dos tipos diferentes de segregación que pueden adoptarse:

- Cuenta segregada a nivel de subcustodio
  Esta estructura de cuenta implica mantener los valores en una cuenta individual del beneficiario final (Ultimate Beneficial Owner, UBO) en los libros del subcustodio o, en algunas jurisdicciones, en una cuenta fiduciaria conocida como titular intermedio (Intermediate Beneficial Owner, IBO). Aunque las cuentas están segregadas en los libros del subcustodio, esta segregación no se replica ni se mantiene en el nivel del CSD, donde aún se utiliza una cuenta ómnibus (por ejemplo, a nombre del subcustodio). Sin embargo, esta cuenta ómnibus estará segregada de los activos propios del subcustodio.
- Cuenta segregada a nivel de CSD

  En este tipo de segregación, los valores se mantienen en una cuenta individual a nombre del UBO o IBO en los libros tanto del subcustodio como del CSD. Uno de los principales beneficios de esta estructura es el aumento de la transparencia en la propiedad de los activos a lo largo de toda la cadena.

Existen diferentes perspectivas respecto a las estructuras de cuentas segregadas. Dado que existen múltiples y diversas prácticas de mercado y leyes en distintas jurisdicciones, no hay un modelo global o regional coherente. Hasta que se definan más directrices legales o se revisen las leyes de valores, o se establezca una nueva normativa, la segregación suele considerarse —en algunas jurisdicciones y por parte de ciertos actores, incluidos los reguladores— como una buena práctica para mitigar el riesgo legal. No obstante, desde el punto de vista operativo, las cuentas segregadas pueden resultar menos eficientes

4.3.3 Estructura de cuenta a nombre de un titular nominal (nominee)

Un nominee es, por lo general, una empresa creada con el propósito de mantener valores en nombre de un cliente. Esta empresa mantiene los valores en fideicomiso para uno o más clientes y, frecuentemente, solo la empresa nominee aparece identificada en el registro de accionistas. Un custodio establecerá una o más empresas nominee para mantener los valores de sus clientes de Servicios de Valores.

El uso de cuentas a nombre de un nominee permite al custodio reducir la carga operativa asociada a los servicios sobre activos. Sin embargo, la utilización de un nominee conlleva solicitudes de información adicionales para identificar la titularidad de los activos.

Registrar los valores a nombre del nominee permite segregar los valores del cliente de los activos del custodio, lo que reduce el riesgo para el cliente en caso de insolvencia del custodio (por ejemplo, frente a reclamaciones de los acreedores del custodio). No obstante, la cuenta a nombre de un nominee no es reconocida en muchos mercados, donde se consideraría al nominee como el propietario legal y beneficiario final (UBO) de los valores mantenidos en la cuenta.

4.4 Estructuras de cuentas de dinero

Las estructuras de cuentas de dinero también pueden variar según el mercado y la moneda. La estructura puede estar determinada por los requisitos del mercado y/o las regulaciones. Las cuentas de dinero pueden ser proporcionadas a un cliente por un custodio y/o por un CSD.

Cuando las monedas se mantienen en el balance del custodio, pueden utilizarse cuentas ómnibus o cuentas segregadas. Sin embargo, en los mercados donde la moneda no se mantiene en el balance del custodio (por ejemplo, en el caso de ciertas monedas restringidas), las cuentas segregadas pueden ser una estructura más común.

4.4.1 Estructuras de cuentas de dinero del custodio

Los custodios proporcionan a los clientes cuentas de dinero para respaldar el movimiento, la gestión y el monitoreo de las posiciones de dinero asociadas a las transacciones de valores (conocidas como operaciones de entrega contra pago o DVP). Para ello, el custodio puede mantener las monedas dentro o fuera de su balance.

- En balance

  El custodio abrirá y operará, en sus libros y registros, una cuenta de dinero en nombre del cliente para cada moneda que mantenga en su balance (a veces denominada moneda “en libros” u “on-book”).
  En este caso, el cliente asume el riesgo de pérdida por insolvencia del depósito. Es decir, el cliente tiene un riesgo de contraparte crediticia frente al custodio

- Fuera de balance

  En ciertos mercados, el custodio mantendrá una moneda fuera de su balance (conocida como moneda “fuera de libros” u “off-book”). Esto puede deberse a que no es posible mantener la moneda en el balance (por ejemplo, en el caso de monedas restringidas) o a que no es deseable (por ejemplo, para mejorar los horarios de corte o plazos del mercado).
  En estas circunstancias, el custodio global abrirá cuentas de dinero con un subcustodio en el mercado local de la moneda, en nombre del cliente. El riesgo de pérdida por insolvencia del depósito recaerá en el subcustodio. En este ejemplo, el cliente tiene un riesgo de contraparte crediticia frente al subcustodio, lo cual estará contemplado en el acuerdo contractual entre el cliente y el custodio global.

4.4.2 Estructura de cuentas de dinero en CSD

Los CSD operan con bancos —incluidos bancos centrales— para llevar a cabo los movimientos de dinero relacionados con las actividades de liquidación del CSD y/o con los servicios sobre activos. La estructura de cuentas de dinero del CSD debe estar diseñada para ofrecer la máxima certeza respecto a la finalización de la liquidación en dinero de las operaciones con valores.

Los movimientos de dinero en un CSD pueden realizarse tanto en dinero del banco central como en dinero de bancos comerciales.

- Dinero del banco central

  El dinero del banco central se refiere al dinero mantenido en cuentas del banco central. Cuando la parte en dinero de una operación se liquida en dinero del banco central, la transacción se registra en los libros del banco central. Esto significa que las cuentas del comprador y del vendedor en el banco central se cargan y abonan, respectivamente.

La liquidación en dinero del banco central minimiza el riesgo de contraparte, ya que el banco central actúa como garante final del dinero. Esto garantiza un alto nivel de confianza y estabilidad en el sistema financiero.

- Dinero de bancos comerciales

  El dinero de bancos comerciales se refiere al dinero mantenido en cuentas de bancos comerciales o de CSDs con licencia bancaria. Este dinero es, en esencia, un depósito que puede utilizarse para transacciones con valores. Cuando la parte en dinero de una operación se liquida en dinero de bancos comerciales, la transacción se registra en los libros de un banco comercial o del CSD. Esto implica cargar y abonar las cuentas del comprador y del vendedor en dicho banco comercial.

  La liquidación en dinero de bancos comerciales conlleva un mayor riesgo de contraparte en comparación con el dinero del banco central, ya que el banco comercial o el CSD, a diferencia del banco central, pueden incurrir en impago.

  Los CSDs suelen operar con cuentas en dinero del banco central en la moneda de su jurisdicción. Las monedas extranjeras, por lo general, se gestionan a través de cuentas en dinero de bancos comerciales.

Sección 3: Riesgos en los Servicios de Valores

5. Introducción a los riesgos en los Servicios de Valores

5.1 Introducción

En este capítulo introductorio se proporciona una definición de riesgo, junto con una explicación de su aplicación desde la perspectiva de los Servicios de Valores. Además, se presentan e ilustran los principales riesgos asociados a los Servicios de Valores.

5.2 Definición

El riesgo, y más específicamente el riesgo financiero, puede definirse como la amenaza de una pérdida o un impacto negativo.

El Comité de Supervisión Bancaria de Basilea (BCBS), principal organismo mundial de normalización para la regulación prudencial de los bancos considera que los riesgos clave para los cuales los bancos deben mantener capital son el riesgo de crédito, el riesgo de mercado y el riesgo operativo. De estos riesgos prudenciales, los Servicios de Valores están predominantemente expuestos al riesgo de crédito y al riesgo operativo, siendo el riesgo de crédito en gran parte de naturaleza intradía o a corto plazo.

El BCBS define el riesgo operativo como el riesgo de pérdida resultante de procesos internos, personas o sistemas inadecuados o fallidos, o de eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional. Dentro del riesgo operativo, las directrices de Basilea recomiendan clasificar cada riesgo operativo en una de las siguientes siete categorías: fraude interno; fraude externo; prácticas laborales y seguridad en el lugar de trabajo; clientes, productos y prácticas comerciales; pérdidas de activos físicos; interrupciones del negocio; ejecución, entrega y gestión de procesos.

Esta taxonomía se ha ajustado para definir con mayor claridad cómo se aplican estas categorías de riesgo a la industria de los Servicios de Valores. Las categorías utilizadas en este informe son las siguientes:

- Riesgo regulatorio, legal y de cumplimiento
- Riesgo del cliente
- Riesgo de proveedores externos
- Riesgo de protección de activos
- Riesgo en la ejecución, entrega y gestión de procesos
- Riesgo de seguridad de la información
- Riesgo tecnológico
- Riesgo relacionado con activos digitales

Es importante señalar que las categorías de riesgo seleccionadas no son excluyentes; por ejemplo, el riesgo de proveedores externos abarca riesgos de interrupción del negocio y fraudes. Sin embargo, dado que estos riesgos pueden presentarse en múltiples momentos, se ha decidido tratarlos dentro de los capítulos correspondientes, según su relevancia, en lugar de establecerlos como una categoría independiente.

Además del riesgo operativo y el riesgo de crédito, los proveedores de Servicios de Valores también deben considerar las siguientes categorías de riesgo:

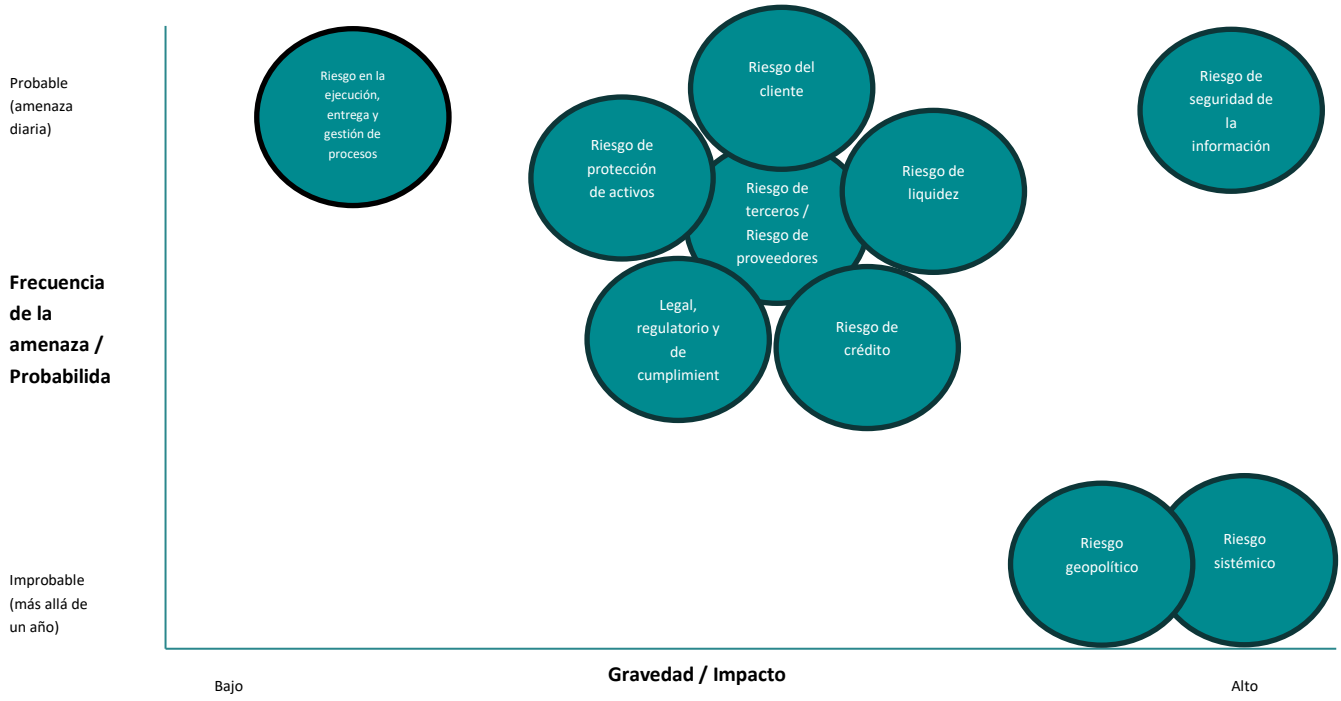
- Riesgo de liquidez
- Riesgo sistémico
- Riesgo geopolítico

Dentro de la industria de los Servicios de Valores, el riesgo de mercado es en gran medida un riesgo de segundo orden, que puede surgir como consecuencia de la materialización de un riesgo de primer nivel, como el riesgo operativo.

5.3 Categorías clave de riesgo

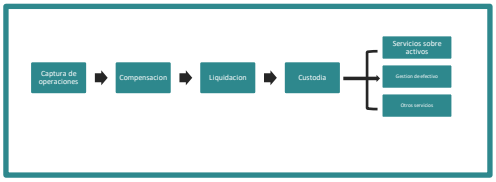
Como se ha indicado anteriormente, para los participantes en la cadena de valor de los Servicios de Valores existen múltiples riesgos para tener en cuenta. El siguiente diagrama muestra las categorías clave de riesgo desde la perspectiva de la frecuencia de la amenaza o probabilidad inherente, y de la gravedad o impacto.

Ilustración 5.3 Diagrama de las categorías clave de riesgo



6. Riesgo regulatorio, legal y de cumplimiento

6.1 Introducción



Este riesgo está presente en todas las etapas del ciclo de vida del activo y afecta a todos los participantes en la cadena de valor de los Servicios de Valores. No obstante, su alcance y naturaleza pueden variar considerablemente. Los riesgos pueden depender de varios factores, entre ellos, el rol del participante, los tipos de activos mantenidos, la(s) jurisdicción(es) y normativas en las que operan los participantes y clientes, así como los servicios involucrados.

Este capítulo busca destacar los principales temas regulatorios, legales y de cumplimiento, y analizar los riesgos y posibles medidas de mitigación en el contexto de la industria de los Servicios de Valores. No obstante, es importante que los usuarios de este informe obtengan asesoramiento actualizado en materia regulatoria, legal y de cumplimiento relevante para su actividad.

6.2 Definiciones

6.2.1 Riesgo regulatorio

El riesgo regulatorio es el riesgo de que una nueva ley o una modificación a una ley y/o normativa existente tenga un impacto significativo en una organización. Este riesgo puede surgir para un proveedor de Servicios de Valores debido a la falta de seguimiento de los cambios normativos, o a no reconocer el impacto que una nueva ley o modificación podría tener sobre su negocio y/o servicios. Estas fallas pueden dar lugar a problemas estratégicos, reputacionales, financieros, de oportunidad y operativos, así como a pérdidas.

6.2.2 Riesgo legal

El riesgo legal es el riesgo de acciones legales y/o pérdidas derivadas del incumplimiento de obligaciones contractuales. Este riesgo puede surgir para un proveedor de Servicios de Valores por un incumplimiento no intencionado o negligente de una obligación contractual. Estas fallas pueden dar lugar a litigios, así como a pérdidas financieras y/o daños reputacionales.

6.2.3 Riesgo de cumplimiento

El riesgo de cumplimiento es el riesgo legal, financiero y penal que resulta del incumplimiento de leyes y/o normativas vigentes a nivel local, regional o internacional. Los fallos de cumplimiento pueden ser institucionales o derivarse de las acciones de individuos. Este riesgo puede dar lugar, para un proveedor de Servicios de Valores, a pérdidas financieras, problemas legales y/o daños a la reputación.

6.3 Marco regulatorio, legal y de cumplimiento

La industria de los Servicios de Valores está sujeta a un entorno complejo en materia regulatoria, legal y de cumplimiento. Un proveedor de Servicios de Valores debe cumplir con diversas normativas y directrices para asegurar que lleva a cabo su actividad de manera segura y sólida, cumpliendo con las leyes y regulaciones locales, regionales y globales, y protegiendo los intereses de sus clientes.

A continuación, se destacan los factores clave que un proveedor de Servicios de Valores debe considerar al analizar el panorama regulatorio, legal y de cumplimiento, así como una tabla que presenta los principales regímenes de protección legal y de supervisión regulatoria, junto con los estándares aplicables.

6.3.1 Dirección estratégica

Una nueva regulación o ley, o un cambio en una existente, puede generar un riesgo regulatorio, pero también puede influir en la dirección estratégica que adopte una organización. Un cambio regulatorio puede representar una oportunidad para innovar en el desarrollo de productos y del mercado. Por el contrario, también puede incrementar los costos operativos, reducir el atractivo de la inversión y/o modificar el panorama competitivo para los proveedores de Servicios de Valores.

6.3.2 Conducta

La conducta es un aspecto clave en la supervisión regulatoria a lo largo de todo el ciclo de vida de los Servicios de Valores, y las organizaciones deben contar con procesos adecuados para garantizar el cumplimiento. Aunque existen muchas definiciones, el enfoque principal en materia de conducta se centra en los comportamientos y la cultura de la organización y de sus empleados. Una conducta inapropiada (por ejemplo, por ejecución indebida de actividades comerciales, fraude u otras infracciones del comportamiento profesional) puede afectar a los clientes, al mercado o a la propia empresa.

6.3.3 Acuerdos legales

Los servicios prestados por un proveedor de Servicios de Valores se describen en un contrato firmado entre el proveedor y su cliente. Un acuerdo legal bien redactado ayuda a prevenir posibles disputas y problemas legales. También puede generar confianza entre ambas partes, fortalecer la relación y derivar en oportunidades comerciales adicionales.

Los acuerdos contractuales deben estar formalizados y definir claramente los parámetros de los servicios ofrecidos y las expectativas de cada parte. En su mayoría, estos acuerdos son estandarizados. Pueden estar complementados por anexos que reflejen prácticas legales, operativas y de mercado específicas de los servicios y/o mercados correspondientes (por ejemplo, finalización de liquidaciones, gestión de colateral, préstamo de valores y definiciones relacionadas con insolvencia), así como por un acuerdo de nivel de servicio (SLA) u otro documento similar.

El proveedor de Servicios de Valores y su cliente pueden requerir la inclusión de cláusulas de protección específicas, según lo exija la legislación local y de acuerdo con el apetito de riesgo del proveedor. También puede ser necesario considerar cláusulas de responsabilidad estricta, como las exigidas por las normativas UCITS y AIFMD, e incluirlas en el lenguaje contractual para asegurar el cumplimiento normativo y la transparencia, así como la definición de responsabilidades.

Es fundamental, al acordar el contenido legal, establecer de forma justa quién asume las responsabilidades: el proveedor, el cliente o un tercero externo. No se debe esperar que el proveedor de Servicios de Valores asuma todos los riesgos y pérdidas; por ello, deben incluirse definiciones claras de responsabilidad. Algunos ejemplos incluyen la no asunción de responsabilidad por las acciones de terceros (cuando la elección del tercero depende del cliente y no del proveedor) o por pérdidas derivadas de casos de fuerza mayor.

Dado que los proveedores de Servicios de Valores son, por lo general, entidades bancarias, los criterios de suficiencia de capital (y el coste del capital) forman parte de su apetito de riesgo y de las decisiones sobre aceptación de riesgo, especialmente en lo relativo a responsabilidades e indemnizaciones. Estos proveedores deben realizar evaluaciones de impacto/probabilidad frente a ingresos/beneficios para fundamentar sus decisiones de aceptar o rechazar un determinado riesgo.

6.3.4 Protección de activos

Muchas jurisdicciones cuentan con leyes y normativas que regulan la protección de activos, con el objetivo de prevenir su pérdida debido a fraude, apropiación indebida, controles inadecuados o insolvencia. Un factor clave para mitigar el riesgo de pérdida de activos es comprender la legislación aplicable a cada contrato entre distintos proveedores de Servicios de Valores, o entre un proveedor y su cliente, así como las normativas vigentes en el país donde se contrata la actividad del cliente. Los acuerdos de interoperabilidad y equivalencia pueden garantizar que los niveles de protección de una jurisdicción se mantengan en otra, asegurando que las transferencias transfronterizas de titularidad de valores no generen consecuencias no deseadas.

6.3.5 Jurisdicción de operaciones

Las regulaciones y su implementación en la legislación local varían de una jurisdicción a otra, y el entorno normativo está en constante evolución. Por ello, es fundamental que tanto los proveedores de Servicios de Valores como sus clientes conozcan las normas aplicables en cada jurisdicción, para asegurar que los modelos de negocio existentes cumplan con los marcos regulatorios vigentes, estar al tanto de los cambios normativos y comprender cómo dichas normas afectan la responsabilidad al operar en esa jurisdicción.

Para las organizaciones globales, también es esencial entender cómo interactúan las distintas regulaciones. Cada componente de un producto debe evaluarse considerando dónde y cómo se ofrece, desglosándolo en sus elementos fundamentales e identificando desde dónde se entrega cada uno.

6.3.6 Seguridad de la información

Las leyes y normativas sobre privacidad de datos y ciberseguridad exigen que los proveedores de Servicios de Valores implementen medidas para proteger la información personal y los activos de sus clientes contra accesos no autorizados, robos o destrucción.

6.3.7 Activos digitales

Con el creciente interés en los activos digitales, deben considerarse distintos factores regulatorios, legales y de cumplimiento. Los reguladores están adaptando las normativas existentes para incorporar disposiciones legales sobre activos digitales, además de crear nuevos marcos y directrices.

6.3.8 Sostenibilidad

La sostenibilidad —también conocida como criterios Ambientales, Sociales y de Gobernanza (ESG)— ha cobrado cada vez más importancia para los clientes en los últimos años. Los proveedores de Servicios de Valores deben ser conscientes de esta necesidad y abordarla adecuadamente. Las nuevas regulaciones ESG exigen a las organizaciones cumplir con las normativas y leyes aplicables, lo que puede requerir la integración de factores ESG en sus procesos de toma de decisiones de inversión para satisfacer los objetivos ESG de sus clientes.

Los proveedores de Servicios de Valores pueden verse obligados a divulgar información sobre sus políticas y prácticas ESG a sus clientes para fomentar la transparencia y la rendición de cuentas. A su vez, los clientes suelen tener que proporcionar a su proveedor de Servicios de Valores sus propias políticas ESG.

6.4 Protección legal y supervisión regulatoria

Las autoridades financieras son responsables de desarrollar normas, directrices y otros textos regulatorios que establecen requisitos mínimos de control para gestionar los riesgos de las entidades bajo su supervisión. Además, estas autoridades también ejercen funciones de supervisión para evaluar el cumplimiento de dichas obligaciones de control por parte de las entidades cubiertas.

Dado el impacto potencial que puede tener un fallo de control por parte de un proveedor de Servicios de Valores en el mercado, las autoridades financieras aplican una supervisión rigurosa sobre las instituciones financieras que custodian y gestionan activos de clientes.

La siguiente tabla resume los principales temas dentro de la cadena de valor de los Servicios de Valores, con ejemplos de las principales regulaciones, leyes y estándares de mercado regionales y globales aplicables a la fecha de este informe. (Nota: Esta tabla no es exhaustiva y no incluye algunas normativas nacionales ni ciertas regulaciones regionales).

Ilustración 6.4 – Tabla de protección legal y supervisión regulatoria[1]

Regulación que aborda	Regulaciones / estándares	Requisitos regulatorios	Requisitos de implementación
Conducta	▪ Regulaciones de Basilea ▪ Directiva de Requisitos de Capital de la UE (CRD VI) y Reglamento de Requisitos de Capital (CRR III) ▪ Reglamento de Depósitos Centrales de Valores de la UE (CSDR) ▪ Regla Volcker de EE. UU. ▪ Normas de conducta de la Autoridad de Conducta Financiera del Reino Unido (FCA) ▪ Normas de conducta empresarial de la Comisión de Bolsa y Valores de EE. UU. (SEC) ▪ Directiva suiza sobre recuperación y resolución bancaria ▪ Principios sobre activos de clientes de IOSCO ▪ Ley Dodd-Frank de EE. UU.	▪ Nuevas normas para operar con ciertos fondos (imposibilidad de conceder crédito / segregación) ▪ Identificación y gestión de funciones económicas críticas ▪ Protocolos de recapitalización interna (bail-in) / suspensión de pagos (stay protocols) ▪ Costes operativos – requisitos de capital ▪ Gobernanza y supervisión centralizadas	▪ Gestión mejorada de la liquidez intradía ▪ Procesos mejorados de monitoreo del crédito ▪ Requisitos reforzados de capital y pruebas de resistencia (stress test) ▪ Medidas de apoyo para la recapitalización interna (bail-in) de pasivos y obligaciones ▪ Régimen mejorado de riesgos y gobernanza en la segregación de funciones ▪ Revisión legal
Protección de activos	▪ UCITS (Organismos de Inversión Colectiva en Valores Mobiliarios) de la UE ▪ Directiva sobre Gestores de Fondos de Inversión Alternativos (AIFMD) ▪ Reglamento de Infraestructura del Mercado Europeo (EMIR) ▪ Reglamento de Depósitos Centrales de Valores (CSDR) ▪ Directiva sobre Mercados de Instrumentos Financieros de la UE (MiFID) ▪ Manual de activos de clientes del Reino Unido (CASS) ▪ Regla de salvaguarda de la SEC (EE. UU.) ▪ Organización Internacional de Comisiones de Valores (IOSCO) ▪ Ley alemana de custodia segura de valores (Safe-Custody Act)	▪ Leyes que regulan los acuerdos con clientes ▪ Acuerdos de interoperabilidad y equivalencia	▪ Revisión legal de normativas / leyes en distintas jurisdicciones ▪ Requisitos operativos como conciliación, reportes y segregación de cuentas

[1] Nota del Editor: estas regulaciones son obligatorias para servicios prestados en Estados Unidos y Europa. Sin embargo, es importante que entidades en otras jurisdicciones conozcan brevemente las mismas, por un lado por ser considerados mejores prácticas, y por otra parte porque estas entidades se lo exigirán aunque el servicio sea prestado en otro país.

Regulación que aborda	Regulaciones / estándares	Requisitos regulatorios	Requisitos de implementación
Diligencia debida del cliente y prevención del blanqueo de capitales / financiación del terrorismo (AML / AFC)	▪ Reglamento sobre Transferencias de Fondos ▪ Directiva contra el blanqueo de capitales (AML) ▪ Directiva sobre abuso de mercado de la UE ▪ Ley de cumplimiento fiscal de cuentas extranjeras de EE. UU. (FATCA) ▪ Norma común de reporte (CRS) ▪ Principios de ISSA sobre delitos financieros	▪ Diligencia debida reforzada de KYC y monitoreo continuo del cliente ▪ Controles reforzados para cuentas ómnibus ▪ Equivalencia de terceros países	▪ Mejoras en la tecnología de filtrado de mensajes ▪ Parámetros adicionales en los mensajes para identificar al beneficiario final ▪ Controles KYC reforzados / evaluación del riesgo de idoneidad del producto y del cliente
Resiliencia operativa	▪ MiFID de la UE (Directiva sobre Mercados de Instrumentos Financieros) ▪ Reglamento de Resiliencia Operativa Digital de la UE (DORA) ▪ Regulación sobre resiliencia operativa del Reino Unido ▪ Guía CPMI-IOSCO sobre resiliencia cibernética para infraestructuras del mercado financiero (FMIs) ▪ Gestión de la continuidad del negocio de la Autoridad Monetaria de Singapur ▪ Manual de políticas de supervisión OR-2 de la Autoridad Monetaria de Hong Kong ▪ Prácticas sólidas de los reguladores de EE. UU. (FRB / OCC / FDIC) para fortalecer la resiliencia operativa	▪ Mayor diligencia debida y supervisión de los proveedores externos de TIC (tecnología de la información y las comunicaciones) ▪ Controles cibernéticos mínimos y actividades de evaluación de riesgos ▪ Identificación y mapeo de las operaciones críticas de la entidad financiera y de los terceros que las respaldan ▪ Definición de la tolerancia a la disrupción (tolerancia al impacto) para las operaciones críticas	▪ Revisión de los acuerdos contractuales con proveedores internos y externos de TIC ▪ Revisión de los programas cibernéticos actuales utilizados para evaluar el entorno TIC conforme a los requisitos mínimos de control de DORA ▪ Desarrollo e implementación de un marco para mejorar continuamente la resiliencia operativa de las operaciones críticas identificadas
Ejecución y compensación	▪ Diversas normas sobre índices financieros de referencia ▪ MiFID II / MiFIR de la UE (Directiva y Reglamento sobre Mercados de Instrumentos Financieros) ▪ EMIR de la UE (Reglamento sobre Infraestructuras del Mercado Europeo) ▪ SFTR de la UE (Reglamento sobre Transacciones de Financiación de Valores)	▪ Diligencia debida reforzada previa y posterior a la negociación ▪ Compensación obligatoria de determinados instrumentos ▪ Normas de segregación de activos ▪ Equivalencia de terceros países ▪ Aumento de los requisitos de reporte	▪ Marco de riesgos y controles reforzado ▪ Divulgación / elección de estructuras de cuenta ▪ Gestión mejorada de liquidez / colateral ▪ Gestión en tiempo real del crédito / márgenes ▪ Categorización de clientes, controles de Conozca a su Cliente (KYC) / Conozca su Producto (KYP)
Liquidación	▪ CSDR de la UE (Reglamento de Depósitos Centrales de Valores) ▪ Target2-Securities (T2S) de la UE ▪ Armonización de la liquidación en la UE ▪ Liquidación T+2 en EE. UU. y Asia-Pacífico (APAC) ▪ CASS de la SEC (Reglamento sobre activos de clientes de la SEC)	▪ Penalizaciones obligatorias por fallos en la liquidación / mecanismos de recompra (buy-ins) ▪ Autorización de los CSDs ▪ Normas de segregación de activos	▪ Controles mejorados de disciplina de liquidación ▪ Cambios tecnológicos / conectividad ▪ Monitoreo mejorado del desempeño de los clientes ▪ Comprensión de los regímenes de equivalencia

		▪ Transparencia de las transacciones internas	
Custodia, seguridad de los activos y fondos	▪ EU: UCITS (para fondos) ▪ EU: AIFMD (para alternativos) ▪ US Safeguarding Rule (para fondos) ▪ EU MiFID II Safeguarding ▪ UK CASS	▪ Normas de segregación de activos ▪ Régimen de responsabilidad / indemnización ▪ Normas sobre la custodia de activos	▪ Revisión de las cláusulas de protección legal y del régimen de responsabilidad e indemnización ▪ Nueva estructura de cuentas / modelo operativo y controles de apoyo
Servicios sobre activos	▪ Directiva de Derechos de los Accionistas de la UE (SRD II) ▪ Diversos regímenes de votación nacionales ▪ Estándares de puntuación del Banco Central Europeo (BCE)	▪ Clasificación de clientes ▪ Aumento de los requisitos de reporte	▪ Mejoras en los controles KYC

Regulación que aborda	Regulaciones / estándares	Requisitos regulatorios	Requisitos de implementación
Fiscalidad / Impuestos	▪ Impuesto a las transacciones financieras de EE. UU. (FTT) ▪ Directiva de armonización de la retención en la fuente (WHT) de la UE ▪ Diversos regímenes de certificados de residencia fiscal	▪ Clasificación de clientes ▪ Requisitos de retención fiscal ▪ Aumento de los requisitos de reporte	▪ Mejoras en los procesos fiscales
Seguridad de la información y protección de datos	▪ Reglamento General de Protección de Datos de la UE (RGPD / GDPR) ▪ Regla cibernética de la SEC de EE. UU. ▪ Marco de ciberseguridad de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ▪ Ley de ciberseguridad de la UE ▪ Reglamento de resiliencia operativa digital de la UE (DORA) ▪ Directivas de seguridad de redes y sistemas de información de la UE (NIS 1 y NIS 2)	▪ Divulgar incidentes cibernéticos relevantes	▪ Informes y procedimientos mejorados ▪ Pruebas tecnológicas
Digital Assets	▪ Reglamento de la UE sobre Mercados de Criptoactivos (MiCA) ▪ Régimen piloto de la UE sobre tecnología de registro distribuido (DLT) ▪ Marco prudencial del Banco de Pagos Internacionales (BIS) para activos digitales ▪ Recomendaciones políticas de IOSCO ▪ Reglamento del Boletín de Contabilidad del Personal (SAB 121) de EE. UU. ▪ Borrador de circular de la HKMA sobre activos digitales ▪ Marco del Tesoro de Australia sobre activos digitales	▪ Incorporación de normativas existentes adaptadas para cubrir los activos digitales	▪ Introducción de marcos normativos que integran los activos digitales
Sustainability	▪ EU Regulación de Reglamento de divulgación de información sobre finanzas sostenibles (SFDR) ▪ EU Directiva sobre información corporativa de sostenibilidad (CSRD)	▪ Requerimientos de divulgación ▪ Incremento de requerimientos de divulgación	▪ Mejoras en procesos operacionales y de información

6.5 Amenazas de riesgo regulatorio, legal y de cumplimiento

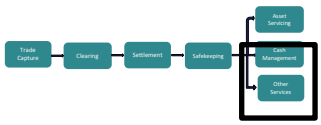
Como ya se ha mencionado, el panorama regulatorio, legal y de cumplimiento es complejo y existen múltiples factores que los proveedores de Servicios de Valores deben tener en cuenta. La siguiente tabla describe los principales riesgos regulatorios, legales y de cumplimiento, así como posibles medidas de mitigación.

Ilustración 6.5 – Tabla de riesgos regulatorios, legales y de cumplimiento

Descripción del riesgo	Mitigación del riesgo
Proveedor de Servicios de Valores con una gobernanza ineficaz	Establecer un régimen interno adecuado de la alta dirección, junto con una estrategia de cumplimiento y gestión de riesgos, para garantizar el gobierno eficaz y el cumplimiento de las normativas y de los requisitos derivados de cambios regulatorios Implementar un conjunto integral de informes de gestión que incluya, entre otros: indicadores clave de riesgo (KRI), indicadores clave de rendimiento (KPI) y acuerdos de nivel de servicio (SLA) Organizar formaciones para asegurar que el personal comprenda sus responsabilidades y conozca los procedimientos de actuación y escalamiento en caso de que se identifique una infracción
No se lleva a cabo una participación activa en relación con los cambios en normativas o leyes	Analizar el entorno regulatorio / legal en busca de cambios próximos Realizar un análisis inicial del impacto de los posibles cambios Participar en las consultas públicas de los reguladores sobre nuevas normativas o regulaciones propuestas Defender y representar intereses ante legisladores / organismos reguladores, ya sea directamente o a través de asociaciones del sector o comerciales
No se gestiona la preparación ante los cambios en normativas o leyes	Realizar un análisis del impacto de los cambios regulatorios / legales sobre el modelo de negocio actual, las operaciones, la tecnología y los clientes Llevar a cabo una evaluación de "riesgo vs retorno" para determinar el apetito de riesgo de continuar con la actividad frente a la rentabilidad financiera Revisar posibles oportunidades de nuevos productos Involucrar a los equipos de operaciones, tecnología, producto y líneas de negocio en la preparación para el cambio
Los cambios regulatorios o legales no se implementan adecuadamente	Utilizar herramientas del marco de gestión de riesgos, como indicadores clave de riesgo (KRI) y autoevaluaciones de control de riesgos (RCSA), para evaluar el riesgo de ejecución de proyectos, el riesgo operativo y el perfil de riesgo del negocio Implementar métricas, incluidos indicadores clave de rendimiento (KPI), para medir la calidad de la implementación
No se evalúan las relaciones con los clientes y los proveedores externos	Considerar desde el inicio —y de forma continua— la información o los datos necesarios para cumplir con la normativa en el marco de una relación con un cliente o proveedor externo (por ejemplo, clasificación del cliente según MiFID, normas sobre sanciones, situación fiscal)
No se acuerdan los términos apropiados con los clientes y los proveedores externos	Realizar un Conozca a Su Cliente (KYC) o Conozca su Proveedor (KYP) Completar una Evaluación de la idoneidad y pertinencia del producto/cliente Revisar las capacidades operativas Completar una Evaluación de Capital y Crediticio Asegurarse que se cumplen todas las consideraciones regulatorias (tales como UCITS / AIFMD / FATCA / VOLCKER / MiFID / DGSD) Introducir en los acuerdos legales la cobertura de riesgos Acordar consideraciones ambientales, sociales y de gobierno (ESG)
El cambio de titularidad legal no se completa de manera oportuna (particularmente en el caso del préstamo de valores)	Asegurar que la documentación legal contemple adecuadamente la capacidad de transferir la titularidad

7. Riesgo del Cliente

7.1 Introducción



El riesgo del cliente puede surgir cuando un proveedor de Servicios de Valores, o un cliente, no ha tomado las medidas necesarias para evaluar la idoneidad de la otra parte antes de iniciar una relación. Estos riesgos también pueden manifestarse cuando las partes no se supervisan mutuamente de forma continua.

Este capítulo se centra en describir el riesgo del cliente y las medidas que deben tomar tanto los proveedores de Servicios de Valores como los clientes para garantizar que este riesgo se mitigue. Se explican medidas como la diligencia debida y el proceso de Conozca a su Cliente (KYC), y se detallan los principales mecanismos de mitigación del riesgo. Cabe señalar que los riesgos que deben evaluarse durante el proceso de incorporación, como el riesgo de crédito o el riesgo de seguridad de la información y protección de datos, también se desarrollan en detalle en otros capítulos de este informe.

7.2 Definición

El riesgo del cliente se refiere a los riesgos que enfrenta un proveedor de Servicios de Valores al incorporar un nuevo cliente según criterios de selección, así como al riesgo de prestarle servicios de forma continua. También se refiere a los riesgos que asume un cliente al establecer y mantener una relación con un proveedor de Servicios de Valores.

7.3 Panorama del riesgo del cliente

Tras la crisis financiera de 2008, varios reguladores globales y regionales reforzaron las normas de "idoneidad y conveniencia" con el fin de mejorar la protección del inversor y crear un mercado de Servicios de Valores más seguro y armonizado. En el centro de estas mejoras están las medidas que debe adoptar un proveedor de Servicios de Valores para garantizar que los productos y servicios sean transparentes y adecuados para el cliente y, del mismo modo, que el cliente sea evaluado por su idoneidad por parte del proveedor. Además, las normativas exigen sistemáticamente mayor transparencia, con nuevos requisitos que obligan al proveedor de Servicios de Valores a enviar información detallada a los clientes sobre los costes y cargos, lo cual debe estar respaldado por una descripción completa.

En los últimos años, también ha aumentado la atención sobre la aplicación de sanciones y las medidas contra el terrorismo. La complejidad de las cadenas de tenencia de valores ha llevado a los reguladores a adoptar nuevos estándares, especialmente relevantes para las cuentas ómnibus que ocultan la titularidad real de partes sancionadas mediante sus "capas". Un proveedor de Servicios de Valores debe asegurarse de que las evaluaciones de KYC (Conozca a su cliente) y de idoneidad y conveniencia profundicen en la base de inversores de los clientes potenciales y que, como mínimo, existan controles para realizar estas evaluaciones de forma continua.

7.4 Diligencia debida

La diligencia debida es el proceso mediante el cual una organización evalúa a otra parte recopilando y analizando información sobre ella para garantizar su idoneidad. Tanto para los proveedores de Servicios de Valores como para los clientes, estas medidas son clave para mitigar el riesgo del cliente. El cumplimiento de las medidas pertinentes implica una articulación clara de responsabilidades, obligaciones, cláusulas de exención y divulgaciones en el contrato.

Aunque la diligencia debida es una parte fundamental del proceso de incorporación, también es necesario realizar diligencia debida de forma continua durante toda la vigencia de la relación. Por lo tanto, tanto los proveedores de Servicios de Valores como los clientes deberán contar con un conjunto sólido de controles para supervisar el desempeño de la otra parte y tener la capacidad de congelar o limitar la actividad en caso de que la contraparte muestre señales de dificultad, comportamiento inapropiado o deterioro en su solvencia crediticia.

7.4.1 Responsabilidades de diligencia debida del proveedor de Servicios de Valores

Antes de formalizar completamente una relación con un cliente, un proveedor de Servicios de Valores debe cumplir con una serie de criterios, con el fin de limitar el riesgo y la exposición tanto para sí mismo como para evitar posibles efectos de contagio dentro del ciclo de vida del activo. Las medidas deben evaluarse y acordarse como parte de un proceso de aprobación de "nuevos negocios" antes de que la actividad entre ambas partes pueda comenzar, y también deben revisarse durante el transcurso de la relación.

Las responsabilidades clave en materia de diligencia debida incluyen, entre otras, las siguientes:

- Evaluación del cliente
- Evaluación de la entidad jurídica del proveedor de Servicios de Valores
- Proceso de aceptación del cliente
- Consideraciones ambientales, sociales y de gobernanza (ESG)

Los proveedores de Servicios de Valores también tienen la responsabilidad de evaluar a sus proveedores externos. Véase el Capítulo 8 para más información.

7.4.1.1 Evaluación del cliente

El proveedor de Servicios de Valores debe tomar medidas claras para evaluar a cada cliente. Esto debe incluir conocer al cliente —comúnmente referido como "Conozca a su cliente" (KYC, por sus siglas en inglés)— así como comprender el conocimiento y la experiencia del cliente.

Los requisitos de KYC son un área de atención común y prioritaria para los reguladores a nivel global. De hecho, el KYC puede adoptar muchas formas y existen múltiples aspectos a considerar. Los riesgos reputacionales y financieros derivados de fallos en la prevención del blanqueo de capitales (AML) aumentan la presión para garantizar que los procesos de KYC, tanto en la evaluación inicial como en la continua del cliente, sean sólidos e infalibles.

Al cumplir con los requisitos de KYC, se deben tener en cuenta, entre otros, los siguientes aspectos:

- Tipo de institución: intermediario financiero, fondo de cobertura, firma de inversión, etc.
- Solvencia crediticia
- Personas políticamente expuestas (PEP)
- Lista de embargo
- Estructura de gestión
- País de domicilio del cliente y cualquier requisito KYC específico del país (por ejemplo, FATCA, Volcker, AMLD)
- Cualquier restricción en el mercado de negocio previsto (por ejemplo, normativas del mercado nacional frente al internacional)
- Expectativas contractuales del cliente (consideración de exclusiones a la terminología legal estándar y cláusulas de protección en relación con el apetito de riesgo)
- Relación entre riesgo y retorno que presenta el cliente (margen y crecimiento frente al apetito de riesgo)

Además, el proveedor de Servicios de Valores debe solicitar al cliente potencial que proporcione información sobre su conocimiento y experiencia, con el fin de poder evaluar si el servicio o producto es adecuado para él. Aunque al principio las implicaciones pueden no ser evidentes, el impacto natural será un riesgo reputacional y la posibilidad de riesgo operativo (pérdidas, errores, litigios e incumplimientos normativos).

Las áreas de atención deben incluir, entre otras, las siguientes:

- Idoneidad del cliente
  - Determinar si el cliente potencial requiere el servicio estándar proporcionado por el proveedor de Servicios de Valores
  - El marco regulatorio y legal, por ejemplo, el riesgo país y la aplicabilidad de las disposiciones en los acuerdos legales
  - Historial de desempeño y cumplimiento de normas regulatorias y de buenas prácticas
  - Cualquier implicación en incumplimientos a la integridad de los mercados financieros, incluidos abuso de mercado, delitos financieros y actividades de blanqueo de capitales
  - Reputación, incluida la base de clientes
- Capacidad operativa
  - Estrategia de negociación prevista, incluyendo volumen, base de clientes, mercado, tipo de operación y productos
  - Procedimientos y controles internos adecuados al propósito, conforme a las normativas regulatorias y estándares de mercado vigentes
  - Capacidad operativa y de sistemas en relación con los volúmenes y la complejidad de productos
  - Recursos operativos, incluidas interfaces/conectividad tecnológica
  - Sistemas internos de control de riesgos
  - Planes de contingencia y disposiciones de recuperación y resolución
- Idoneidad en términos de crédito y liquidez
  - Fortaleza financiera suficiente para respaldar el negocio propuesto, anticipar fondos y/o obtener líneas de crédito
  - Requisitos de colateral
  - Sistemas y acuerdos de pago que permitan a los clientes transferir de forma oportuna los activos o dinero requeridos (como margen)
  - Sistemas y/o acceso a información que ayude a los clientes a respetar cualquier límite máximo de negociación

7.4.1.2 Evaluación de la entidad jurídica del proveedor de Servicios de Valores

Tras realizar una evaluación general del cliente, el proveedor de Servicios de Valores debe evaluar el riesgo del negocio del cliente y comprender si la entidad jurídica a la que se prevé prestar los servicios dispone de recursos financieros adecuados.

Los factores a considerar incluyen:

- Capital suficiente para cubrir los riesgos (es decir, hasta qué punto se requerirá el depósito o retiro de dinero del balance del banco y una evaluación de las implicaciones sobre el uso del capital)
- Comprensión de las necesidades de liquidez del cliente
- Evaluación de los riesgos operativos

El capital por riesgo operativo se determina a menudo en función de un factor sobre los ingresos percibidos por la prestación del servicio, o bien mediante la modelización de pérdidas internas y externas relevantes, y el análisis de escenarios basados en riesgos.
Cabe señalar que ciertos proveedores de Servicios de Valores —específicamente los grandes custodios globales— han sido designados como Instituciones Financieras de Importancia Sistémica Global (SIFIs, por sus siglas en inglés). Como consecuencia, estas organizaciones están sujetas a mayores exigencias regulatorias en materia de estabilidad financiera, incluyendo mayores requisitos de capital, liquidez y capacidad de resolución.

7.4.1.3 Proceso de aceptación del cliente

Una vez finalizada la diligencia debida detallada anteriormente, el proveedor de Servicios de Valores normalmente debe seguir un proceso de toma de decisiones conforme a sus marcos de gobernanza. Este proceso, comúnmente conocido como “aceptación del negocio”, consiste en presentar la información pertinente para su aprobación. Dichos procesos deben contar con una representación equilibrada de personas con suficiente experiencia y nivel jerárquico provenientes de distintas áreas (como gestión de riesgos, operaciones, cumplimiento, negocio y finanzas) que garanticen decisiones justas, imparciales y con la aprobación adecuada de la entidad jurídica. En caso de que no se logre una decisión, las excepciones pueden ser escaladas a un comité superior. También puede existir un proceso específico de aprobación de operaciones para evaluar nuevos negocios en fases tempranas.

7.4.1.4 Evaluación ambiental, social y de gobernanza (ESG)

Dada la creciente importancia de los factores Ambientales, Sociales y de Gobernanza (ESG) en la industria financiera, un proveedor de Servicios de Valores puede desear —y en algunos mercados está obligado— evaluar a su cliente en función de su apetito interno de riesgo ESG. Esta evaluación puede incluir la verificación de nombres en bases de datos que recopilan información sobre noticias negativas relacionadas con ESG, así como la identificación de vínculos con sectores industriales asociados a impactos ambientales adversos. Esta evaluación puede realizarse de forma independiente o como parte de un proceso más formalizado, siguiendo un modelo de gobernanza similar al utilizado en las revisiones de KYC.

7.4.2 Responsabilidades de diligencia debida del cliente

Al seleccionar y designar a un proveedor de Servicios de Valores, el propio cliente tiene la responsabilidad de llevar a cabo su propia diligencia debida. También debe asegurarse completamente —y a su vez asegurar al proveedor de Servicios de Valores— de que comprende el(los) producto(s) y servicio(s) que se le van a prestar.

Un enfoque comúnmente utilizado durante este proceso es el uso de una solicitud de propuesta (RFP). Este proceso implica la revisión del proveedor de Servicios de Valores, su estructura, gestión, capacidades de control / reporte y la gama de servicios de apoyo ofrecida. Dicha evaluación exhaustiva —que puede realizarse bajo un acuerdo de confidencialidad (NDA)— es fundamental para garantizar que la parte delegada o designada tiene la capacidad de respaldar adecuadamente el negocio.

Las áreas de atención podrían incluir, entre otras:

- Capital (ICAAP, divulgación pública del Pilar 3 de Basilea) para evaluar si cuenta con suficiente fortaleza financiera para respaldar el negocio del cliente
- Marco regulatorio y legal y aplicabilidad de las disposiciones contenidas en los acuerdos legales
- Divulgación de resultados anuales, informes de auditoría e informes de control emitidos por el proveedor de Servicios de Valores y auditados externamente (como SAS70, SSAE16 e ISAE 3402)
- Marco de gobernanza, incluyendo la estructura directiva y del consejo
- Política de gestión de riesgos y marco de control; divulgación de políticas y procedimientos
- Historial de desempeño y cumplimiento de las normas regulatorias y de mejores prácticas
- Planes de contingencia y disposiciones de recuperación y resolución
- Reputación, incluida la base de clientes
- Capacidad y funcionalidad operativa y de sistemas en relación con los volúmenes y la complejidad de productos
- Estructura de cuentas, incluyendo conformidad con requisitos de segregación

Cualquier solicitud dirigida al proveedor de Servicios de Valores tiene como objetivo proporcionar al cliente una visión clara de la calidad y sostenibilidad de las operaciones ofrecidas por el proveedor. No obstante, debe tenerse en cuenta que el proveedor solo podrá compartir información pública y no propietaria, salvo que esté específicamente cubierta bajo un NDA. El proveedor tiene la responsabilidad de asegurar que la información no pública relativa a sus operaciones —y, por supuesto, a otros clientes— permanezca confidencial. Se recomienda revisar la información recopilada al menos una vez al año o de forma dinámica durante la relación.

7.5 Amenazas de riesgo del cliente

Existen múltiples riesgos relacionados con el cliente que pueden surgir al establecer y mantener una relación entre un proveedor de Servicios de Valores y un cliente. A continuación, se describen las amenazas clave de riesgo aplicables a ambas partes, junto con posibles medidas de mitigación que podrían considerarse.

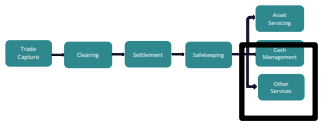
Ilustración 7.5 – Tabla de riesgos del cliente

Descripción del riesgo	Mitigación del riesgo
Incumplimiento del proveedor de Servicios de Valores en la realización de controles iniciales y continuos de AML/KYC sobre el cliente y los beneficiarios finales (UBOs – Ultimate Beneficial Owners)	▯ Implementar políticas y procedimientos KYC sólidos, incluidas revisiones periódicas con frecuencias basadas en riesgos e implicaciones claras y transparentes para suspender los servicios si la información requerida no se proporciona dentro de los plazos. ▯ Crear procesos para garantizar que se puedan divulgar los detalles del UBO y que se realicen las revisiones y los análisis KYC requeridos en toda la cadena de valor de los Servicios de Valores (consulte los Principios de cumplimiento de delitos financieros de la ISSA)

Descripción del riesgo	Mitigación del riesgo
Incumplimiento del proveedor de Servicios de Valores o del cliente en la supervisión continua de la relación	▪ Implementar y aplicar procedimientos de control para supervisar continuamente a las partes contratantes, tales como: ○ Solvencia crediticia continua ○ El marco de gobernanza ○ Cumplimiento de las regulaciones y normas pertinentes ○ Evaluación de sanciones ○ o Perfil comercial, uso de la cuenta y evaluación del volumen de transacciones frente a las expectativas
Incumplimiento del proveedor de Servicios de Valores o del cliente en identificar un modelo operativo de servicio no estándar / procesos manuales de alto riesgo	▪ Asegurar que el proceso de incorporación incluya una revisión detallada por parte de expertos operativos del proveedor de Servicios de Valores para identificar dónde el cliente ha solicitado procesos no estándar ▪ Colaborar con el cliente para acordar e implementar enfoques automatizados ▪ Asegurar que el cliente complete un proceso exhaustivo de solicitud de propuesta (RFP – Request for Proposal)
No se implementa un acuerdo contractual sólido	Implementar un acuerdo que detalle la relación contractual entre el proveedor de Servicios de Valores y el cliente antes de la incorporación del negocio, y modificarlo en caso de un cambio en el modelo de negocio o en los requisitos Asegurar una documentación clara de las responsabilidades, indemnizaciones, terminación, confidencialidad, seguridad, resiliencia, representaciones y garantías
Falta de licencias, capacidades y recursos financieros adecuados para el Cliente	Asegurar que el proceso de incorporación cuente con principios de asignación claros, que consideren el país de domicilio y las licencias del cliente frente a las licencias y autorizaciones de la entidad legal del proveedor de Servicios de Valores que presta los servicios Considerar que las implicaciones de riesgo financiero (como los depósitos en balance y los requisitos de crédito) estén suficientemente cubiertas para el cliente por la entidad legal del proveedor de Servicios de Valores que presta los servicios
Configuración de la cuenta de cliente inadecuada por el proveedor de servicios de valores	Asegurar que existan procesos de control que verifiquen que las cuentas de dinero y valores no puedan ser activadas ni por el proveedor de Servicios de Valores ni por el cliente sin que existan acuerdos debidamente formalizados Asegurar que existan procesos de control para verificar la correcta configuración de las cuentas del cliente y los requisitos de datos estáticos por parte del proveedor de Servicios de Valores Implementar paquetes de información para el cliente por parte del proveedor de Servicios de Valores, a fin de que el cliente confirme la configuración correcta, así como establecer procesos periódicos de confirmación de datos estáticos
Procesos inadecuados de fijación de aranceles, aplicación de tipos de interés y facturación para el cliente	Asegurar que exista un proceso de control para confirmar que la fijación de precios por parte del proveedor de Servicios de Valores sea adecuada para el cliente en relación con el coste y el riesgo (considerando cualquier proceso manual no estándar de alto riesgo y protecciones contractuales reducidas) Asegurar que exista un proceso de control, realizado por expertos operativos del proveedor de Servicios de Valores, para confirmar que el enfoque de facturación siga un modelo estandarizado y automatizado para el cliente

8. Riesgo de proveedores externos

8.1 Introducción



Cuando un proveedor externo ofrece servicios esenciales a un proveedor de Servicios de Valores —que forman parte intrínseca de la oferta de Servicios de Valores para los clientes— es necesario gestionar varios riesgos.

Es fundamental que el proveedor de Servicios de Valores evalúe tanto la idoneidad como la adecuación de cada proveedor externo. Esto no solo desde la perspectiva del nivel de servicio y del riesgo, sino también porque existe un creciente enfoque regulatorio en la gobernanza de terceros, la subcontratación, la resiliencia operativa y la continuidad del negocio. Por lo tanto, la formalización y el fortalecimiento de los acuerdos tanto externos como internos con proveedores externos es una prioridad clave dentro de la planificación de recuperación y resolución.

8.2 Definición

Un proveedor externo es una entidad que proporciona funciones, capacidades o servicios a un proveedor de Servicios de Valores, pero que no forma parte directa de las actividades realizadas por dicho proveedor. El proveedor externo puede ser una entidad ajena al proveedor de Servicios de Valores o una entidad legal diferente dentro de la misma organización. También pueden existir proveedores en cadena (por ejemplo, proveedores de cuarto o quinto nivel), los cuales deben ser igualmente incluidos dentro de este marco.

8.3 Servicios de proveedores externos

- Los servicios y funciones comunes que los proveedores externos ofrecen a los proveedores de Servicios de Valores incluyen, entre otros:
- Servicios de subcustodia
- Externalización de procesos empresariales (BPO – Business Process Outsourcing)
- Proveedores de servicios especializados (como servicios de voto por poder y servicios de presentación / reclamo de impuestos)
- Proveedores de datos que suministran información como:
  - Cotizaciones de acciones y tipos de cambio
  - Datos de referencia de instrumentos y datos de eventos corporativos
  - Instrucciones estándar de liquidación e identificadores de entidades legales
  - Calificaciones crediticias y datos de mercado
- Servicios de mensajería y comunicación como SWIFT
- Servicios y aplicaciones tecnológicas tales como:
  - Sistemas operativos centrales (sistemas de back-office)
  - Servicios de gobernanza corporativa como plataformas de voto por poder
  - Sistemas financieros
  - Sistemas de conciliación
- Servicios de supervisión de redes de subcustodios (Network Management)
- Plataformas de conciliación de operaciones / liquidación, procesamiento de instrucciones e informes

8.3.1 Externalización

Un tipo de servicio de terceros es la externalización. La externalización se refiere a un acuerdo entre un proveedor de Servicios de Valores y un proveedor externo mediante el cual este último lleva a cabo un proceso, función o actividad que, de otro modo, sería realizado por el propio proveedor de Servicios de Valores.

A lo largo de la cadena de valor de los Servicios de Valores, prácticamente todos los participantes tienen la posibilidad de externalizar actividades a un proveedor externo, siempre que no existan restricciones regulatorias o contractuales. Sin embargo, aunque el proceso empresarial pueda ser externalizado, el proveedor de Servicios de Valores sigue siendo responsable y debe mantener una supervisión adecuada de la entidad que presta el servicio, de los resultados de su procesamiento y ser capaz de gestionar los riesgos que surjan como resultado de haber delegado en un proveedor externo, incluida la continuidad del negocio.

8.3.2 Red de subcustodios

Una función crítica para un proveedor de Servicios de Valores es la capacidad de acceder a mercados nacionales para respaldar los requisitos de inversión de sus clientes. Esto es especialmente relevante para los custodios globales que proporcionan a sus clientes conectividad "global" y para los I(CSD) que ofrecen acceso directo a instituciones elegibles para transmitir y mantener valores sin necesidad de abrir cuentas en cada CSD nacional.

Para acceder a mercados nacionales, un proveedor de Servicios de Valores puede utilizar su propia red de subcustodios, conectarse directamente con el CSD o contratar proveedores externos a nivel local. Cuando se utiliza un subcustodio, este actúa como intermediario con el CSD, opera las cuentas donde se mantienen finalmente los activos y transmite todas las instrucciones relevantes recibidas del proveedor de Servicios de Valores. De manera similar, el ICSD accederá a los mercados nacionales mediante un subcustodio o mediante una relación directa con el CSD nacional, conocidas como "conexiones entre CSDs" (CSD links).

El grupo de Gestión de Red de Subcustodios de un proveedor de Servicios de Valores desempeña una función crítica de gestión de terceros. Tiene la responsabilidad de gerenciar las distintas relaciones con subcustodios conforme a una política de gestión de red acordada. El proveedor de Servicios de Valores tendrá un marco similar para gestionar y supervisar su red de CSDs, y los ICSDs contarán con un equipo similar para supervisar sus propias relaciones con subcustodios. Muchas de las funciones de supervisión llevadas a cabo por la Gestión de Red de Subcustodios son fundamentales para garantizar la seguridad de los activos, la eficiencia operativa y el cumplimiento normativo.

Alternativamente, los proveedores de Servicios de Valores que utilizan subcustodios externos pueden decidir delegar la función de supervisión en un proveedor externo (como una consultora especializada). En estos casos, el proveedor de Servicios de Valores sigue siendo responsable de supervisar esa actividad y de gestionar los riesgos derivados de haber delegado en un proveedor externo.

La función de Gestión de Red de Subcustodios puede ser una unidad independiente dentro del proveedor de Servicios de Valores, pero trabaja estrechamente con las áreas de negocio, tecnología y operaciones. Tiene una responsabilidad definida sobre diversos proveedores externos. Esto incluye típicamente la selección, diligencia debida, documentación, evaluación de desempeño y riesgos de subcustodios, CCPs, CSDs y bancos Nostro (cuentas de dinero), así como la supervisión de las plataformas gestionadas por la función de Gestión de Red. Este equipo también posee un conocimiento profundo de los mercados nacionales, lo cual es esencial para la protección de activos, la eficiencia operativa y la inteligencia de negocio.

El equipo de red contará con experiencia en mercados nacionales y conocimiento de las convenciones y regulaciones locales, siendo una parte integral del servicio al cliente al proporcionar educación sobre las particularidades de cada mercado. Además, este equipo puede tener la responsabilidad de difundir inteligencia de mercado tanto a nivel interno como hacia los clientes.

Las evaluaciones que la función de Gestión de Red de Subcustodios supervisará incluirán:

- Estructura de gobernanza
- Disposiciones de continuidad del negocio
- Participantes clave y cómo se traducen en el perfil de riesgo
- Capital
- Inversiones
- Disposiciones de recuperación y resolución
- Calidad de los servicios, como impuestos y eventos sobre activos
- Requisitos técnicos y de mensajería / compatibilidad
- Modelo de finalidad de liquidación
- Modelo de gestión de riesgos
- Modelo de gestión del cambio
- Cumplimiento normativo (por ejemplo, CSDR en Europa)
- Precios
- Cumplimiento de los términos y condiciones

8.4 Supervisión de terceros

Un proveedor de Servicios de Valores debe establecer un marco claro para gestionar las actividades de los proveedores externos, lo que puede requerir la creación de unidades especializadas para supervisar estas relaciones. Un aspecto clave para el proveedor de Servicios de Valores es encontrar el equilibrio entre colaborar estrechamente con el proveedor externo para garantizar procesos y eficiencia óptimos, y conservar la capacidad institucional de cambiar a otro proveedor externo si fuera necesario.

Cuando una actividad ha sido externalizada, una consideración fundamental —influenciada por factores contractuales, regulatorios y el apetito de riesgo— es en qué medida puede recuperarse dicha actividad y durante cuánto tiempo puede mantenerse esa recuperación. Además, el creciente enfoque de la industria en la resiliencia operativa ha incrementado el escrutinio regulatorio sobre estas relaciones. Los proveedores de Servicios de Valores deben ser especialmente cuidadosos al comprender sus obligaciones regulatorias al evaluar estas relaciones.

8.5 Amenazas de riesgo de proveedores externos

Los riesgos operativos, comerciales y reputacionales son los principales elementos que deben considerar los proveedores de Servicios de Valores al contratar y utilizar los servicios de un proveedor externo. A continuación, se presenta una tabla que resume las principales amenazas de riesgo y algunas posibles medidas de mitigación.

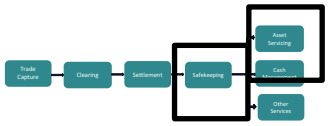
Ilustración 8.5 – Tabla de riesgos de proveedores externos

Descripción del riesgo	Mitigación del riesgo
Idoneidad del proveedor externo no evaluada ni calificada por el proveedor de Servicios de Valores	Establecer y aplicar una estrategia para proveedores externos Crear un equipo de profesionales cualificados en el proveedor de Servicios de Valores que sea capaz de evaluar la idoneidad y conveniencia de un proveedor externo potencial Evaluar y supervisar de forma continua los servicios y el desempeño de un proveedor externo, incluyendo: ▪ Validar la elegibilidad mediante la verificación de la calificación crediticia, solidez financiera/recursos en relación con la actividad, seguro de responsabilidad civil, buena reputación, autorizaciones regulatorias (cuando corresponda), planes de continuidad del negocio (BCP), gestión de terceros, criterios y riesgos ESG, asegurando la conformidad con la identidad corporativa ▪ Gestionar el riesgo de concentración para evitar que un proveedor externo asuma demasiado volumen de negocio con el proveedor de Servicios de Valores, lo que podría comprometer la calidad del servicio ▪ Asegurar que el proveedor externo preste los servicios contratados con los niveles de calidad acordados, dentro de los plazos de procesamiento establecidos y a los precios acordado Establecer un proceso de alertas de noticias para identificar posibles problemas con un proveedor externo
Aprobaciones regulatorias / del cliente no gestionadas adecuadamente antes de utilizar al proveedor externo	Implementar un proceso interno en el proveedor de Servicios de Valores para evaluar si se requieren aprobaciones regulatorias para contratar con un proveedor externo, y cuáles Completar todas las aprobaciones regulatorias antes de formalizar un contrato con un proveedor externo Establecer un proceso para revisar todos los contratos con clientes a fin de identificar requisitos de aprobación previa o notificación
Fallo del proveedor externo que provoca la interrupción de la prestación del servicio	Establecer una política en el proveedor de Servicios de Valores para garantizar que se haya identificado una solución alternativa que esté disponible en caso de fallo del proveedor externo. Esto puede incluir la aprobación de un proveedor externo alternativo o la internalización del servicio
Proveedor alternativo no designado de manera oportuna	Crear un marco de contingencia detallado en el proveedor de Servicios de Valores, incluyendo procedimientos escritos y un cronograma, que cubra el proceso necesario para trasladar un servicio de un proveedor externo a una solución alternativa en caso de que se produzca un evento desencadenante
Proceso adecuado de gestión de incidentes no implementado y/o no seguido	Implementar un acuerdo contractual entre el proveedor de Servicios de Valores y el proveedor externo que defina las responsabilidades de este último en cuanto a la gestión de incidentes Asignar responsabilidades internas en el proveedor de Servicios de Valores para la política, gestión y función de supervisión de proveedores externos, incluyendo la gestión de incidentes

Descripción del riesgo	Mitigación del riesgo
Fallo del proveedor externo al no seguir el proceso de gestión de incidentes esperado	Incluir, en el acuerdo contractual entre el proveedor de Servicios de Valores y el proveedor externo, cláusulas que cubran las implicaciones y responsabilidades en caso de incumplimiento de los procesos de gestión de incidentes
Fallo del subcustodio debido a la incapacidad de prestar el servicio o a problemas en el mercado local	Implementar un proceso de monitoreo continuo del subcustodio por parte del proveedor de Servicios de Valores Completar la selección y designación contractual de un subcustodio alternativo, con cuentas de contingencia activas abiertas para ser utilizadas en caso de un evento desencadenante Acordar un enfoque para la toma de decisiones, en caso de que ocurra un evento desencadenante, que permita desviar el negocio nuevo o existente al proveedor de contingencia

9. Riesgo de protección de activos

9.1 Introducción



Existen varias formas en las que los activos de un cliente pueden estar en riesgo de pérdida o no disponibilidad a lo largo de la cadena de valor de los Servicios de Valores. Estos riesgos incluyen fraude o apropiación indebida de activos, controles inadecuados, errores en el manejo de eventos o insolvencia de uno o más proveedores de Servicios de Valores.

La crisis financiera de 2008, y específicamente el colapso de Lehman Brothers, puso en evidencia los riesgos para los proveedores de Servicios de Valores y dio lugar a un mayor enfoque regulatorio en la seguridad de los activos y la protección del inversor en toda la cadena de valor. En tiempos más recientes, tanto el colapso de ciertas plataformas de criptomonedas —que también actuaban como custodios de dichos criptoactivos— como la aplicación de sanciones y contramedidas, han resaltado la importancia crítica y los beneficios para los clientes de contar con normas sólidas de protección de activos.

Este capítulo explora los principios clave de la protección de activos, así como los diferentes riesgos y las oportunidades de mitigación. Cabe señalar que el enfoque de este capítulo está en los activos financieros (valores), que pueden mantenerse fuera del balance de un proveedor de Servicios de Valores. En la mayoría de los casos, el dinero es fungible y está en balance con los bancos, y está sujeto a regulaciones prudenciales que garantizan el cumplimiento de requisitos adecuados de solidez y seguridad.

9.2 Definición

La protección de activos implica las medidas adoptadas por los proveedores de Servicios de Valores para garantizar la seguridad de los activos de los clientes y mitigar el riesgo de pérdida o no disponibilidad, ocultación, uso o transferencia fraudulenta de activos, impactos derivados de insolvencia dentro de la cadena de valor de Servicios de Valores y el incumplimiento de requisitos legales o normativos, de acuerdo con las leyes nacionales, regionales o internacionales de protección de activos.

9.3 Principios clave de la protección de activos

Muchos de los requisitos clave en materia de protección de activos dependen de la naturaleza y la(s) jurisdicción(es) de los activos en custodia, así como de los participantes y clientes involucrados en los Servicios de Valores. Por tanto, el riesgo de protección de activos debe evaluarse y mitigarse en la etapa de incorporación del cliente, así como cuando un proveedor de Servicios de Valores se extienda a nuevas jurisdicciones o tipos de activos.

Los riesgos relacionados con la protección de activos están presentes a lo largo de todo el ciclo de vida de los Servicios de Valores. Las medidas para detectar incumplimientos o irregularidades se aplican a lo largo del ciclo, con énfasis particular en las etapas de liquidación, custodia, informes y servicios sobre activos. Por lo tanto, los proveedores de Servicios de Valores deben garantizar:

- Registro oportuno y preciso de los activos y su propiedad
- Conciliación periódica entre sus propios registros y los de otros proveedores de Servicios de Valores en la cadena (anteriores o posteriores)
- Reporte oportuno y completo a sus clientes

Considerando el entorno regulatorio en constante evolución, los proveedores de Servicios de Valores también deben mantenerse actualizados con respecto a la agenda regulatoria y garantizar la implementación oportuna de cualquier cambio necesario para cumplir con la normativa (por ejemplo, en sistemas, aspectos legales, marcos de riesgo, sanciones).

El informe de la Organización Internacional de Comisiones de Valores (IOSCO) de 2014 proporciona recomendaciones sobre la protección de activos y establece una serie de principios clave sobre este tema: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD401.pdf

A continuación, se resumen estos principios:

- Los activos propios del proveedor de Servicios de Valores deben estar física y legalmente separados de los activos de los clientes. En caso de insolvencia del proveedor, un administrador debe poder identificar los activos pertenecientes al cliente, y que el subcustodio actúa meramente como custodio en nombre del cliente. La importancia de las convenciones de denominación de cuentas es crítica.
- El proveedor debe ser capaz de identificar en todo momento, y sin demora, la cantidad, ubicación, titularidad y el estado legal de los activos del cliente. Deben existir procesos de conciliación para confirmar esto. Además, se debe contar con el consentimiento previo del cliente para cualquier uso de sus activos.
- El proveedor debe emitir periódicamente (y cuando sea solicitado) un estado de cuenta a sus clientes.
- El proveedor debe comprender las implicaciones de mantener activos en regímenes jurídicos extranjeros y garantizar claridad y transparencia al divulgar los marcos normativos aplicables a la protección de activos de clientes.

ESTUDIO DE CASO: FTX Trading

El 11 y el 14 de noviembre de 2022, FTX Trading Ltd (una firma de intercambio de criptomonedas) y sus filiales presentaron una solicitud de protección bajo el Capítulo 11 del Código de Quiebras de EE. UU. Las investigaciones, basadas en el análisis de los deudores, consideran que las plataformas de FTX debían a sus clientes aproximadamente 8.700 millones de USD. El informe de los deudores destacó la mezcla y el uso indebido de los depósitos de los clientes y señaló lo siguiente:

“El Grupo FTX promovía un compromiso con la protección de los depósitos de los clientes contra usos indebidos o asignaciones erróneas, y defendía públicamente los esfuerzos legislativos y regulatorios para proteger a los clientes de la industria cripto. A través de su sitio web, redes sociales, y en declaraciones y presentaciones ante el Congreso, reguladores y otras terceras partes, el Grupo FTX afirmaba mantener una estricta separación entre los fondos de los clientes y los corporativos, incluyendo el mantenimiento de los fondos de clientes en cuentas bancarias ómnibus 'en beneficio de' (‘FBO’, por sus siglas en inglés) los clientes de la plataforma FTX. En todo momento, con la excepción de jurisdicciones aisladas, las afirmaciones del Grupo FTX a este respecto eran falsas.”

(Fuente: Tribunal de Quiebras de EE. UU., Delaware – caso 22-11068 – Segundo Informe Provisional, fechado el 26 de junio de 2023).

FTX mezcló activos de clientes con activos propios. Si hubiera seguido los principios clave de regulación para la segregación de activos de clientes, esta situación podría haberse evitado. Al momento de escribir este informe, los reguladores están en etapas avanzadas de finalizar normativas que aclaren y garanticen marcos apropiados; por ejemplo, el Reglamento sobre Mercados de Criptoactivos (MiCA) de la ESMA.

9.4 Amenazas al riesgo de protección de activos

Las siguientes tablas describen las amenazas de riesgo más frecuentes que pueden comprometer la protección de activos. Estas amenazas incluyen:

- Riesgo político / país
- Riesgo derivado de un marco regulatorio en evolución
- Riesgo relacionado con la estructura de cuentas y el registro
- Riesgo de insolvencia / incumplimiento
- Riesgo de fraude y negligencia

No obstante, es importante destacar que, incluso tras aplicar prácticas estrictas de mitigación de riesgos, no es posible eliminar completamente el riesgo de protección de activos. La ausencia de marcos legales establecidos y probados, eventos de riesgo país (como congelación de activos) y la insolvencia de participantes están entre los factores de riesgo clave que deben considerarse en las decisiones de inversión de un cliente y en la evaluación del apetito de riesgo, tanto del proveedor de Servicios de Valores como del propio cliente.

9.4.1 Riesgo político / país

El riesgo político o país puede surgir cuando existe inestabilidad o incertidumbre en la gobernanza o en el régimen político de un país. La agitación política o económica puede derivar en cambios en las leyes, regulaciones o políticas que impacten la protección de activos.

Las implicaciones para los proveedores de Servicios de Valores y sus clientes, en caso de que se produzca esta situación, pueden ser graves, incluyendo la posibilidad de que los activos sean bloqueados, congelados o incluso perdidos. Los proveedores de Servicios de Valores y los clientes deben realizar un análisis de cada mercado para comprender el entorno político y económico y monitorear continuamente la situación con el fin de poder reaccionar en caso de que se produzcan cambios.

Ilustración 9.4.1 – Tabla de Riesgo Político / País

Descripción del riesgo	Mitigación del riesgo
Colapsos del mercado	Asegurar que existan equipos internos dedicados al monitoreo de las distintas jurisdicciones donde los clientes mantienen activos a través del proveedor de servicios de valores Establecer acuerdos de contingencia y diversificación con una gestión proactiva del inventario para mantener activos transferibles en una ubicación transfronteriza
Inestabilidad política, guerras o actos de terrorismo que afectan la liquidez, los sistemas, las bolsas de valores o los bancos centrales	Asegurar que existan equipos internos enfocados en monitorear el entorno político dentro del proveedor de servicios de valores Contar con planes de contingencia con gestión proactiva del inventario para mantener activos transferibles en una ubicación transfronteriza Asegurar una gestión activa de la liquidez en dinero

Descripción del riesgo	Mitigación del riesgo
Imposición de embargos o sanciones que limitan el movimiento o acceso a los activos	Contar con herramientas sólidas de detección de embargos / sanciones y procedimientos de escalamiento bien definidos Garantizar que los documentos legales cubran las responsabilidades y la posible responsabilidad del proveedor de servicios de valores / cliente en caso de la imposición de un embargo o sanción
Expectativas regulatorias poco claras o que carecen de transparencia	Asegurar un análisis sólido del riesgo país y mantener vínculos con reguladores locales y expertos legales en la jurisdicción correspondiente
El proveedor de servicios de valores carece de transparencia sobre los inversores, lo que dificulta la detección de inversores / activos sancionados	Implementar requisitos reforzados de idoneidad para cuentas ómnibus en jurisdicciones o negocios con riesgo Establecer procesos de KYC mejorados, incluyendo la identificación del Beneficiario Final (UBO) Asegurar el monitoreo continuo del desempeño y las transacciones de los inversores y los activos

9.4.2 Riesgo de evolución del marco regulatorio

Las regulaciones cambian constantemente, y los reguladores crean e implementan regulaciones nuevas y actualizadas a medida que los mercados evolucionan y crecen. Cualquier cambio en un marco regulatorio puede requerir la intervención de un proveedor de servicios de valores o de un cliente, ya que un incumplimiento regulatorio podría tener implicaciones potenciales para la seguridad de los activos. Por lo tanto, la supervisión continua de los diferentes marcos regulatorios es fundamental para garantizar su cumplimiento.

Ilustración 9.4.2 Tabla de Riesgo de evolución de marco regulatorio

Descripción del riesgo	Mitigación del riesgo
Alta frecuencia y complejidad de los cambios regulatorios	Garantizar una participación activa para mantenerse al tanto de la agenda regulatoria
Impacto en la reputación y el negocio debido al incumplimiento de las regulaciones	Realizar evaluaciones de impacto internas para garantizar la implementación oportuna de cualquier cambio para lograr el cumplimiento (por ejemplo, sistema, legal, marco de riesgo)
Los cambios regulatorios carecen de transparencia o no son claros	Garantizar un sólido análisis de riesgo país y conexiones con reguladores locales y expertos legales jurisdiccionales.

9.4.3 Riesgo relacionado con la estructura de cuentas y el registro

La elección de la estructura de cuenta puede influir en el nivel de protección de los activos, es decir, en la garantía de que el cliente retiene, en última instancia, la titularidad (legal) con todos los derechos asociados (ingresos, eventos corporativos, voto por poder, etc.) y el acceso a los activos de conformidad con las regulaciones aplicables en las distintas jurisdicciones involucradas.

Como se describe en el capítulo sobre estructuras de cuentas, las opciones más comunes son:

- Cuenta ómnibus (donde los activos de múltiples inversores se mantienen juntos)
- Cuenta segregada (donde los activos están separados, ya sea a nivel del subcustodio o del CSD)
- Cuenta a nombre de un nominado (donde los activos pueden estar en una cuenta ómnibus o segregada, pero están registrados a nombre de un nominado)

Estas estructuras de cuenta pueden aplicarse en diferentes niveles de la cadena de servicios de valores, aunque no siempre están permitidas o son aconsejables según las normativas aplicables. Si bien existen diversas estructuras, siempre que se sigan buenas prácticas (como convenciones de nomenclatura, acuerdos contractuales sólidos, registros precisos y oportunos a nivel del titular del activo, conciliaciones y cumplimiento de regulaciones locales), las estructuras mencionadas deberían ofrecer una protección adecuada de los activos. Sin embargo, hay ventajas e inconvenientes —especialmente en términos de costos y eficiencia— que influyen en la decisión sobre qué enfoque adoptar.

Ilustración 9.4.3 – Riesgo relacionado con la estructura de cuentas y el registro

Descripción del riesgo	Mitigación del riesgo
Uso inapropiado del concepto de nominado	Utilizar la estructura de cuenta a nombre de un nominado solo en mercados donde el concepto esté reconocido Cuando el concepto de nominado esté reconocido en una jurisdicción, la cuenta debe estar registrada a nombre del nominado y no del proveedor de servicios de valores Evaluar los activos mantenidos a nombre del nominado para asegurar que no exista responsabilidad sobre el nominado (por ejemplo, activos parcialmente desembolsados con obligaciones o llamadas pueden no ser apropiados)
Falta de reconocimiento del concepto de nominado en una jurisdicción	Establecer una cuenta en el subcustodio o CSD a nombre del Cliente o del Beneficiario Final (UBO)
Incumplimiento o insolvencia del subcustodio	Asegurar que los activos del Proveedor de Servicios de Valores estén separados y sean distinguibles a nivel de subcustodio Asegurar que los activos del Cliente estén completamente segregados de los activos propios y de todos los demás activos Mantener la cuenta del subcustodio a nombre del nominado del Proveedor de Servicios de Valores, del Cliente o del UBO, y que sea visible para los acreedores

Descripción del riesgo	Mitigación del riesgo
Incumplimiento o insolvencia del depositario central de valores (CSD)	Asegurar que los activos del Proveedor de Servicios de Valores estén separados y sean distinguibles a nivel del CSD Asegurar que los activos del Cliente estén completamente segregados de los activos propios y de todos los demás activos Mantener la cuenta en el CSD a nombre del nominado del Proveedor de Servicios de Valores, del Cliente o del UBO, y que sea visible para los acreedores Entender el proceso del CSD para transferir activos a otro CSD en caso de liquidación (por razones de incumplimiento, insolvencia o retiro de la licencia del CSD)

9.4.4 Riesgo de insolvencia / incumplimiento

El impacto de la insolvencia o el incumplimiento de un Proveedor de Servicios de Valores o de un Cliente tendrá un efecto significativo tanto en la parte insolvente / en incumplimiento como en las demás partes que hagan negocios con ella. Sin embargo, la insolvencia —en particular— también puede tener implicaciones más amplias para toda la industria. Por ello, es fundamental que se implementen medidas sólidas de protección de activos para garantizar que los activos del Proveedor de Servicios de Valores y del Cliente estén separados y protegidos ("ring-fenced").

Asimismo, deben establecerse procesos sólidos de conciliación y reporte, junto con revisiones continuas de solvencia crediticia realizadas por ambas partes. En las jurisdicciones donde existan regímenes de protección de activos, los acuerdos contractuales deben reflejar estos requisitos regulatorios.

Ilustración 9.4.4 – Tabla de Riesgo de Insolvencia / Incumplimiento

Descripción del riesgo	Mitigación del riesgo
Insolvencia o incumplimiento del Proveedor de Servicios de Valores	Implementar criterios sólidos de selección de Proveedores de Servicios de Valores y un proceso de aceptación comercial por parte del Cliente Asegurar que los activos del Cliente estén completamente segregados de los activos del Proveedor de Servicios de Valores Verificar continuamente la calificación crediticia, los límites de crédito, el control y monitoreo del crédito junto con mitigantes contractuales (derecho de retención y derecho de venta)
Insolvencia o incumplimiento del Cliente	Implementar criterios sólidos de selección de Clientes y un proceso de aceptación comercial por parte del Proveedor de Servicios de Valores Contar con la capacidad de segregar los activos del Cliente en caso de insolvencia del Cliente, para que el Proveedor de Servicios de Valores pueda continuar con su actividad normal Verificar continuamente la calificación crediticia, los límites de crédito, el control y monitoreo del crédito junto con mitigantes contractuales (derecho de retención y derecho de venta)

Descripción del riesgo	Mitigación del riesgo
Insolvencia o incumplimiento del subcustodio o del CSD	Establecer criterios sólidos de selección de subcustodios / CSD por parte del Proveedor de Servicios de Valores Asegurar que los activos del Proveedor de Servicios de Valores y/o del Cliente estén protegidos y sean distinguibles a nivel del mercado local, y realizar un monitoreo continuo Comprender las garantías gubernamentales u otros mecanismos de respaldo disponibles para evitar la interrupción de las funciones del CSD
Contagio por parte de un Proveedor de Servicios de Valores de importancia sistémica global	Aplicar las disposiciones de recuperación y resolución bancaria Comprender las implicaciones financieras del contagio por parte de un Proveedor de Servicios de Valores de importancia sistémica global, incluyendo exposiciones crediticias por operaciones no liquidadas, préstamos y tomas de valores, etc.
El marco legal, en el que se mantienen los activos, puede no haber establecido estructuras claras y comprobadas de seguridad de activos o protección ante insolvencias	Contar con un proceso claro de revisión y aceptación de los requisitos regulatorios y legales jurisdiccionales en materia de protección de activos Incluir en los acuerdos contractuales del Proveedor de Servicios de Valores un lenguaje apropiado que explique las limitaciones de los regímenes de protección de activos
El lenguaje legal del acuerdo contractual difiere del marco regulatorio / legal del país	Contar con un proceso claro de revisión y aceptación de los requisitos regulatorios y legales jurisdiccionales en materia de protección de activos Monitorear el régimen regulatorio y legal en cada jurisdicción para garantizar que los cambios sean identificados y se incorporen las modificaciones contractuales necesarias a los acuerdos

9.4.5 Riesgo de Fraude y Negligencia

El fraude y la negligencia son dos amenazas adicionales para la protección de los activos. Mientras que la negligencia implica cometer un error por descuido, el fraude es un acto intencional diseñado para engañar.

El fraude es cometido por delincuentes que continuamente desarrollan métodos nuevos y cada vez más sofisticados para engañar. En el ámbito de los Servicios de Valores, el fraude puede ocurrir a través de diversos medios, como el acceso no autorizado a la información del Cliente, transacciones fraudulentas o delitos cibernéticos.

La negligencia, por parte de un Proveedor de Servicios de Valores o un Cliente, se refiere a errores como ingresar incorrectamente una transacción, enviar una operación fuera de plazo, proporcionar información incorrecta o la omisión de transacciones/información. Aunque las acciones negligentes no son intencionales, sus consecuencias pueden ser graves. Por lo tanto, es igualmente importante tomar medidas para minimizar este tipo de riesgos.

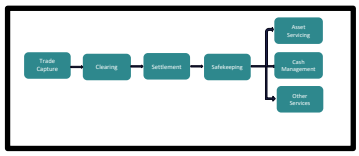
Tanto la negligencia como el fraude pueden ocurrir en diversos puntos de la cadena de valor de los Servicios de Valores. Por ello, es responsabilidad tanto de los Proveedores de Servicios de Valores como de los Clientes tomar medidas activas para identificar dónde pueden presentarse estos riesgos y contar con medidas de mitigación para prevenirlos.

Ilustración 9.4.5 Tabla de Riesgos de Fraude y Negligencia

Descripción del riesgo	Mitigación del riesgo
Operaciones ficticias o transacciones fraudulentas enviadas al Proveedor de Servicios de Valores	Implementar criterios sólidos de selección y un proceso de aceptación de negocio tanto para el Proveedor de Servicios de Valores como para el Cliente Asegurar un marco de riesgos, políticas y procedimientos sólidos, incluyendo el establecimiento de estándares éticos esperados / código de conducta para definir el comportamiento ante el riesgo Implementar métodos automatizados en el Cliente que cubran: ○ la transmisión de transacciones ○ procesos rigurosos de autenticación / validación ○ procesos de asignación / confirmación y verificación (donde estén soportados por la jurisdicción) ○ conciliaciones periódicas de libros y registros
Transacciones no procesadas de manera precisa, completa y oportuna	Implementar controles integrales de verificación de transacciones y conciliaciones de extremo a extremo tanto en el Proveedor de Servicios de Valores como en el Cliente Asegurar la existencia de políticas y procedimientos sólidos, formación del personal y una cultura de gestión de riesgos Fomentar métodos automatizados para la transmisión de transacciones, junto con procesos rigurosos de autenticación / validación del Cliente
Procesos manuales / sin procesamiento directo (STP) / datos estáticos incorrectos	Implementar métodos automatizados para la transmisión de transacciones, junto con procesos de autenticación / validación estrictos tanto en el Proveedor de Servicios de Valores como en el Cliente Proporcionar incentivos a los Clientes para evitar instrucciones manuales, tardías e inexactas Asegurar controles jerárquicos de entrada, aprobación y liberación de transacciones

10. Ejecución, Entrega y Riesgo de Gestión de Procesos

10.1 Introducción



Todas las partes involucradas en la cadena de Servicios de Valores están expuestas al riesgo de pérdida o retraso derivado de errores operativos, ya sea por procesos internos inadecuados, errores humanos o fallos de sistemas. Estos riesgos se conocen comúnmente como riesgos de ejecución, entrega y gestión de procesos.

Este capítulo analiza cómo un error de esta naturaleza puede dejar tanto al Cliente como al Proveedor de Servicios de Valores expuestos a la pérdida parcial o total del valor de una inversión, derecho u oportunidad, lo que podría dar lugar a reclamos entre las partes. Por ello, las disposiciones contractuales entre el Cliente y su Proveedor de Servicios de Valores relacionadas con el incumplimiento contractual y la negligencia son esenciales para mitigar el riesgo y facilitar la recuperación de pérdidas.

Es importante señalar que estos riesgos no son exclusivos de la relación entre el Cliente y el Proveedor de Servicios de Valores. Son riesgos inherentes a cualquier proveedor de servicios que custodie activos y gestione transacciones.

10.2 Definición

El riesgo de ejecución, entrega y gestión de procesos se define como el riesgo de pérdida resultante de procesos internos inadecuados o fallidos, errores humanos, fallos de sistemas o eventos externos. Este riesgo puede afectar tanto a Proveedores de Servicios de Valores como a Clientes al utilizar funciones de Servicios de Valores, y representa el riesgo asumido por el Proveedor de Servicios de Valores al realizar servicios en nombre del Cliente y viceversa.

10.3 Riesgos de Captura de Operaciones, Compensación y Liquidación

Este aspecto del servicio se refiere a la captura de los detalles de la operación por parte del Cliente, seguido por la creación de una transacción de entrega o recepción de valores, junto con los procesos de conciliación, compensación y liquidación como etapas principales que concluyen la transferencia/intercambio de activos tras la ejecución de la operación entre dos contrapartes comerciales.

10.3.1 Riesgo en la Captura de Operaciones

El proceso de captura de operaciones está expuesto a varios riesgos operativos que pueden llevar a fallos en la liquidación. Por tanto, es clave que dicho proceso esté lo más automatizado posible y que se implementen controles para verificar y validar la integridad y exactitud de la captura de la operación

Ilustración 10.3.1 Tabla de Riesgos en la Captura de Operaciones

Descripción del riesgo	Mitigación del riesgo
Instrucciones del cliente no capturadas	Uso de formatos de mensajería estructurados para aumentar el procesamiento directo (STP) Establecer conciliación de control de mensajes Establecer controles y alertas para instrucciones corregidas/rechazadas Supervisar las operaciones alegadas
Detalles de la operación no capturados / autenticados con precisión	Aceptar instrucciones a través de procesamiento directo automatizado (STP), sujeto a: ○ Controles de sistema establecidos que puedan identificar de manera única que la instrucción se originó del Cliente o de un intermediario que actúe en su nombre ○ Controles de sistema establecidos para validar de forma única la cuenta correcta del Cliente y las instrucciones estándar de liquidación (SSIs) Aceptar instrucciones manuales solo de manera excepcional (por ejemplo, en una situación de contingencia o para operaciones no estándar), sujeto a: ○ Controles establecidos para la captura precisa de instrucciones manuales (por ejemplo, medios de alto riesgo como fax o correo electrónico) ○ Controles para garantizar la verificación de la instrucción manual con el fin de validar la autenticidad del cliente mediante verificación de firma / llamada de confirmación / verificación del remitente del correo electrónico. (Estos tipos de medios representan un alto riesgo para el cliente y deben evitarse tanto como sea posible)

10.3.2 Riesgo de Compensación

Los Proveedores de Servicios de Valores que utilizan Contrapartes Centrales (CCPs) para compensar operaciones actúan como contraparte de la operación en nombre de un Cliente. Como resultado de este proceso, los Proveedores de Servicios de Valores están expuestos a múltiples riesgos asociados con la compensación, incluidos los riesgos de crédito, de mercado y operacionales.

Ilustración 10.3.2 Tabla de Riesgos de Compensación

Descripción del riesgo	Mitigación del riesgo
Las instrucciones de operación del Cliente no son capturadas por la CCP	Utilizar formatos de mensajería estructurados para aumentar el procesamiento directo (STP) Establecer controles de conciliación de transacciones entre el archivo de operaciones (es decir, el lugar donde se ejecutan las operaciones) y el archivo de la CCP (es decir, las operaciones neteadas procesadas por la CCP) Establecer controles para instrucciones reparadas / rechazadas

Descripción del riesgo	Mitigación del riesgo
Las instrucciones recibidas no coinciden con las de la contraparte	Establecer controles para el manejo de instrucciones no coincidentes Implementar controles para monitorear y recuperar notificaciones de la CCP que puedan identificar discrepancias Establecer comunicación y revisiones del servicio para plantear cualquier problema recurrente con las instrucciones del Cliente
El Proveedor de Servicios de Valores no monitorea debidamente el riesgo de crédito y la exposición frente a la CCP	Asegurarse de que la CCP tenga criterios de entrada y un protocolo de incorporación integral, y que realice una debida diligencia completa sobre cada uno de sus miembros tanto antes de su incorporación como de forma continua Establecer controles en el Proveedor de Servicios de Valores para monitorear el mercado y las posiciones del Cliente Asegurarse de que el Cliente proporcione los niveles apropiados de garantía, ya sea en dinero o valores, como respaldo frente a posibles pérdidas
El Proveedor de Servicios de Valores no detecta una notificación de *buy-in (recompra forzada)*	Establecer un proceso operativo en el Proveedor de Servicios de Valores para asegurar que las notificaciones de buy-in sean recuperadas automáticamente desde la CCP Crear un flujo de trabajo en caso de que no se admita STP, para monitorear el sitio web o portal de mensajería de la CCP en busca de notificaciones relevantes Establecer un proceso de notificación sensible al tiempo y un SLA para informar a los Clientes sobre un evento de buy-in Asegurarse de que el Cliente haya depositado suficiente garantía para proteger al Proveedor de Servicios de Valores en caso de que ocurran buy-ins En caso de que se ejecute un buy-in contra una operación del Cliente, cubrir inmediatamente la pérdida utilizando la garantía proporcionada por el Cliente
Incumplimiento de un miembro compensador en la CCP	Asegurarse de que el Proveedor de Servicios de Valores cuente con procesos rigurosos de gestión de riesgos frente a CCP para identificar posibles problemas de riesgo de contraparte antes de que ocurran Asegurarse de que la CCP tenga protocolos de comunicación establecidos para notificar a otros miembros de compensación sobre el incumplimiento de un miembro, de acuerdo con su reglamento y la normativa correspondiente Asegurarse de que tanto la CCP como el Proveedor de Servicios de Valores mantengan niveles adecuados de garantía (ya sea en dinero o en valores) Asegurarse de que las llamadas de margen se realicen de forma oportuna por parte del Proveedor de Servicios de Valores Asegurarse de que el Proveedor de Servicios de Valores pague el margen adicional de forma puntual, conforme al reglamento de la CCP, y que los requisitos internos de capital y liquidez cubran adecuadamente los riesgos crediticios asociados a la exposición frente a la CCP Tener políticas de insolvencia e incumplimiento divulgadas públicamente en el sitio web del Proveedor de Servicios de Valores Asegurarse de que el Cliente haya nominado un GCM (General Clearing Member) de respaldo en caso de que su GCM del Proveedor de Servicios de Valores incurra en incumplimiento, y que existan protocolos operativos para transferir (port) sus posiciones al GCM sustituto

Descripción del riesgo	Mitigación del riesgo
Incumplimiento del cliente	Asegurar que el proveedor de servicios de valores implemente un proceso mediante el cual el cliente proporcione suficiente garantía (colateral) para mitigar el riesgo del proveedor de servicios de valores, y que se soliciten niveles adecuados de margen al cliente conforme a los cambios diarios del valor de mercado (mark-to-market) Asegurar que el proveedor de servicios de valores supervise que exista un derecho de prenda / derecho de venta o compensación para ofrecer cobertura adicional frente a la exposición al cliente Contar con políticas de insolvencia e incumplimiento públicamente divulgadas en el sitio web del proveedor de servicios de valores
Incumplimiento de la cámara de compensación (CCP)	Implementar un marco documentado de monitoreo de riesgos y responsabilidades, así como un proceso de escalamiento y comunicación en el proveedor de servicios de valores para supervisar el desempeño y la solvencia de las cámaras de compensación (CCPs) Asegurar que los requisitos de capital y liquidez del proveedor de servicios de valores cubran adecuadamente los riesgos de crédito asociados a la exposición a la cámara de compensación (CCP) Asegurar que el proveedor de servicios de valores haya identificado una CCP de respaldo para transferir (“port”) posiciones, con el fin de limitar o evitar la degradación del servicio y perjuicio financiero al cliente Contar con políticas de insolvencia e incumplimiento públicamente divulgadas en el sitio web del proveedor de servicios de valores

10.3.3 Riesgo de Liquidación

Una transacción de valores puede no liquidarse por diversas razones, entre ellas – con mayor frecuencia – una instrucción tardía, una instrucción faltante, una instrucción incompleta o incorrecta, o por falta de dinero o valores. Sin embargo, existen otras causas menos comunes, como la insolvencia del cliente o de la contraparte, un código de valor suspendido debido a sanciones o un problema de conciliación. Cada una de estas situaciones puede generar riesgo de liquidación tanto para el proveedor de servicios de valores como para el cliente, por lo que la gestión y el monitoreo proactivo de las operaciones entrantes y las liquidaciones pendientes son requisitos clave para mitigar este riesgo.

ESTUDIO DE CASO: FTX Trading

El 11 y el 14 de noviembre de 2022, FTX Trading Ltd (una firma de intercambio de criptomonedas) y sus filiales presentaron una solicitud de protección bajo el Capítulo 11 del Código de Quiebras de EE. UU. Las investigaciones, basadas en el análisis de los deudores, consideran que las plataformas de FTX debían a sus clientes aproximadamente 8.700 millones de USD. El informe de los deudores destacó la mezcla y el uso indebido de los depósitos de los clientes y señaló lo siguiente:

"El Grupo FTX promovía un compromiso con la protección de los depósitos de los clientes contra usos indebidos o asignaciones erróneas, y defendía públicamente los esfuerzos legislativos y regulatorios para proteger a los clientes de la industria cripto. A través de su sitio web, redes sociales, y en declaraciones y presentaciones ante el Congreso, reguladores y otras terceras partes, el Grupo FTX afirmaba mantener una estricta separación entre los fondos de los clientes y los corporativos, incluyendo el mantenimiento de los fondos de clientes en cuentas bancarias ómnibus 'en beneficio de' ('FBO', por sus siglas en inglés) los clientes de la plataforma FTX. En todo momento, con la excepción de jurisdicciones aisladas, las afirmaciones del Grupo FTX a este respecto eran falsas."

(Fuente: Tribunal de Quiebras de EE. UU., Delaware – caso 22-11068 – Segundo Informe Provisional, fechado el 26 de junio de 2023).

FTX mezcló activos de clientes con activos propios. Si hubiera seguido los principios clave de regulación para la segregación de activos de clientes, esta situación podría haberse evitado. Al momento de escribir este informe, los reguladores están en etapas avanzadas de finalizar normativas que aclaren y garanticen marcos apropiados; por ejemplo, el Reglamento sobre Mercados de Criptoactivos (MiCA) de la ESMA.

Ilustración 10.3.3 Tabla de Riesgo de Liquidación

Descripción del riesgo	Mitigación del riesgo
Cliente / Proveedor de Servicios de Valores envía instrucciones de liquidación incorrectas	Establecer controles del sistema para validar el contenido y asegurar que la instrucción esté completa Establecer plantillas de instrucciones de liquidación permanentes (Standing Instructions, SIs) para asegurar que se envíen formatos de mensaje compatibles Utilizar plataformas del sector para garantizar que se utilicen las SIs correctas Usar instrucciones SWIFT y otras plataformas de comunicación estandarizadas que aseguren que los campos obligatorios estén completados para cada tipo de liquidación
Operación no verificada para disponibilidad de valores	Establecer controles del sistema para validar el contenido y asegurar que la instrucción esté completa Establecer plantillas de instrucciones de liquidación permanentes (Standing Instructions, SIs) para asegurar que se envíen formatos de mensaje compatibles Utilizar plataformas del sector para garantizar que se utilicen las SIs correctas Usar instrucciones SWIFT y otras plataformas de comunicación estandarizadas que aseguren que los campos obligatorios estén completados para cada tipo de liquidación

Descripción del riesgo	Mitigación del riesgo
La operación no verificada por disponibilidad de dinero.	Establecer controles para verificar la fuente de fondos (por ejemplo, dinero, límites de crédito, divisas, etc.) Asegurar que el dinero para la recepción de valores esté disponible en la cuenta y no aparezca como contractual a menos que exista un acuerdo de crédito según los requisitos del mercado y del Proveedor de Servicios de Valores Realizar conciliaciones automatizadas periódicas de las posiciones de dinero contra las cuentas de dinero del Subcustodio / CSD, conforme a las regulaciones locales y/o convenciones de mercado
Subcustodio / CSD no instruido.	Establecer controles robustos de revisión integral y conciliación de transacciones en el Proveedor de Servicios de Valores Implementar un proceso automatizado de extremo a extremo y STP desde el Cliente, pasando por la cadena de Subcustodios del Proveedor de Servicios de Valores, hasta el CSD
Estado de conciliación de la operación del cliente no supervisado y cliente no informado (cuando corresponda).	Establecer capacidad automatizada de conciliación de operaciones Contactar a las partes de negociación o liquidación para identificar razones de fallos en la preconciliación cuando las operaciones no coincidan Aceptar nuevas instrucciones del Cliente y enviarlas al Subcustodio / CSD según corresponda para lograr estado de conciliación Reportar el estado de conciliación al cliente final Establecer alertas frecuentes automatizadas de flujo de trabajo para asegurar una supervisión completa del estado de conciliación
Fallo en la liquidación de la operación no supervisado.	Establecer capacidad automatizada de monitoreo de operaciones Contactar a las partes de negociación o liquidación para identificar razones de fallos en la preconciliación cuando las operaciones no coincidan Aceptar nuevas instrucciones del Cliente y enviarlas al Subcustodio / CSD según corresponda para lograr estado de liquidación Reportar el estado de liquidación de operaciones al Cliente Acordar procesos / políticas para cancelar operaciones fallidas con antigüedad adecuada cuando corresponda, en conformidad con las guías regulatorias locales y/o convenciones del mercado

Descripción del riesgo	Mitigación del riesgo
Transacciones no liquidadas de manera oportuna, incluidas las transacciones transfronterizas.	Establecer capacidad automatizada de monitoreo de operaciones Establecer plantillas de Instrucciones de Liquidación Estándar (SSI) para asegurar que se envíen formatos de mensajes conformes con los estándares del mercado, por ejemplo, los estándares del Securities Market Practice Group (SMPG) https://www.smpg.info/ Utilizar instrucciones SWIFT u otras plataformas de comunicación estandarizadas que garanticen que los campos obligatorios estén completos para cada instrucción de liquidación Asegurar que dinero y valores estén disponibles para la liquidación oportuna antes de la fecha prevista Organizar un préstamo de valores ('borrow') para cubrir cualquier posición corta o utilizar facilidades de préstamo automático de Sub-custodio / CSD donde estén disponibles Optimizar el inventario ofreciendo o aceptando liquidación parcial o dividiendo entregas para los mismos valores nominales que las instrucciones de recepción Asegurar que se conozcan los plazos de mercado para instrucciones transfronterizas y que las instrucciones se envíen conforme a los horarios del mercado para evitar instrucciones tardías o demoras en la liquidación por desalineación de convenciones de mercado
Compra forzosa / venta forzosa no evitada.	Garantizar la liquidación oportuna de las transacciones Implementar reportes regulares sobre entregas cortas Asegurar comprensión robusta y comunicación sobre mercados de buy-in / sell-out, plazos y penalizaciones Implementar monitoreo y reporte dinero de operaciones en riesgo de buy-in con notificaciones oportunas de buy-in/sell-out
Multas / penalizaciones por incumplimiento de conciliación o liquidación no prevenidas.	Asegurar que las entregas estén cubiertas por saldos disponibles de valores antes de operar y/o implementar un libro de operaciones compensadas para garantizar que las entregas estén cubiertas por compras correspondientes para la misma fecha de liquidación prevista Garantizar liquidación oportuna de transacciones Proporcionar reportes regulares de entregas cortas para identificar posiciones cortas Organizar préstamos para posiciones cortas mediante acuerdos de préstamo de valores o utilizar facilidades de préstamo automático de Sub-custodio / CSD donde estén disponibles Maximizar el inventario retenido ofreciendo o aceptando liquidación parcial Asegurar un buen entendimiento del régimen de multas en cada mercado/tipo de valor según convenciones de mercado y regulaciones, incluidos los reglamentos de CCP / CSD Asegurar monitoreo y reporte dinero de límites potenciales o incumplidos

10.4 Riesgos de Custodia de Valores

Un riesgo clave dentro de la cadena de valor de los Servicios de Valores es la pérdida de activos mientras están en custodia. El Proveedor de Servicios de Valores debe garantizar que los activos de un Cliente (tanto desmaterializados como físicos) estén debidamente protegidos contra la insolvencia del Subcustodio y/o del Depósito Central de Valores (CSD), fraude, errores en el procesamiento, etc. Para más información, por favor revise el Capítulo 9: Protección de Activos.

Ilustración 10.4 Tabla de Riesgos de Custodia de Valores

Descripción del riesgo	Mitigación del riesgo
Los activos del Cliente no están protegidos contra la insolvencia del Subcustodio y del Depósito Central de Valores (CSD)	Implementar una selección y supervisión rigurosa, incluyendo la debida diligencia de los Subcustodios y el entendimiento de las estructuras de cuentas del CSD y las regulaciones locales de custodia Asegurar la monitorización diaria de noticias relacionadas con el Subcustodio y el CSD (por ejemplo, revisando calificaciones crediticias) Implementar un proceso robusto de gestión de incidentes y crisis Proveer revisiones y evaluaciones continuas de opiniones legales relacionadas con la protección contra insolvencias Asegurar el cumplimiento de todas las regulaciones relevantes de protección de activos Garantizar la titulación, denominación y registro adecuados de las cuentas Realizar conciliaciones frecuentes de los activos mantenidos en un Subcustodio / CSD versus los libros y registros propios del Proveedor de Servicios de Valores
Los activos del Cliente no están protegidos contra la apropiación fraudulenta	Establecer y mantener un control robusto de acceso a sistemas y físico (privilegios basados en roles, validación continua estricta) Asegurar conciliaciones frecuentes de activos mantenidos en un Subcustodio / CSD así como de los registros del registrador (para valores físicos) versus los libros y registros propios del Proveedor de Servicios de Valores Proveer generación frecuente de estados de cuenta para los Clientes

Descripción del riesgo	Mitigación del riesgo
Los activos del Cliente no están protegidos contra entregas erróneas	Establecer y mantener un control robusto de acceso a sistemas y físico (privilegios basados en roles, validación continua estricta) Establecer un modelo operativo automatizado que minimice las oportunidades de error humano Establecer controles dobles aplicados por sistemas y realizados por personal capacitado y competente Asegurar conciliaciones frecuentes de activos en un Subcustodio / CSD versus los libros y registros propios del Proveedor de Servicios de Valores Proveer generación frecuente de estados de cuenta para los Clientes Implementar controles robustos para verificar la disponibilidad de tenencias / posiciones en la cuenta del Cliente antes de enviar operaciones de entrega a un Subcustodio / CSD o liberar la instrucción de entrega para liquidación (especialmente donde existan cuentas ómnibus con estas partes)
Los activos del Cliente no están protegidos contra cambios en el mercado o eventos de fuerza mayor (por ejemplo, sanciones que restringen el acceso a activos en los mercados locales)	Asegurar la monitorización diaria de noticias de mercado, sanciones, etc., y la provisión de información a los Clientes Implementar una coordinación estrecha con los Subcustodios Asegurar el cumplimiento continuo de los regímenes regulatorios existentes y monitorear nuevos regímenes que requieran cumplimiento
Los activos físicos no están protegidos	Asegurar que los valores físicos estén registrados cuando sea posible Garantizar que la bóveda / sala segura sea apropiadamente segura, resistente al fuego / agua y asegurada por el valor / naturaleza de los activos custodiados Implementar un método seguro y con seguro para cubrir el traslado de valores físicos entre ubicaciones Asegurar conciliaciones regulares de valores físicos con los libros y registros del Proveedor de Servicios de Valores y del Registrador cuando exista Asegurar el cumplimiento continuo de los regímenes regulatorios existentes y monitorear nuevos regímenes que requieran cumplimiento

10.5 Amenazas de Riesgo en la Prestación de Servicios de Activos

La prestación de servicios de activos se refiere a las acciones realizadas para gestionar los activos una vez que están en custodia de un Proveedor de Servicios de Valores. Esto puede incluir el procesamiento de acciones corporativas, ingresos y asuntos fiscales. En un sentido más amplio, también abarca la gobernanza corporativa, como el voto por poder y las demandas colectivas.

10.5.1 Riesgo en el Procesamiento de Acciones Corporativas

Los riesgos clave asociados con el procesamiento de acciones corporativas son de naturaleza operativa, cuando una acción corporativa llega tarde, no se identifica, no se ejecuta o se realizan procesos incorrectos. Esto puede ocasionar fallos que podrían causar un riesgo reputacional tanto para el Proveedor de Servicios de Valores como para el Cliente.

ESTUDIO DE CASO: Mensajes No Estructurados en Acciones Corporativas

El uso de tipos de mensajes no estructurados para enviar instrucciones sobre eventos corporativos voluntarios puede resultar en errores en el procesamiento de dichas instrucciones. Aunque la pérdida potencial generalmente es la diferencia de precio entre el valor del título al participar en el evento y el precio actual de mercado, también existe el riesgo de pérdida por el valor total de los valores.

Por ejemplo, un Cliente envía un MT599 a su Proveedor de Servicios de Valores con múltiples instrucciones en el mensaje. Debido a las diferentes instrucciones, el equipo de operaciones omite una instrucción para participar en un canje opcional de bonos, lo que provoca que el Cliente no reciba la cantidad equivalente del nuevo bono. El Emisor incumple el bono antiguo.

Como resultado del error, el Proveedor de Servicios de Valores deberá comprar el nuevo bono o pagar al Cliente por el valor del nuevo bono sin posibilidad de recuperar el valor del bono antiguo**.**

Ilustración 10.5.1 Tabla de Riesgos en el Procesamiento de Acciones Corporativas

Descripción del riesgo	Mitigación del riesgo
La acción corporativa no es identificada de manera oportuna y/o precisa por el Proveedor de Servicios de Valores	Asegurar una fuente confiable y alimentación de información proveniente de fuentes independientes o proveedores de datos de acciones corporativas para permitir la comparación, conciliación y creación de una interpretación final del anuncio para su transmisión a los clientes El Proveedor de Servicios de Valores debe garantizar que exista un Acuerdo de Nivel de Servicio (SLA) con el Sub-custodio que establezca los requisitos y que los procesos se realicen conforme a los reglamentos de los libros de reglas del CSD y regulaciones del mercado local
El Cliente no es notificado por el Proveedor de Servicios de Valores sobre la acción corporativa original o cualquier cambio relacionado	Diseñar e implementar un modelo operativo que aproveche la tecnología para notificar automáticamente a los tenedores sobre un nuevo evento de acción corporativa o cualquier cambio en una acción corporativa publicada Elaborar un marco de riesgos con puntos de control para identificar fallos en la notificación Implementar un modelo de procesamiento automático (STP) para ayudar en notificaciones oportunas y precisas Fomentar que el Cliente implemente un modelo STP para el procesamiento de acciones corporativas Establecer controles dobles aplicados por el sistema, llevados a cabo por personal capacitado y competente, para revisar los detalles del evento Asegurar alertas y reportes de notificación por parte del Proveedor de Servicios de Valores que incluyan el estado, como confirmado/no confirmado y completo/incompleto

Descripción del riesgo	Mitigación del riesgo
Acción no tomada en evento voluntario	Implementar un modelo operativo para recibir las respuestas del Cliente mediante métodos automatizados y de procesamiento directo (STP), y establecer controles duales impuestos por el sistema, realizados por personal capacitado y competente, para ingresar y aprobar elecciones voluntarias Asegurar que se envíen mensajes de confirmación y notificaciones de excepciones o seguimientos al Cliente antes de las fechas límite del evento Garantizar que los Clientes sigan el modelo operativo y utilicen mensajería electrónica para apoyar el STP, además de revisar y responder a las confirmaciones o notificaciones cuando sea apropiado Realizar conciliaciones por parte del Proveedor de Servicios de Valores entre las instrucciones recibidas y las enviadas
Instrucciones del cliente enviadas incorrectamente al mercado	Establecer controles duales impuestos por el sistema, realizados por personal capacitado y competente, para ingresar y aprobar instrucciones manuales al Subcustodio o al CSD Asegurar la conciliación entre las instrucciones recibidas y las enviadas.
Derechos del Cliente no aplicados por el Subcustodio / CSD	Implementar un modelo operativo y tecnología diseñados para asegurar que las opciones de derechos de los clientes en eventos corporativos se calculen automáticamente, considerando la disponibilidad de la posición y garantizando su protección Asegurar la conciliación de la posición de valores o dinero recibida del Subcustodio / CSD con los libros y registros del Proveedor de Servicios de Valores
Instrucciones permanentes (SIs) para los derechos del Cliente no aplicadas	Garantizar un proceso robusto para almacenar y aplicar las Instrucciones Permanentes (SIs) del cliente para asegurar que los derechos se apliquen correctamente conforme a las preferencias del cliente Asegurar una comunicación oportuna a los clientes de acuerdo con las SIs del cliente para los derechos correspondientes
Instrucciones recibidas después del cierre de operaciones del Proveedor de Servicios de Valores pero antes del cierre del mercado no ejecutadas	Asegurar que el acuerdo contractual entre el Proveedor de Servicios de Valores y el cliente describa claramente el impacto de emitir instrucciones fuera de plazo Garantizar que existan acuerdos de nivel de servicio (SLAs) en el Proveedor de Servicios de Valores y un proceso, como un scorecard, para monitorear los tiempos de las instrucciones del cliente, así como considerar capacitaciones y seguimiento para evitar recurrencias

10.5.2 Riesgo de Voto por Poder

Los riesgos asociados con el voto por poder son principalmente riesgos operativos derivados de fallos para identificar, notificar o procesar con precisión un evento. Esto, una vez más, puede ocasionar riesgos reputacionales tanto para el Proveedor de Servicios de Valores como para el Cliente.

Ilustración Tabla de Riesgo de Voto por Poder

Descripción del riesgo	Mitigación del riesgo
Evento de voto por poder y detalles no identificados de manera oportuna y/o precisa por el Proveedor de Servicios de Valores	Asegurar una fuente confiable de información proveniente de fuentes independientes para permitir la comparación, conciliación y creación de la interpretación final del anuncio para su transmisión a los clientes El Proveedor de Servicios de Valores debe asegurar un acuerdo de nivel de servicio (SLA) con el Subcustodio que establezca los requisitos y que los procesos se lleven a cabo conforme a los reglamentos del libro de normas del CSD y regulaciones del mercado local
Cliente no informado sobre el requisito de voto por poder	Diseñar un modelo operativo, apoyado por tecnología, para garantizar que los derechos de voto por poder se calculen automáticamente, considerando la disponibilidad de la posición y asegurando su protección Asegurar que el modelo operativo proporcione la capacidad de notificar automáticamente a los clientes que poseen posiciones sobre los requisitos y resultados de votación
Evento de voto por poder no rastreado y Cliente no notificado después del anuncio, perdiendo cambios en los términos	Garantizar una fuente y flujo de información confiable. Diseñar un modelo operativo, respaldado por tecnología, que pueda notificar automáticamente a los clientes con posiciones, con una completa auditoría de seguimiento Contar con un marco de puntos de control para identificar fallas en las notificaciones Implementar un modelo de reporte STP para facilitar notificaciones oportunas y precisas
El Cliente no responde a la solicitud de voto	Establecer controles para recordatorios oportunos al cliente en caso de falta de respuesta Asegurar que exista un acuerdo contractual entre el Proveedor de Servicios de Valores y el Cliente que documente responsabilidades, incluidos tiempos de respuesta y plazos
La entrada manual de votos por poder por parte del Cliente en las aplicaciones de procesamiento conduce a instrucciones de voto incorrectas o preferencias mal registrada	Apoyar procesos operativos y tecnologías en el Proveedor de Servicios de Valores que permitan al Cliente o a las autoridades de votación ingresar la información de voto por poder Implementar procesamiento automatizado de datos con verificaciones de validación para evitar la entrada manual de datos de votación en diferentes sistemas de procesamiento Asegurar que exista una conciliación diaria completa para detectar desequilibrios o anomalías donde sistemas de procesamiento separados manejen transacciones de voto por poder
La gestión manual por parte del Proveedor de Servicios de Valores de materiales de voto como papeletas, poderes notariales, certificados de tenencia conduce a votos no autorizados	Implementar en el Proveedor de Servicios de Valores una solución centralizada de gestión documental con capacidades de seguimiento, incluyendo expiración de documentos e identificadores para diversas entidades cubiertas por estos documentos Implementar controles automáticos para la documentación que aseguren la verificación suficiente de las identidades del Cliente y las autoridades de votación y su elegibilidad

Descripción del riesgo	Mitigación del riesgo
El Proveedor de Servicios de Valores no envía o envía un evento de voto por poder incompleto o incorrecto al Subcustodio / CSD	Establecer controles y alertas de excepción para asegurar que el evento de voto por poder correcto sea identificado y completado con precisión Establecer controles en el Proveedor de Servicios de Valores para asegurar que el evento de voto por poder sea enviado al Subcustodio / CSD Asegurar controles de conciliación entre el Cliente / Proveedor de Servicios de Valores y el Subcustodio / CSD

10.5.3 Riesgos en Acciones Colectivas

Las acciones colectivas requieren controles robustos dado que los plazos para la finalización suelen ser prolongados. Los riesgos operativos pueden surgir cuando el Proveedor de Servicios de Valores no identifica una acción colectiva, cuando un Cliente no es notificado o no responde a la acción, o cuando no se realiza un seguimiento activo de la misma.

Ilustración 10.5.3 Tabla de Riesgos de Acciones Colectivas

Descripción del riesgo	Mitigación del riesgo
Evento y detalles de la acción colectiva no identificados por el Proveedor de Servicios de Valores	Asegurar una fuente confiable de información proveniente de fuentes independientes para permitir la comparación Garantizar que el Proveedor de Servicios de Valores implemente un Acuerdo de Nivel de Servicio (SLA) con el Subcustodio que establezca los requisitos y que los procesos se realicen conforme a los reglamentos del CSD y las regulaciones del mercado local
Cliente no informado sobre los detalles de la acción colectiva	Diseñar un modelo operativo en el Proveedor de Servicios de Valores para asegurar que la información de las acciones colectivas se calcule automáticamente considerando la disponibilidad de la posición Asegurar la conciliación de los detalles recibidos del Subcustodio / CSD con los libros y registros del Proveedor de Servicios de Valores Diseñar un modelo operativo en el Proveedor de Servicios de Valores para garantizar la entrada de datos precisa y completa, manteniendo registros de las tenencias y el historial de transacciones del Cliente para calcular la elegibilidad en la acción colectiva

Descripción del riesgo	Mitigación del riesgo
Decisión del cliente sobre la acción colectiva no ejecutada	Implementar seguimiento automatizado de las decisiones sobre acciones colectivas para todos los Clientes
El cliente no responde a la información sobre la acción colectiva	Establecer controles para recordatorios oportunos al Cliente en caso de falta de respuesta Asegurar que exista un acuerdo contractual entre el Proveedor de Servicios de Valores y el Cliente que documente las responsabilidades del Cliente, incluyendo tiempos de respuesta y fechas límite Garantizar que las notificaciones al Cliente expliquen claramente los derechos, plazos y el proceso para participar en los acuerdos
El proveedor de servicios de valores no envía, o envía información incompleta, sobre la acción colectiva al subcustodio / CSD o agente de la acción colectiva	Establecer controles para asegurar que el evento correcto de acción colectiva sea identificado y completado con precisión Establecer controles o alertas de excepción para garantizar que el evento de acción colectiva sea enviado al Subcustodio / CSD o agente de la acción colectiva Asegurar que existan controles de conciliación entre el Cliente / Proveedor de Servicios de Valores y el Subcustodio / CSD
Las acciones colectivas no son monitoreadas activamente por el proveedor de servicios de valores ni por los clientes a largo plazo	Mantener detalles de pago del Cliente autorizados y verificados, dado que las acciones colectivas pueden tardar un tiempo significativo en completarse Gestión activa por parte del Proveedor de Servicios de Valores y del Cliente en situaciones donde el Cliente haya cambiado de Proveedor, para asegurar que las acciones colectivas continúen siendo monitoreadas y que los pagos se realicen correctamente una vez recibidos

10.5.4 Riesgo en el Procesamiento de Ingresos

De manera similar al procesamiento de eventos corporativos, un riesgo clave para un Proveedor de Servicios de Valores y su Cliente es la falla en procesar la notificación de eventos de ingresos y la conciliación de los derechos correspondientes al Cliente. Nuevamente, la falta de completar este proceso podría resultar en un riesgo reputacional.

Ilustración 10.5.4 Tabla de Riesgos en el Procesamiento de Ingresos

Descripción del riesgo	Mitigación del riesgo
Evento de ingreso y detalles no identificados	Asegurar una fuente y flujo de información confiables provenientes de fuentes independientes para permitir la comparación Establecer controles para garantizar la precisión de los eventos de ingresos recibidos manualmente Asegurar que el Proveedor de Servicios de Valores cree un Acuerdo de Nivel de Servicio (SLA) con el Sub-custodio que establezca los requisitos y que los procesos se lleven a cabo en cumplimiento con los reglamentos del CSD y las regulaciones del mercado local
Ingreso no aplicado a los derechos del Cliente	Diseñar un modelo operativo, respaldado por tecnología, que asegure que los derechos del Cliente se calculen automáticamente considerando la disponibilidad de la posición y que dicha posición esté protegida Garantizar la conciliación de la posición de dinero recibida del Sub-custodio / CSD con los libros y registros del Proveedor de Servicios de Valores
FX no aplicado de manera precisa y oportuna según los requerimientos del Cliente	Proporcionar un seguimiento y registro automatizado de los requerimientos de FX del Cliente
Eventos no rastreados y Cliente no notificado después del anuncio, perdiendo cambios en los términos	Asegurar una fuente y flujo de información confiables Diseñar un modelo operativo, respaldado por tecnología, para notificar automáticamente a los tenedores Diseñar un marco de riesgo en el Proveedor de Servicios de Valores con puntos de control para identificar fallos en las notificaciones Implementar reportes STP para apoyar notificaciones oportunas y precisas
Instrucciones permanentes (SIs) no aplicadas a los derechos del Cliente	Asegurar un proceso robusto para almacenar y aplicar las instrucciones permanentes del Cliente (SIs) para garantizar que los derechos se apliquen correctamente conforme a la preferencia del Cliente Asegurar reportes oportunos a los Clientes, conforme a las instrucciones permanentes del Cliente para los derechos
Todo o parte de un derecho no recibido por el Proveedor de Servicios de Valores del Emisor	Asegurar que exista un modelo operativo, apoyado por tecnología, que monitoree los anuncios del Emisor y situaciones geopolíticas para anticipar cualquier situación que el Emisor pueda estar experimentando o a la que esté sujeto Garantizar la conciliación de la posición de dinero recibida del Sub-custodio / CSD con los libros y registros del Proveedor de Servicios de Valores

10.5.5 Riesgo en el Procesamiento de Impuestos

Un Proveedor de Servicios de Valores que ofrece servicios fiscales a sus Clientes debe asegurarse de que cada Cliente proporcione información fiscal precisa y completa. Además de los riesgos operativos, tanto el Proveedor como sus Clientes podrían estar expuestos a pérdidas financieras y, potencialmente, a multas por no entregar la información completa dentro de los plazos requeridos.

10.5.5.1 Riesgo de Aplicación de Alivio Fiscal en Origen

Aplicar el alivio fiscal adecuado en origen, dependiendo del estatus del Cliente y la documentación fiscal, puede constituir un riesgo significativo. Esto es especialmente relevante en mercados que no permiten la recuperación posterior de impuestos. La complejidad de los tratados fiscales y el desarrollo de vehículos/fondos fiscalmente transparentes han incrementado el riesgo de incumplimiento en la ejecución de estas actividades, lo que ha llevado al mayor uso de expertos fiscales.

Ilustración 10.5.5.1 Tabla de Riesgo de Alivio Fiscal en Origen

Descripción del riesgo	Mitigación del riesgo
Configuración incorrecta de la tabla de impuesto	Establecer una tabla de impuestos precisa Garantizar revisiones periódicas independientes de las tasas impositivas
No se aplica la tasa impositiva adecuada	Asegurar una revisión independiente de la configuración de la tasa impositiva en relación con el estado del Cliente Establecer permisos y controles duales “crear / aprobar” aplicados por el sistema para la configuración de la tasa impositiva
No se identifican los mercados con exención de impuestos en origen	Garantizar una fuente confiable y flujo de información Asegurar que el Proveedor de Servicios de Valores cree un Acuerdo de Nivel de Servicio (SLA) con el Subcustodio que establezca los requisitos y que los procesos se lleven a cabo en cumplimiento con las regulaciones del mercado local y las leyes fiscales
No se obtiene la documentación fiscal adecuada del Cliente antes de la presentación	Establecer eventos en el calendario y controles para recordar oportunamente a los Clientes la documentación fiscal requerida, incluidas las renovaciones Establecer informes de monitoreo / documentación faltante, y proporcionar información gerencial para identificar áreas de preocupación Asegurar que existan procedimientos para verificar que la documentación sea precisa y cumpla con todas las reglas aplicables contra el lavado de dinero (por ejemplo, el control de nombres de Beneficiarios Finales (UBO) contra listas de sanciones)
No se generan instrucciones de exención de impuestos en origen sobre las tenencias del Cliente	Implementar procesos y controles para asegurar la configuración de la exención de impuestos en origen sobre las tenencias del Cliente Establecer informes de exención de impuestos en origen y realizar un monitoreo continuo
No se reportan o pagan los Impuestos sobre Transacciones Financieras (ITF) / Impuesto de Timbre	Asegurar la comprensión de qué Clientes son elegibles o están exentos de los Impuestos sobre Transacciones Financieras (FTTs) Automatizar la identificación de las reglas de elegibilidad, los requisitos de pago y los de reporte

Descripción del riesgo	Mitigación del riesgo
No se completa la presentación requerida ante la autoridad fiscal	Establecer controles para cumplir con los requisitos pertinentes de las autoridades fiscales Implementar un monitoreo de cumplimiento para asegurar el conocimiento y la conformidad con cualquier cambio en los requisitos
Documentación fiscal del cliente no presentada ante las autoridades fiscales dentro de los plazos requeridos	Establecer controles y procesos de monitoreo para garantizar que los plazos requeridos sean conocidos Asegurar que la documentación fiscal válida sea presentada dentro de los plazos requeridos Conciliar los pagos proyectados de ingresos entre el CSD, el Subcustodio y el Custodio Global para identificar cualquier discrepancia en la documentación fiscal

10.5.5.2 Riesgo de Recuperación de Impuestos

Ciertos mercados, aunque permiten la reducción de impuestos dependiendo de los tratados y del estatus del Cliente, no funcionan de manera particularmente rápida y pueden tener plazos prolongados para recibir las recuperaciones de impuestos. Un punto para destacar aquí es la importancia de contar con los datos de pago actualizados en los archivos, ya que existe el riesgo de que la relación entre el Proveedor de Servicios de Valores y el Cliente haya finalizado antes de que se reciban los fondos de la recuperación de impuestos.

Ilustración 10.5.5.2 Tabla de Riesgo de Recuperación de Impuestos

Descripción del riesgo	Mitigación del riesgo
Configuración incorrecta de la tabla de impuestos	Establecer una tabla de impuestos precisa Asegurar revisiones independientes periódicas de las tasas impositivas
No se aplica la tasa impositiva adecuada	Asegurar una revisión independiente de la configuración de la tasa impositiva según el estado del Cliente Establecer permisos y controles dobles “crear / aprobar” en el sistema para la configuración de la tasa impositiva
No se identifican los mercados para la recuperación de impuestos	Garantizar una fuente y flujo de información confiables El Proveedor de Servicios de Valores debe asegurar que el Acuerdo de Nivel de Servicio (SLA) con el Subcustodio establezca los requisitos y que los procesos se realicen en cumplimiento con las regulaciones locales del mercado / leyes fiscales
No se obtiene la documentación fiscal adecuada del Cliente	Establecer eventos en el calendario / controles para recordar oportunamente a los Clientes sobre la documentación fiscal requerida, incluyendo renovaciones Establecer reportes de monitoreo / documentación faltante y reportes de gestión para identificar áreas de preocupación Asegurar que existan procedimientos para verificar que la documentación sea precisa y cumpla con todas las reglas aplicables de prevención de lavado de dinero (AML), por ejemplo, revisión de nombres de Beneficiarios Finales (UBO) contra listas de sanciones

Descripción del riesgo	Mitigación del riesgo
No se generan las solicitudes de recuperación de impuestos	Establecer reportes de reembolsos pendientes antiguos y realizar monitoreo continuo
No se presentan las solicitudes de recuperación de impuestos dentro de los plazos establecidos	Establecer controles de conciliación entre las instrucciones de recuperación de impuestos recibidas y las enviadas Establecer monitoreo de plazos y procesos de seguimiento con el Cliente
No se monitorea la recepción de los importes recuperados de impuestos	Establecer procesos de conciliación con Subcustodios y autoridades fiscales Establecer cronogramas de reembolso esperados y monitorear reembolsos fuera de plazo
Impuestos sobre Transacciones Financieras (FTT) / Impuesto de Timbre no reportados / pagados	Asegurar la comprensión de qué Clientes son elegibles o están exentos de los Impuestos sobre Transacciones Financieras (FTTs) Automatizar la identificación de las reglas de elegibilidad, los requisitos de pago y de reporte
El exceso de pago de impuestos en ciertas jurisdicciones no puede ser reembolsado y/o se imponen multas sobre las solicitudes de devolución de impuestos	Realizar controles adicionales sobre las tasas impositivas en mercados con poca o ninguna capacidad de recuperación (reclaim)
No se obtiene suficiente evidencia documental / prueba de elegibilidad para la devolución de impuestos por parte del Cliente antes de presentar la reclamación (reclamación especulativa), lo que genera retrasos en la devolución y riesgo de perder el estatus de agente fiscal	Asegurar la comprensión de los requisitos en cada jurisdicción Establecer un proceso detallado de validación previa al reembolso (pre-reclaim) Garantizar que el Cliente esté informado de los requisitos e implicaciones en caso de no cumplir con los plazos establecidos
Informes requeridos a la autoridad fiscal no completados	Establecer controles para seguir y cumplir con los requisitos de la autoridad fiscal correspondiente Implementar un monitoreo de cumplimiento para asegurar la conciencia y cumplimiento de cualquier cambio en los requisitos
Documentación fiscal del cliente no presentada ante las autoridades fiscales dentro de los plazos establecidos	Establecer controles y procesos de monitoreo para asegurar que los plazos requeridos sean conocidos por el Proveedor de Servicios de Valores Asegurar que el Cliente esté al tanto de los plazos y las implicaciones en caso de incumplimiento Garantizar que la documentación fiscal válida se presente dentro de los plazos requeridos

10.6 Riesgos Asociados al Cambio de Divisas (FX - Foreign Exchange)

Los riesgos relacionados con los servicios de cambio de divisas (FX) son principalmente operativos, aunque también podría presentarse un riesgo reputacional si existen fallos continuos. Desde la perspectiva del Cliente, es importante la divulgación de los métodos de fijación de precios de FX por parte del Proveedor de Servicios de Valores, así como instrucciones claras y oportunas. Desde el punto de vista del Proveedor de Servicios de Valores, un procesamiento preciso y oportuno se facilita mediante procesos automatizados (STP) e instrucciones permanentes (standing instructions).

Ilustración 10.6 Tabla de Riesgos Asociados al Cambio de Divisas

Descripción del riesgo	Mitigación del riesgo
Falta de una metodología clara para la fijación de precios del FX	Asegurar una documentación clara entre el Proveedor de Servicios de Valores y el Cliente que establezca el enfoque estándar para la fijación de precios de FX
El FX no se procesa de manera precisa, completa y oportuna según los requisitos del Cliente	Garantizar un proceso claro de apertura de cuenta y configuración de instrucciones permanentes de FX con controles y permisos duales en el sistema para 'crear / aprobar' Implementar revisiones periódicas y confirmaciones del establecimiento de cuentas/instrucciones permanentes Implementar un modelo operativo de procesamiento directo (STP) con una gestión robusta de colas Asegurar que exista un proceso de confirmación con registro completo de auditoría
Fallo en la liquidación de operaciones de FX	Selección de contrapartes de FX aprobadas por el Proveedor de Servicios de Valores Monitoreo de exposiciones Uso de compensación de contrapartes (CLS - Continuous Linked Settlement) Reconciliación diaria robusta

11. Riesgo de Seguridad de la Información y Protección de Datos

11.1 Introducción

Este capítulo analiza cómo un Proveedor de Servicios de Valores garantiza la seguridad de la información y la protección de los datos mediante la implementación de medidas tales como seguridad de red, seguridad de aplicaciones, seguridad en puntos finales y ciberseguridad. Cada una de estas medidas debe gestionarse para asegurar la confidencialidad, integridad y disponibilidad continuas de los datos tanto del Proveedor de Servicios de Valores como del Cliente.

11.2 Definición

El riesgo de seguridad de la información y protección de datos es el riesgo al que está expuesto un Proveedor de Servicios de Valores frente a amenazas y ciberataques relacionados con la operación y uso de sistemas de información. Las amenazas pueden originarse por factores internos o externos, materializarse de manera electrónica o física, y comprometer a las organizaciones por diferentes métodos como malware, ingeniería social o cadenas de suministro.

11.3 Panorama de la Seguridad de la Información

Aunque el robo de activos y dinero suele ser una amenaza clave para un Proveedor de Servicios de Valores, también puede estar expuesto al robo de información valiosa. Los libros, registros y bases de datos que mantienen estos proveedores pueden proporcionar a los delincuentes acceso a datos sensibles como inversiones de clientes, detalles de portafolios, desempeño y estrategias, información de relaciones y acuerdos de tarifas. Los ataques cibernéticos y de ransomware pueden causar daños sustanciales a los clientes y afectar la capacidad del proveedor para ejecutar servicios críticos.

Grupos de amenazas avanzadas persistentes (APT) de estados-nación y bandas criminales organizadas están aumentando su sofisticación, representando un desafío significativo para los profesionales de seguridad encargados de proteger los datos. El ciberespacio sigue siendo un dominio operativo preferido para el espionaje industrial y una herramienta para algunos estados-nación para apoyar sus objetivos de política económica. Estos actores de amenaza, si tienen éxito, pueden permanecer en los sistemas informáticos de un Proveedor de Servicios de Valores para obtener información en favor de los objetivos de política exterior de su estado patrocinador.

Por ello, es fundamental contar con un programa de seguridad de la información sólido, con un conjunto robusto de controles de seguridad que aseguren la integridad y solvencia de la información del proveedor. Estos proveedores dependen en gran medida de los sistemas tecnológicos que soportan sus actividades. La implementación de una estrategia de defensa en profundidad basada en capas concéntricas de defensa es la forma más aceptada para prevenir actividades maliciosas informáticas.

Las medidas de seguridad de la información, tales como la segregación de redes, aislamiento de internet y la resiliencia, están diseñadas para evitar que un solo punto de falla comprometa por completo recursos o sistemas críticos. Las protecciones se aplican en el perímetro externo, en áreas internas y en las ubicaciones más sensibles o valiosas. Se espera que los problemas ocurran en varios lugares y que las defensas sean probadas por quienes intentan causar daño.

Un entorno bien construido garantiza que la falla de un componente no provoque la caída total del sistema. Esto implica “defensas en capas”, “defensa en profundidad”, “seguridad desde el diseño”, “accesos con privilegios mínimos”, “accesos

según necesidad de conocimiento", "segregación de funciones", "suponer brechas" y la implementación de controles fuertes para hacerlos cumplir.

Para que un programa de Seguridad de la Información sea efectivo, es fundamental entender primero qué es lo que se intenta proteger. Identificar procesos críticos y conjuntos de datos ayuda a construir la base para prácticas sólidas de seguridad. Un Proveedor de Servicios de Valores puede usar esquemas de clasificación de datos para identificar continuamente qué elementos de su organización son los más importantes y, por tanto, requieren mayor esfuerzo de protección. Evaluar los riesgos de aplicaciones, infraestructura y procesos críticos también ayuda a enfocar los esfuerzos de manera priorizada. No todas las áreas tienen igual importancia ni requieren los mismos niveles de protección. Comprender qué se debe proteger y cómo protegerlo mejor ayuda a asegurar un marco confiable de seguridad de la información.

El continuo desarrollo en Seguridad de la Información, y la dependencia de tecnologías cambiantes (p. ej., robótica, aprendizaje automático, inteligencia artificial, almacenamiento en la nube, criptomonedas y blockchain), impactan a los Proveedores de Servicios de Valores. La amenaza a la Seguridad de la Información probablemente aumente y las organizaciones deben seguir invirtiendo en estrategias de mitigación de riesgos, así como desarrollar redes colaborativas y técnicas activas específicas para los Servicios de Valores.

11.4 Áreas Clave de Riesgo en Seguridad de la Información y Protección de Datos

En la cadena de valor de Servicios de Valores, se pueden distinguir cuatro grandes grupos de riesgos de seguridad de la información y protección de datos, que pueden ser de origen interno o externo. A continuación, se identifican las amenazas clave y los motivos detrás de ellas.

11.4.1 Ciberataques

Las consecuencias adversas significativas derivadas de ciberataques se observan con demasiada frecuencia en muchas industrias, servicios y entornos de infraestructura. Esta amenaza es real y requiere atención constante y detallada para quienes operan en la industria de Servicios de Valores. Como se ha visto en sectores como salud, educación y energía, los ciberataques mayores — motivados por la intención de interrumpir materialmente infraestructuras clave — se encuentran entre las amenazas más significativas y de mayor impacto.

Los Proveedores de Servicios de Valores son la infraestructura del sector de inversión, y la interrupción de CSDs (depósitos centrales de valores), a nivel global y doméstico, de firmas financieras significativas (incluidos custodios globales y subcustodios), junto con utilidades industriales de amplia escala (como SWIFT y otros grandes proveedores de la industria), podrían tener un efecto adverso mayor en el flujo de dinero a nivel nacional e internacional.

Por regulación local, un Proveedor de Servicios de Valores debe implementar un marco de ciberseguridad aceptado por la industria. Existen estándares como la serie ISO 27000, el Marco de Ciberseguridad NIST y el Perfil de Servicios Financieros del Cyber Risk Institute para ayudar a medir las políticas, estándares, controles y procedimientos de ciberseguridad de un proveedor. En caso de un ciberataque, la gestión debe reaccionar rápidamente para detectar el ataque, aislar el problema y evaluar el impacto. Por ello, los principales marcos de seguridad basan sus controles defensivos en los principios de "gobernar, identificar, proteger, detectar, responder y recuperarse".

Aunque un Proveedor de Servicios de Valores debe tener un marco de ciberseguridad robusto, también debe evaluar el riesgo de ciberataques a sus Clientes, Proveedores de Terceros y contrapartes. La diligencia debida del programa de gestión de riesgos cibernéticos y controles asociados a estas partes es crítica. Se deben imponer obligaciones contractuales adecuadas para que cumplan con las políticas y estándares del Proveedor de Servicios de Valores, lo que puede incluir un proceso de certificación para que la parte demuestre su cumplimiento.

Entre todos los ciberataques que podrían generar un impacto sistémico en el mercado, un ataque de ransomware contra un Proveedor de Servicios de Valores grande es uno de los más dañinos potencialmente. Un ataque de ransomware a un Proveedor puede causar problemas significativos de liquidez en el mercado y eliminar la capacidad de dicho proveedor para administrar los activos de sus clientes. Si bien las Instituciones Financieras de Importancia Sistémica Global (SIFIs) y las grandes instituciones financieras pueden tener defensas más fuertes, es plausible que un actor motivado perpetre este delito. En tal caso, el alcance podría ser amplio y el impacto muy alto para el mercado.

El motivo habitual de un ciberataque suele ser el beneficio financiero o apoyar la política económica de un estado-nación.

Estudio de Caso: ICBC

ICBC Financial Services, subsidiaria del Banco Industrial y Comercial de China (ICBC), sufrió un ataque de ransomware el 8 de noviembre de 2023. El incidente interrumpió las operaciones y sistemas del ICBC, afectando el nivel de servicio en la ejecución de transacciones de clientes y comunicaciones. El suceso generó inquietudes generales sobre la postura de ciberseguridad de las instituciones financieras.

ICBC actuó tras descubrir el ataque, reportándolo a las autoridades mientras coordinaba con expertos en ciberseguridad. El incidente también fue reportado públicamente en un artículo del Financial Times al día siguiente.

El ataque fue atribuido al grupo de hackers LockBit, un grupo de ransomware como servicio (RaaS) activo desde septiembre de 2019. Su ransomware es usado para ataques altamente dirigidos contra empresas y organizaciones, también conocido como 'virus cripto' debido a que sus demandas de rescate giran en torno a pagos financieros a cambio de la desencriptación. Es un virus auto-propagante que bloquea el acceso de usuarios a sistemas informáticos, apuntando a empresas y organizaciones gubernamentales a nivel global con amenazas como interrupción de operaciones, extorsión para beneficio financiero, robo de datos y publicación ilegal como chantaje si la víctima no cumple.

11.4.2 Robo de Activos

Un Proveedor de Servicios de Valores puede ser particularmente susceptible al robo de activos. Esto se debe a que maneja diariamente valores significativos en transacciones, especialmente instrucciones de entrega/recepción de valores contra pago (DvP / RvP), pagos grandes de vencimientos de bonos, eventos corporativos, pagos de dividendos e ingresos, pagos y depósitos de repos tripartitos.

El motivo del robo de activos generalmente es la obtención de beneficio financiero.

11.4.3 Robo de Información

El riesgo de robo de información sensible es una preocupación especial para un Proveedor de Servicios de Valores. Esto podría incluir el robo de:

- Propiedad intelectual, como contratos con Clientes, cronogramas de precios, información sobre productos o servicios
- Datos sensibles del Cliente, como posiciones de valores, tenencias, estados de cuenta y datos personales de contacto

El motivo del robo de información puede ser obtener una ventaja sobre una organización competidora o causar un daño reputacional si la información es filtrada intencionalmente. Dependiendo de la cantidad y tipo de información robada, este robo podría ser utilizado para apoyar la política económica de un estado-nación. También puede ser usado para obtener beneficio financiero, ya sea mediante extorsión solicitando un rescate a cambio de mantener la confidencialidad, o mediante operaciones comerciales basadas en información no divulgada.

11.4.4 Manipulación del Mercado

La manipulación del mercado es el riesgo de manipulación de precios y/o fuentes de noticias mediante un ataque coordinado de un grupo de APT (Amenaza Avanzada Persistente). Los precios de las acciones se ajustarían automáticamente y las órdenes de compra/venta se ejecutarían automáticamente, generando beneficio financiero potencial si los atacantes fueran accionistas. Para un Proveedor de Servicios de Valores, esto podría incluir manipulación mediante:

- Múltiples órdenes simultáneas de compra y venta de una acción, donde la actividad incrementada artificialmente eleva el precio de la acción
- Rumores simultáneos o “noticias falsas” sobre una acción, manipulando ilícitamente múltiples fuentes de noticias
- Alimentaciones de precios intradía manipuladas simultáneamente por proveedores externos de datos financieros
- Cambiar los términos de una reorganización compleja o evento corporativo, como una fusión, para afectar artificialmente su atractivo en el mercado
- Penetrar y comprometer una fuente de precios de un proveedor externo o una agencia de noticias para influir en el precio de una acción específica, permitiendo al actor malicioso comprar o vender a ese precio artificial. Dado que el compromiso del sistema o red está físicamente alejado de la transacción financiera, este tipo de comercio ilícito podría ser difícil de rastrear

El motivo de la manipulación del mercado es la ganancia financiera, buscando manipular artificialmente el precio de un activo.

11.5 Amenazas de Seguridad de la Información y Riesgo de Protección de Datos

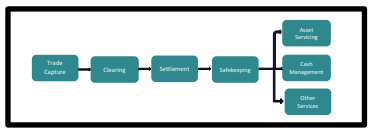
La tabla a continuación destaca las principales amenazas de riesgo de Seguridad de la Información y Protección de Datos que podrían impactar a un Proveedor de Servicios de Valores.

Ilustración 11.5: Tabla de Riesgos de Seguridad de la Información y Protección de Datos

Descripción del riesgo	Mitigación del riesgo
Falta de confidencialidad de los valores en tránsito	Asegurar que los datos estén debidamente encriptados durante la transmisión electrónica de instrucciones sobre valores (por ejemplo, SWIFT) Utilizar protocolos o canales de comunicación seguros al transmitir datos de valores, tales como Secure Sockets Layer (SSL), Secure File Transfer Protocols (SFTP) o soluciones similares a la banca electrónica
Falta de confidencialidad de los valores en almacenamiento	Utilizar cifrado de datos al almacenar información sobre valores en sistemas de archivos o bases de datos Establecer controles de acceso lógico robustos y sistemas de privilegios de usuario basados en el principio de "necesidad de conocer", con procesos periódicos de renovación y revisión Garantizar que existan rutinas de cifrado de datos con la suficiente fortaleza para resistir ataques de fuerza bruta
Actividad sospechosa no detectada	Desplegar sistemas de detección de intrusiones para monitorear tráfico sospechoso Implementar una estrategia de registro y monitoreo para sistemas críticos que asegure que todas las comunicaciones y acciones electrónicas se investiguen adecuadamente en busca de comportamientos sospechosos
Falta de conciencia del personal sobre las prácticas esperadas de seguridad de la información	Crear e implementar programas de formación robustos que eduquen a los usuarios sobre comportamientos esperados y prácticas adecuadas de seguridad de la información Desarrollar campañas de concientización Realizar intentos organizados y regulares de phishing con fines educativos
Sistemas de procesamiento de valores vulnerables a ataques electrónicos	Desplegar programas de gestión de vulnerabilidades para asegurar que los sistemas de procesamiento de valores no sean susceptibles a amenazas actuales Crear rutinas de gestión de parches para asegurar que los sistemas se actualicen regularmente conforme se descubran nuevas vulnerabilidades Aprovechar programas de pruebas de penetración para simular ataques reales y mejorar defensas contra técnicas manuales
Privilegios de acceso de empleados a datos de valores no gestionados adecuadamente	Implementar programas de gestión de identidad y acceso que administren todas las fases del ciclo de vida de la identidad Usar recertificaciones de acceso para garantizar que a quienes ya no requieren acceso a datos de valores se les revoque dicho acceso Implementar autenticación multifactor para sistemas críticos Asegurar la existencia de rutinas de terminación que monitoreen empleados que dejan la empresa para remover apropiadamente su acceso a sistemas críticos
Sistemas tecnológicos no reforzados contra posibles ciberataques	Mantener y desplegar documentos de endurecimiento de sistemas (documentos de base de seguridad) y scripts automatizados para aumentar la resiliencia técnica contra posibles ataques Evaluar las configuraciones de sistemas anualmente para asegurar que los cambios requeridos se incorporen a la línea base de seguridad

12. Riesgo de Tecnología de la Información

12.1 Introducción



Al igual que la información proporcionada en el capítulo sobre Seguridad de la Información y Protección de Datos, las actividades de Servicios de Valores dependen en gran medida de la infraestructura tecnológica subyacente para operar cada día. Un sistema tecnológico poco fiable o inestable puede resultar en la incapacidad para procesar operaciones, dejando esencialmente a un Proveedor de Servicios de Valores en un estado inoperable. Por lo tanto, es importante que los Proveedores de Servicios de Valores comprendan el riesgo tecnológico y cómo estos pueden impactar positiva o negativamente las operaciones.

12.2 Definición

El riesgo de Tecnología de la Información es una categoría amplia que, en esencia, se utiliza para definir casi cualquier cosa que pueda salir mal dentro de un entorno tecnológico. Esto incluye amenazas a los datos, procesos y/o sistemas críticos.

12.3 Confiabilidad y Resiliencia

Una de las áreas principales en las que se enfoca el riesgo tecnológico es la confiabilidad. Los sistemas deben construirse con la resiliencia adecuada que asegure que continúen operando durante momentos de crisis.

12.3.1 Evaluaciones de Impacto en el Negocio

El grado en que un sistema debe continuar operando durante un incidente se define a través de una Evaluación Integral de Impacto en el Negocio. Periódicamente, alineado con el apetito de riesgo del Proveedor de Servicios de Valores, cada Proveedor debe evaluar el impacto que una interrupción puede tener en cada producto y servicio que opera. Estas evaluaciones deben revisar requisitos legales, regulatorios y contractuales, definiendo el impacto global que una interrupción tendría en la organización.

Un Proveedor debe asegurar una comprensión clara de qué sistemas son críticos para el negocio y priorizar la financiación adecuadamente para proteger dichos sistemas. Igual de importante es determinar una estrategia de ubicación y entender cuánto infraestructura debe construirse y operarse desde una o más ubicaciones separadas, considerando también aspectos geopolíticos (ver capítulo sobre Riesgos Geopolíticos para más información).

Finalmente, se debe asegurar que existan arreglos de recuperación entre regiones para actividades críticas, permitiendo la recuperación de carga de trabajo de una ubicación operativa a otra. Al igual que con otros planes de contingencia, estos arreglos de recuperación deben ser probados regularmente.

12.3.2 Objetivo de Tiempo de Recuperación (RTO)

Basado en los resultados del análisis de impacto, se determina un Objetivo de Tiempo de Recuperación. Este objetivo se incorpora en la estrategia general de continuidad del negocio.

Elegir tiempos de recuperación precisos es fundamental para asegurar la continuidad apropiada del negocio, especialmente para negocios críticos tanto para el Proveedor como para la industria en general. Por ejemplo, un sistema o producto crítico podría requerir un tiempo de recuperación de dos horas. En este caso, la tecnología debe garantizar que incluso durante interrupciones inesperadas, el producto esté indisponible no más de dos horas. Dada la importancia sistémica del sector financiero, existen requisitos regulatorios que determinan los objetivos de tiempo de recuperación y que exigen pruebas regulares de recuperación del sistema. Aun así, un Proveedor de Servicios de Valores debe cumplir múltiples plazos intradía para asegurar que las transacciones de valores y dinero se completen; por lo tanto, dependiendo del momento en que ocurra un incidente, podrían necesitar planearse acciones adicionales de contingencia.

12.4 Marcos de Trabajo de Tecnología de la Información

Existen marcos de trabajo generalmente aceptados que articulan áreas de enfoque para crear un programa robusto de gestión del riesgo tecnológico.

- Dos de los marcos más comunes actualmente usados son:
- Organización Internacional de Normalización (ISO) 20000 – Gestión de Servicios de Tecnología de la Información
- Biblioteca de Infraestructura de Tecnología de la Información (ITIL) versión 4

Un Proveedor que implemente sistemas de inteligencia artificial puede considerar además los siguientes marcos:

- ISO 23894 - Marco para Sistemas de Inteligencia Artificial (IA) que usan Aprendizaje Automático (ML)
- ISO 42001 - Tecnología de la Información IA, guía para la gestión de riesgos

12.5 Amenazas del Riesgo Tecnológico

La tabla a continuación resalta riesgos específicos desde la perspectiva del Proveedor de Servicios de Valores, sirviendo como un subconjunto de lo cubierto por los marcos más amplios.

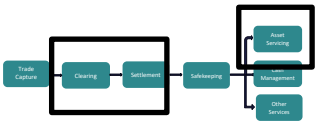
Ilustración 12.5 Tabla de Riesgo de Tecnología de la Información

Descripción del riesgo	Mitigación del riesgo
Falta un inventario tecnológico de los sistemas de valores	Asegurar que el sistema de gestión de Tecnología de la Información incluya todos los componentes necesarios para operar los sistemas, que la licencia esté actualizada y que los registros de expiración y renovaciones se realicen a tiempo Desplegar un sistema de gestión de Tecnología de la Información que rastree y catalogue los activos/sistemas tecnológicos importantes para el procesamiento de valores Identificar al propietario del sistema en el sistema de gestión de Tecnología de la Información para cada componente tecnológico, para asegurar que las personas adecuadas sean notificadas si ocurren problemas en el sistema
Existe una limitada realización de pruebas antes de poner las aplicaciones de valores en producción	Crear un equipo de aseguramiento de calidad para probar todos los aspectos de los sistemas de valores antes de que una aplicación pase a producción Realizar, si es posible, pruebas “smoke” en los sistemas en vivo de manera que no interrumpan las operaciones antes de ponerlos en producción Realizar pruebas de regresión para asegurar que las nuevas funcionalidades no afecten negativamente las actividades heredadas Crear procedimientos de reversión para asegurar que los nuevos cambios puedan revertirse en los entornos de producción si ocurren interrupciones del sistema
La planificación deficiente de la capacidad resulta en problemas de rendimiento del sistema	Usar sistemas de gestión de rendimiento para monitorear la utilización del sistema e identificar picos inusuales Asegurar que los planes de construcción tecnológica consideren las métricas de gestión de rendimiento existentes, junto con los requerimientos de crecimiento proyectado y condiciones de estrés
Faltan procedimientos de respaldo para las interfaces	Completar pruebas y monitoreo de la operación de interfaces entre el sistema de valores, sistema de dinero, CSDs y fuentes externas de datos Implementar procedimientos de respaldo para contingencias y cortes Implementar tiempos de recuperación definidos en cumplimiento con requisitos regulatorios y de SLA
Prácticas limitadas de gestión de cambios que resultan en pérdida de integridad de las plataformas de valores	Documentar todos los cambios a nivel de producción como parte de un programa formal de gestión de cambios Gestionar efectivamente la notificación y aprobación de todos los cambios en el sistema Mantener registros que rastreen todos los cambios en el sistema para facilitar la resolución de incidentes
La infraestructura que ejecuta los sistemas de procesamiento de valores provoca interrupciones del sistema que no son monitoreadas	Aprovechar un centro de operaciones técnicas para monitorear la actividad en todos los aspectos de un programa de Tecnología de la Información Configurar alarmas para alertar al personal sobre comportamientos inusuales o preocupantes del sistema Establecer protocolos de escalamiento para comunicar eficazmente problemas del sistema

Descripción del riesgo	Mitigación del riesgo
Las deficientes prácticas de respuesta ante incidentes causan tiempos prolongados de recuperación	Implementar una función de gestión de incidentes que actúe como un elemento de escalamiento dentro de una función de monitoreo existente Asegurar que existan rutinas de gestión de incidentes que incluyan notificación y escalamiento adecuados para todos los incidentes potenciales. Esto podría incluir puntos únicos de contacto, diferentes canales de comunicación y mecanismos de escalamiento
Se adopta nueva tecnología sin el conocimiento o experiencia suficiente	Realizar una evaluación de cualquier nueva tecnología, como la inteligencia artificial (IA) Adoptar un marco aceptado por la industria para nuevas tecnologías cuando esté disponible

13. Riesgo de Crédito

13.1 Introducción



El riesgo de crédito para un Proveedor de Servicios de Valores puede originarse en obligaciones dentro del balance, como préstamos u otras facilidades crediticias, si un Cliente no realiza los pagos requeridos. El riesgo de crédito puede generarse por elementos como liquidación de operaciones, riesgo de crédito contraparte e indemnizaciones por préstamos de valores, así como cartas de crédito. Para un Cliente, el riesgo de crédito puede originarse en elementos dentro del balance mantenidos por un Proveedor de Servicios de Valores, como depósitos en dinero, en caso de incumplimiento del Proveedor.

Como entidad regulada, un Proveedor de Servicios de Valores debe implementar acciones como evaluación apropiada del riesgo de crédito, establecimiento de límites y monitoreo de exposición para asegurar que el crédito asumido no supere su apetito de riesgo y/o restricciones regulatorias (como reglas de exposición grande). De igual manera, los Clientes deben realizar su propia evaluación de riesgo de crédito del Proveedor. Este capítulo explora estas acciones, los riesgos al extender crédito y los posibles mitigantes.

13.2 Definición

El riesgo de crédito es el riesgo de pérdida derivado del incumplimiento de un deudor debido a su incapacidad o falta de voluntad para cumplir sus obligaciones financieras en tiempo y forma (por ejemplo, derivado de una facilidad crediticia otorgada a un participante prestatario). Para un Proveedor de Servicios de Valores, el deudor será principalmente su Cliente, una contraparte de trading o tesorería.

13.3 Panorama del Riesgo de Crédito

Hay múltiples participantes involucrados en el ciclo de vida de los Servicios de Valores y, como resultado, la necesidad de crédito puede surgir en muchos momentos. Los participantes que asumen riesgo crediticio incluyen Proveedores de Servicios de Valores (Custodios Globales, Subcustodios e (I)CSDs) así como Clientes.

Como banco del Cliente, un Proveedor de Servicios de Valores proveerá una cuenta de depósito a la vista para que el Cliente financie sus inversiones y costos operativos, y para la recepción de ingresos y cobros. Un Proveedor puede optar por proveer al Cliente facilidades de crédito (particularmente crédito intradía) para permitirle cumplir obligaciones de liquidación o adelantar ingresos no recibidos aún del emisor o contraparte de una operación compensada. Estas facilidades pueden ser no asesoradas y no comprometidas y pueden ser retiradas por razones de país o contraparte.

El Proveedor de Servicios de Valores realizará análisis y establecerá límites tomando en cuenta la calificación del obligado, garantías (tipos y valor de activos sobre los cuales tiene un derecho de retención) y la capacidad financiera / adecuación de capital de la entidad que otorga el crédito. Además, hay ciertos mercados (por ejemplo, mercados del Medio Oriente) donde no se permiten exposiciones nocturnas o sobregiros y para los cuales un Proveedor no puede proveer facilidades. Como organizaciones con apetito de riesgo muy bajo, los CSDs suelen operar políticas conservadoras y, por lo tanto, las líneas de crédito se otorgan en principio solo contra colateral.

Un riesgo crediticio también surge para un Cliente que mantiene una cuenta en dinero con un Proveedor (por ejemplo, un Custodio Global o Subcustodio en ciertos mercados restringidos). El Cliente debe asegurarse de haber realizado su propio análisis crediticio de la entidad legal específica a la que está expuesto, lo que puede incluir un análisis de riesgo de concentración. Los Clientes también deben considerar en qué medida existen esquemas gubernamentales de garantía de depósitos y si aplican reglas de preferencia de depósito (que pueden favorecer a ciertos domicilios de depositantes sobre otros).

13.4 Áreas Clave de Riesgo de Crédito

El riesgo crediticio puede ocurrir en múltiples puntos en la cadena de valor de los Servicios de Valores. Las áreas clave para un Proveedor de Servicios de Valores se describen a continuación.

13.4.1 Compensación

Un Proveedor de Servicios de Valores ofrece al Cliente la capacidad de ejecutar operaciones “en bolsa” y debe asegurarse de que el Cliente pueda cumplir con todas sus obligaciones diarias de liquidación y con las obligaciones hacia la bolsa para mantener pagos de margen. El Proveedor, actuando en capacidad de GCM, está expuesto a riesgo crediticio por asumir el riesgo principal de las ejecuciones del Cliente y, por lo tanto, asumiendo responsabilidad ante el CCP en caso de fallo en la liquidación o insolvencia del Cliente. Para protegerse de esta responsabilidad (entre la fecha de operación y la fecha de liquidación, incluyendo fluctuaciones de precio ‘mark-to-market’), el Proveedor tomará colateral elegible del Cliente para mitigar este riesgo.

El CCP se protege manteniendo margen inicial tanto del comprador como del vendedor para asegurar que las disminuciones de valor estén cubiertas. Además, realiza un mark-to-market diario para asegurar que ambas partes puedan cumplir con sus obligaciones.

Un Proveedor mitigará su riesgo mediante un análisis riguroso y continuo del riesgo del Cliente y establecerá límites sobre la capacidad del Cliente para ejecutar operaciones y sus obligaciones de liquidación resultantes. También debe asegurarse de que el Cliente tenga disponible colateral, como valores o dinero, para cumplir con llamadas de margen y el dinero para cumplir con la obligación diaria de liquidación en dinero con el CCP. Si el colateral es insuficiente, se realiza una llamada para colateral adicional elegible.

Esta facilidad de compensación se realiza normalmente en una agencia de terceros. Esto ocurre cuando el Cliente tiene relación directa con la organización de compensación y nombra a un Proveedor para operar esta cuenta en nombre del Cliente. Los acuerdos de nivel de servicio y contratos describen claramente las operaciones de la cuenta. Si el Cliente no puede proporcionar fondos a tiempo, existe el riesgo de que el Proveedor mantenga activos como principal hasta que dichos valores sean totalmente pagados por el Cliente. En tal caso, el Proveedor está expuesto tanto a riesgo crediticio respecto al Cliente como a riesgo de mercado por el valor de los valores.

Dadas las obligaciones sustanciales derivadas del trading en bolsa, estos arreglos requieren un alto nivel de automatización en análisis de riesgo y flujos de precios para monitorear continuamente las actividades de trading del Cliente y los requisitos de colateral. Deben existir procedimientos claros y acuerdos que permitan al Proveedor “detener la compensación” en caso de incumplimiento o insolvencia del Cliente.

13.4.2 Liquidación

Un riesgo claro es que los valores sean entregados a la contraparte comercial, pero no se reciba el pago, o que el pago sea enviado pero no se reciban los valores. Ambas situaciones llevan a exposición crediticia para el Proveedor y, en última instancia, para el Cliente.

Para mitigar este riesgo, se ha introducido el intercambio simultáneo de valores y dinero (Delivery vs Payment; Receipt vs Payment). Sin embargo, existen diferentes tipos de modelos DvP/RvP según el mercado (incluyendo intercambio simultáneo por transacción individual hasta intercambio basado en neteo de valores y/o dinero), junto con ciertos mercados más incipientes que aún no implementan DvP/RvP verdadero. Además, no todos los tipos de transacciones pueden beneficiarse de un arreglo DvP/RvP; por ejemplo, acciones corporativas incluyendo IPOs pueden requerir pago en dinero previo a la recepción de valores o activos.

Además, los mercados operan con distintos ciclos de liquidación después de la fecha de operación: mientras más largo el ciclo, mayor el riesgo crediticio. En condiciones de mercado desafiantes, esto puede crear incertidumbre sobre si una operación se liquidará o no. Para reducir este riesgo, la mayoría de los mercados operan ahora con un ciclo de liquidación T+2 (fecha de operación más dos días) y algunos han cambiado, y otros planean cambiar, a ciclos T+1 o liquidación en el mismo día.

13.4.3 Liquidación Contractual

Un Proveedor de Servicios de Valores frecuentemente ofrece contabilidad en fecha contractual de liquidación. En este caso, el Proveedor decide, basado principalmente en el riesgo país de un mercado particular, reflejar en la cuenta del Cliente la liquidación en la fecha valor esperada en lugar de la fecha real. En el contexto de la liquidación contractual de los productos de venta, el Proveedor asume riesgo crediticio sobre la contraparte para la recepción del dinero, así como sobre el Cliente si este se vuelve insolvente y el dinero no puede ser recibido del mercado.

El Proveedor realiza pre-matching y afirmación (positiva y negativa) conforme a las convenciones locales. Los plazos varían según el mercado pero normalmente se realizan un día antes de la fecha de liquidación (SD-1). En algunos mercados, el pre-matching/afirmación es una obligación vinculante para liquidar operaciones en la fecha pactada. En estos casos, en el contexto de liquidación contractual, el Proveedor asume riesgo crediticio sobre su Cliente en el momento del matching/afirmación si el Cliente falla en proveer financiamiento suficiente para la fecha de liquidación.

Al considerar la extensión de servicios de liquidación contractual, el Proveedor debe tener en cuenta las leyes y regulaciones aplicables, que pueden variar por jurisdicción y regulador (por ejemplo, reglas UK CASS, leyes bancarias federales de EE.UU., etc.).

13.4.4 Ingresos Contractuales

El Proveedor también puede ofrecer contabilidad en fecha contractual de ingresos en ciertos mercados. De nuevo, el Proveedor decide basado principalmente en el riesgo país reflejar en la cuenta del Cliente la fecha valor esperada del pago de ingresos en lugar de la fecha real. En este caso, el Proveedor asume riesgo crediticio sobre el Emisor para la recepción del dinero.

También deben considerarse todas las leyes y regulaciones aplicables en el contexto de la provisión de ingresos contractuales.

13.5 Cláusulas de Protección Crediticia

Un Proveedor generalmente tendrá derecho de recurrir a los activos del Cliente, incluyendo (frecuentemente) cuentas de dinero. Este derecho generalmente protege contra pérdidas por falta de pago de liquidaciones o pagos de honorarios y se establece como garantía contra deudas y/o para satisfacción de deuda. Este derecho generalmente está establecido en el contrato con el Cliente pero también puede surgir por ley. Además de atender preocupaciones de riesgo crediticio, la presencia o ausencia de este recurso puede afectar las consideraciones de capital regulatorio para el Proveedor.

La ley local aplicable (usualmente la que rige la cuenta de valores o dinero en el Proveedor) puede establecer requisitos que deben cumplirse para que este recurso sea dinero y puede limitar el recurso dinero disponible. Por tanto, es importante considerar que el ejercicio de este recurso puede estar limitado por ley, regulación o guía regulatoria. Por ejemplo, si se incluyen cuentas de dinero, puede haber restricciones regulatorias para que el Proveedor use la “compensación” además de otros requisitos para proteger a los Clientes (véase, por ejemplo, UK CASS 7).

El recurso sobre activos generalmente comprende dos aspectos: derecho de retención y derecho de venta.

13.5.1 Derecho de Retención

Esto es cuando el Proveedor que retiene o controla activos del Cliente, aunque no es propietario de ellos, puede retener activos específicos del Cliente (por ejemplo, activos ligados a una transacción) o activos cuyo valor corresponde a la deuda. Retener activos por un valor mayor o fuera del alcance del servicio puede ser cuestionado bajo leyes locales o regulaciones. En cualquier caso, la permisibilidad de estos derechos adicionales debe revisarse cuidadosamente.

Por sí solo, el derecho de retención no da derecho a vender los activos, por lo que no extingue la deuda. Sin embargo, puede usarse para asegurar el pago por parte del Cliente deudor (un gravamen es un ejemplo de derecho de retención).

13.5.2 Derecho de Venta

Esto es cuando el Proveedor puede disponer de activos del Cliente y retener los ingresos de la venta para satisfacer una deuda, permitiendo usualmente al Proveedor asumir la propiedad de los activos antes de ejercer el derecho de venta. El Proveedor también suele tener un derecho de retención que puede haber sido ejercido (o requerido) antes del derecho de venta.

Las leyes locales pueden crear mecanismos para la disponibilidad y ejercicio de ambos derechos, pero cada derecho debe estar específicamente contemplado en el contrato.

Generalmente, todas las partes de un arreglo con recurso a activos deberían considerar:

- Requisitos legales o regulatorios aplicables, tales como si el acuerdo de garantía debe estar documentado por escrito (y cómo), y cómo el colateral es “proporcionado”, “controlado” o está en “posesión” del Proveedor
- Certidumbre en la descripción de los valores o cuentas sujetas a uno o ambos derechos
- Cumplimiento por las partes para asegurar la efectividad de los derechos (por ejemplo, requerimiento de registro)
- Otros derechos relacionados con valores o cuentas (incluyendo derechos subyacentes del cliente o derechos dados a terceros, como acuerdos de financiamiento) y si los derechos (de retención o venta) permanecen efectivos
- Pasos previos y mecánicas necesarias para dar efecto a uno o ambos derechos

13.6 Amenazas de Riesgo de Crédito

La tabla siguiente destaca las principales amenazas que podrían afectar a un Proveedor y/o Cliente.

Ilustración 13.6 Tabla de Riesgo de Crédito

Descripción del riesgo	Mitigación del riesgo
El cliente incumple un adelanto de línea de crédito debido a la incapacidad o falta de voluntad para cumplir con sus obligaciones financieras	Se deben establecer estrategias de riesgo crediticio (Marco de Apetito de Riesgo) para los Clientes, incluyendo estrategias de préstamo, calificaciones crediticias revisadas regularmente y límites para industrias / países Debe implementarse un monitoreo continuo de las exposiciones totales Suscripción prudente Gestión prudente de préstamos vencidos, cobranza y recuperación Debe existir una gestión adecuada del uso de las líneasde riesgo crediticio intradía (minimizando la exposición potencial por prestatario y en general, por ejemplo, en exposiciones grandes — préstamos que no excedan el porcentaje permitido de capital elegible según la jurisdicción) Capacidades tecnológicas para detener inmediatamente cualquier débito en dinero y entregas de valores en caso de un evento desencadenante
Pérdida crediticia durante el proceso de liquidación de una transacción que surge de la falta de recepción de dinero o activos después de haber entregado dinero o activos a la segunda parte	Evaluación crediticia de las contrapartes Implementación de límites con contrapartes para riesgo crediticio de contraparte y propósitos de liquidación
El cliente ya no puede obtener divisas extranjeras (FX) para atender su deuda externa (por ejemplo, como consecuencia de restricciones de convertibilidad)	Monitoreo continuo de países individuales Monitoreo continuo de Clientes y los lugares donde tienen negocios Terminación de nuevos negocios en caso de eventos desencadenantes o riesgos
El proveedor de servicios de valores y/o el cliente se ven afectados negativamente debido a un evento geopolítico global o regional o desarrollos en la economía de un país (por ejemplo, incumplimiento de deuda soberana)	Estrategias de riesgo crediticio (Marco de Apetito de Riesgo) a nivel institucional que establecen estrategias de préstamo y límites por industrias y países Monitoreo continuo de exposiciones totales por país / región Suscripción prudente y gestión estricta de límites por países Monitoreo continuo de países individuales Terminación de nuevos negocios en caso de eventos desencadenantes que lleven a riesgos fuera del apetito de riesgo

14. Riesgo de Liquidez

14.1 Introducción

Desde la perspectiva de un Proveedor de Servicios de Valores, el cumplimiento de las obligaciones de liquidación de su Cliente con los CSDs, bancos centrales y Subcustodios puede generar riesgo de liquidez cuando un Proveedor de Servicios de Valores no puede acceder a financiamiento. Un Proveedor de Servicios de Valores también puede experimentar desafíos de liquidez cuando el dinero que sale excede significativamente el dinero que entra (por ejemplo, transacciones importantes de RvP procesadas por encima de DvPs).

14.2 Definición

La liquidez se define como la capacidad de acceder a financiamiento, convertir activos en dinero de manera rápida y eficiente o renovar / emitir nueva deuda — especialmente durante periodos de estrés en el mercado — para cumplir con obligaciones a corto plazo.

14.3 Panorama del Riesgo de Crédito Intradía

Un Proveedor de Servicios de Valores está especialmente expuesto al riesgo de liquidez intradía. El riesgo de liquidez intradía, y su medición, ha sido un área de enfoque significativa por parte de la comunidad de Servicios de Valores — y sus reguladores — impulsado por el aumento significativo en los valores de exposición, así como por la complejidad de manejar las necesidades de liquidez intradía que surgen de actividades de liquidación en diferentes zonas horarias.

Además, con la tendencia hacia la reducción de los ciclos de liquidación de dos a un día hábil, los procesos de liquidez se están comprimiendo en un plazo más corto, lo que será particularmente desafiante para transacciones en múltiples divisas que incluyen un componente de FX.

Se han observado los siguientes cambios en los requerimientos de financiamiento:

- Cambios en el apetito de crédito (particularmente para crédito intradía) y reducción en el acceso a crédito barato, lo que ha incrementado los requerimientos de pre-financiamiento por parte de muchos participantes del mercado
- Cambios en los plazos de liquidación que también han aumentado la necesidad de financiar la noche previa a la fecha de liquidación (por ejemplo, T2S, T+1)

14.4 Amenazas al Riesgo de Liquidez

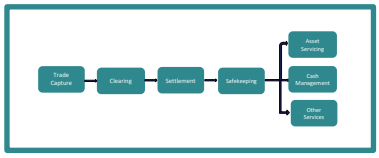
La siguiente tabla presenta las amenazas al riesgo de liquidez para los Proveedores de Servicios de Valores, así como para sus Clientes.

Ilustración 14.4 Tabla de Riesgo de Liquidez

Descripción del riesgo	Mitigación del riesgo
Servicios no mantenidos por el Proveedor de Servicios de Valores debido a falta de liquidez	Completar un proceso integral de evaluación interna de suficiencia de liquidez (ILAAP) Implementar un sistema de gestión de liquidez
Financiamiento por parte del Proveedor de Servicios de Valores no puede ser accedido a tiempo	Asegurar el acceso a una gestión precisa de la liquidez Garantizar el acceso a líneas de financiamiento del Banco Central cuando sea apropiado
Requisitos de colateral incrementados por el Proveedor de Servicios de Valores no reconocidos por el Cliente	Proveedor de Servicios de Valores y Cliente deben gestionar y monitorear conjuntamente los requerimientos de crédito intradía de forma continua
Financiamiento por parte del Cliente no puede ser accedido a tiempo	Implementar un sistema de gestión de liquidez por parte del Cliente para gestionar los flujos (asegurando que funcione también durante periodos de estrés de mercado) Seleccionar un Proveedor de Servicios de Valores financieramente sólido

15. Riesgo Sistémico

15.1 Introducción



La industria de Servicios de Valores es clave para el funcionamiento del sistema financiero en general. La cadena de valor de los Servicios de Valores implica también interconexiones e interdependencias entre múltiples Proveedores de Servicios de Valores y FMIs (Infraestructuras del Mercado Financiero). Este capítulo se centra en el riesgo de un colapso del sistema financiero en su totalidad — más que en la falla de una o más instituciones — y en las medidas que se pueden tomar para mitigar el impacto si este riesgo se materializa.

15.2 Definición

El Fondo Monetario Internacional (FMI), el Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés) y el Banco de Pagos Internacionales (BIS) definen formalmente el Riesgo Sistémico como el riesgo de una interrupción generalizada en la provisión de servicios financieros causada por una afectación total o parcial del sistema financiero y que puede causar graves consecuencias negativas para la economía real. Un sistema financiero se considera estable cuando las instituciones financieras son capaces de proporcionar a hogares, comunidades y empresas el financiamiento que necesitan para invertir, crecer y participar en una economía que funcione adecuadamente.

Entre estas instituciones financieras existen instituciones sistémicas, conocidas como Instituciones Financieras Sistémicamente Importantes (SIFIs). El FSB define una SIFI como una institución financiera cuyo deterioro o fracaso desordenado, debido a su tamaño, complejidad e interconexión sistémica, causaría una interrupción significativa en el sistema financiero más amplio y en la actividad económica. Dado que las FMIs están en el corazón del sistema financiero y juegan un papel principal para asegurar su estabilidad, las FMIs están de facto reguladas como entidades sistémicas.

15.3 Evaluación de la Importancia Sistémica

En la práctica, existen dos maneras de medir la importancia sistémica de una institución financiera o infraestructura dentro del sistema. El primer enfoque se basa en información sobre posiciones y exposiciones al riesgo, que típicamente es confidencial y solo se comparte externamente con los reguladores. El segundo enfoque se basa en datos públicos de mercado, como retornos de acciones, precios de opciones o swaps de incumplimiento crediticio, ya que se cree que reflejan toda la información sobre empresas que cotizan públicamente.

Aunque se han propuesto varias medidas prominentes a lo largo del tiempo (como el Faltante Esperado Marginal, el Faltante Esperado Sistémico, la Medida de Riesgo Sistémico, la Diferencia Condicional del Valor a Riesgo), pueden simplificarse en dos tipos diferentes:

- Medir la escasez esperada de capital de una institución condicionada a que ocurra una crisis financiera.
- Medir el Valor en Riesgo (Value-at-Risk) del sistema financiero condicionado a un evento específico que afecte a una empresa dada.

En otras palabras, todos los intentos de medir formalmente el riesgo sistémico, hasta ahora, han:

- Estado estructurados alrededor de las interacciones entre una empresa y el sistema del que forma parte.
- Distinguido entre el impacto de la empresa (en crisis) sobre el sistema y el impacto del sistema (en crisis) sobre la empresa.

15.4 Conceptos Clave del Riesgo Sistémico

Para un Proveedor de Servicios de Valores, además de las medidas cuantitativas, el riesgo sistémico también puede articularse en torno a varios conceptos clave. Estos incluyen:

- Riesgo sistémico entrante y saliente
- Contagio y amplificación
- Concentración e interconectividad

15.4.1 Riesgo sistémico entrante y saliente

Esta noción de direccionalidad es importante. De hecho, como parte del mismo sistema cuyo riesgo se está evaluando, un Proveedor de Servicios de Valores necesita distinguir entre el riesgo que el sistema le impone a él (entrante) y el riesgo que él impone al sistema (saliente). Esta distinción entre los riesgos asumidos (y por tanto la resiliencia al estrés sistémico) y los riesgos que se generan (y por tanto la contribución al estrés sistémico) es fundamental. Por ello también es necesario distinguir entre “estrés” y “vulnerabilidad”. Cuando el riesgo sistémico se materializa, se considera que la organización que es origen del problema está liberando estrés (saliente) que otros participantes del sector deben absorber (entrante), y lo harán si no sufren vulnerabilidades significativas.

15.4.2 Contagio y amplificación

El contagio y la amplificación son mecanismos que operan durante eventos que pueden tener un impacto sistémico. El contagio puede convertir un incidente aislado en un incidente generalizado, y la amplificación puede convertir un incidente menor en uno severo. Ambos mecanismos suelen estar presentes en eventos sistémicos, que impactan a un número significativo de participantes de Servicios de Valores de manera material.

El contagio puede adoptar varias formas: puede ser directo (por ejemplo, exposiciones bilaterales) o indirecto (por ejemplo, filtraciones de información). La amplificación también puede tomar diversas formas, como ciclos de retroalimentación negativa o pro-ciclicidad.

15.4.3 Concentración e interconectividad

Por su escala e interconectividad, un gran Proveedor de Servicios de Valores evita que otros participantes del mercado tengan que establecer más relaciones bilaterales de las que ya tienen. Concretamente, al aprovechar la cadena de valor de los Servicios de Valores para acceder a uno o varios mercados, los participantes en Servicios de Valores evitan la necesidad de establecer múltiples acuerdos bilaterales con otros participantes en diferentes mercados. Así, mientras un Proveedor de Servicios de Valores que soporta la cadena de valor concentra el riesgo de los participantes (quienes se vuelven más dependientes de él), simultáneamente reduce el nivel de interconectividad en el mercado. Por tanto, existe un equilibrio entre concentración e interconectividad.

15.5 Amenazas del Riesgo Sistémico

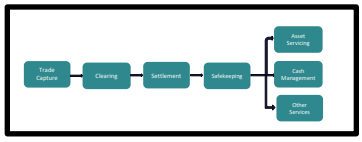
La siguiente tabla muestra los principales riesgos sistémicos y cómo pueden ser mitigados:

Ilustración 15.5 Tabla de Riesgo Sistémico

Descripción del riesgo	Mitigación del riesgo
Política no implementada en el Proveedor de Servicios de Valores para gestionar eventos de riesgo sistémico	Implementar una política interna adecuada para la alta dirección que cubra los factores clave de riesgo sistémico y el enfoque a seguir Asegurar que tanto los riesgos entrantes como salientes estén documentados y comprendidos Contar con un conjunto completo de herramientas de informes de gestión sobre riesgos sistémicos
Estallido de guerra en un país de relevancia sistémica	Identificar y evaluar países con alta probabilidad de riesgo de guerra Limitar la exposición a mercados, actividades y clientes de alto riesgo en caso de que un evento parezca inminente Terminar contratos o establecer acuerdos alternativos en caso de guerra
Caída del mercado	Monitorear y evaluar continuamente el estado de los mercados globales Asegurar que existan procesos para gestionar una caída del mercado
Fallo de una Institución Financiera de Importancia Sistémica (SIFI) o de una Infraestructura de Mercado Financiero (FMI)	Evaluar y documentar riesgos de concentración frente a otros participantes de Servicios de Valores y tener en marcha acuerdos para cambiar a otros participantes en caso de un problema o fallo fundamental Incluir capacitación para asegurar que el personal entienda sus responsabilidades, así como las acciones y procedimientos de escalamiento en caso de que ocurra un fallo

16. Riesgo Geopolítico y Geoeconómico

16.1 Introducción



El panorama geopolítico y geoeconómico para las instituciones financieras ha cambiado significativamente en los últimos años. Los eventos geopolíticos y los objetivos geoeconómicos pueden amenazar la estabilidad financiera y causar una gran interrupción tanto para organizaciones como para países. Pueden surgir múltiples riesgos cuando ocurren eventos geopolíticos y geoeconómicos que impactan a las firmas financieras, como sanciones, alianzas globales inciertas y cambiantes, así como salidas de capital. Por lo tanto, las organizaciones necesitan evaluar constantemente el clima geopolítico.

Este capítulo explora el cambiante panorama geopolítico y geoeconómico y destaca algunos de los eventos clave que han ocurrido en los últimos años y que han impactado a la industria de Servicios de Valores. También identifica los diferentes riesgos para un Proveedor de Servicios de Valores que podrían surgir en caso de un problema geopolítico y/o geoeconómico y qué mitigantes están disponibles para minimizar el impacto de estos riesgos.

16.2 Definición

La geopolítica se refiere al uso del poder político e influencia por parte de un país u organización para asegurar intereses nacionales. Por otro lado, la geoeconomía es el uso de actividades y recursos económicos para obtener beneficios económicos.

Por lo tanto, los riesgos geopolíticos y geoeconómicos consisten en la exposición a los efectos de:

- Inestabilidad política

  Esto incluye cambios de gobierno, disturbios políticos o conflictos

- Relaciones internacionales

  Incluye tensiones diplomáticas, conflictos militares o alianzas entre estados nación o bloques supranacionales

- Disturbios sociales

  Incluye protestas, huelgas o movimientos sociales.

- Políticas económicas

  Incluye políticas tales como relaciones financieras, restricciones comerciales, aranceles, sanciones o cambios en la política económica.

Por naturaleza, la industria de Servicios de Valores es global, involucrando la custodia de activos en una jurisdicción para apoyar a participantes en otras. Por ello, los Proveedores de Servicios de Valores son inherentemente sensibles al riesgo geopolítico y geoeconómico, que puede tener los siguientes efectos adversos:

- Interrupción del servicio

  La prestación del servicio a los Proveedores de Servicios de Valores se ve interrumpida

- Pérdida de valores, dinero o derechos sobre dinero

  Los Proveedores pueden sufrir pérdidas debido a conflictos de leyes, moratorias y decomiso de activos o contramedidas a sanciones

- Sanciones y penalizaciones

  Podrían estar sujetos a multas, sanciones y acuerdos voluntarios relacionados con incumplimientos de AML y violaciones de sanciones

- Fallas de seguridad

  Pérdida de activos físicos, datos y propiedad intelectual, y amenazas físicas al personal senior

- Riesgo reputacional

  Daño a la reputación de un Proveedor por hacer negocios con regímenes con antecedentes negativos en derechos humanos, medio ambiente y política, o por un fallo percibido o real en la protección de los activos de los inversores en caso de conflicto

16.3 El Panorama Geopolítico y Geoeconómico

El panorama geopolítico y geoeconómico cambia constantemente a medida que se transforman las alianzas entre países, surgen problemas políticos, comerciales y criminales, y surgen conflictos. Estos cambios no solo afectan a las personas o a los países, sino también a las instituciones financieras y su forma de operar. A continuación, se destacan algunos ejemplos de los riesgos geopolíticos y geoeconómicos vigentes al momento de redactar este informe.

16.3.1 Relaciones entre EE.UU. y China

Un riesgo geopolítico que ha ganado protagonismo en la última década es la relación entre dos de las mayores economías del mundo: EE.UU. y China. La relación entre estas dos naciones es tanto una oportunidad como una amenaza para los mercados financieros globales. El comercio entre estas dos potencias económicas, junto con la UE, ha impulsado un fuerte crecimiento económico. Sin embargo, también ha habido un notable impulso hacia una menor globalización y un desacople de la relación para aliviar la preocupación por la dependencia de mercados extranjeros con incertidumbre en los modelos de suministro continuos. La reciente imposición de aranceles ha demostrado que el riesgo geoeconómico puede causar disrupciones en el mercado. Si estas tensiones se intensifican, podría haber riesgos para el comercio global y cadenas de suministro interrumpidas, lo que impactaría los mercados financieros y causaría riesgos significativos. Los Proveedores de Servicios de Valores deben estar conscientes de estos riesgos y asegurarse de tener mitigantes robustos para enfrentarlos.

16.3.2 Guerra Rusia / Ucrania

La guerra entre Rusia y Ucrania ha causado una importante interrupción en la vida de las personas en la región geográfica. Sin embargo, también ha tenido un impacto significativo en la industria financiera y, específicamente, en la industria de Servicios de Valores. La introducción de sanciones por parte de los reguladores obligó a los Proveedores de Servicios a cumplir con estrictos regímenes de sanciones establecidos por múltiples países (como EE.UU., UE y Reino Unido). La industria ha enfrentado el desafío de normativas complejas y cambiantes sobre sanciones, y debe monitorear de cerca tanto negocios nuevos como existentes para garantizar el cumplimiento.

16.3.3 Tensiones en Oriente Medio

Las crecientes tensiones en Oriente Medio entre Israel y Gaza, y más recientemente la escalada con Líbano, están causando inestabilidad en la región. Aunque los impactos geopolíticos por ahora se limitan a la región inmediata, existe el riesgo de una mayor escalada si otros países se involucran directamente. Esto podría tener repercusiones más amplias, impactando las cadenas de suministro, la salud y aumentando la migración de personas que buscan escapar del conflicto.

16.3.4 Sostenibilidad

Un riesgo geopolítico y geoeconómico emergente es el de la sostenibilidad, con un enfoque cada vez mayor por parte de políticos y reguladores en el cambio climático, los recursos naturales y la seguridad energética. A medida que cambian y surgen nuevas alianzas estratégicas entre países, la necesidad de contar con medidas robustas para gestionar el riesgo potencial de estos cambios será cada vez más necesaria. Los Proveedores de Servicios de Valores ya están considerando medidas ESG (ambientales, sociales y de gobernanza) al evaluar nuevos negocios. El tema de la sostenibilidad y su impacto en los negocios probablemente crecerá conforme evolucionen las políticas y regulaciones.

ESTUDIO DE CASO: Geoeconomía y la pandemia de Covid-19

La industria transfronteriza de Servicios de Valores —y la infraestructura que la soporta— nació en la década de 1970 y creció exponencialmente con la desregulación y la globalización desde los años 80. El retroceso de la globalización —por parte de estados nación económicamente significativos— desafía por lo tanto la base sobre la cual se construye esta industria.

El compromiso con la desregulación y la globalización fue socavado por la crisis financiera y, más recientemente, por la pandemia de Covid-19. Cuando esta última golpeó a principios de 2020, causó interrupciones significativas en las economías y mercados financieros. Estas interrupciones —como problemas de suministro y distribución, preocupaciones sobre la productividad, además de una grave emergencia sanitaria— llevaron a intervenciones gubernamentales en muchos mercados con cambios en las políticas fiscal y monetaria. La industria de Servicios de Valores, como parte del sistema financiero, también fue impactada con niveles significativos de inestabilidad y volatilidad. Los proveedores de Servicios de Valores tuvieron que manejar altos volúmenes de operaciones mientras que los empleados debían trabajar de forma remota de manera repentina.

Aunque los mercados se recuperaron relativamente rápido y mostraron resiliencia en el manejo de la pandemia, el impacto de un evento geoeconómico tan inesperado —y la necesidad de procesos amplios e integrales de gestión de riesgos— nunca ha sido más claro.

16.4 Amenazas de Riesgo Geopolítico y Geoeconómico

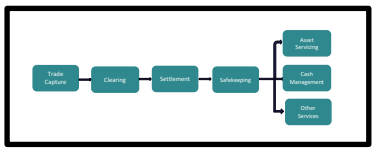
La tabla a continuación resalta los posibles riesgos geopolíticos y geoeconómicos que podrían ocurrir, así como las formas en que estos riesgos pueden ser mitigados.

Ilustración 16.4: Tabla de Riesgos Geopolíticos y Geoeconómicos

Descripción del riesgo	Mitigación del riesgo
Falta de una política definida para el enfoque del riesgo geopolítico	▪ Asegurar que las evaluaciones de riesgo de mercado aborden el riesgo político de manera amplia y no se limiten exclusivamente a riesgos legales
No se identifican nuevos riesgos geopolíticos y geoeconómicos emergentes	▪ Asignar una responsabilidad clara de gestión para monitorear riesgos geopolíticos y geoeconómicos emergentes ▪ Evaluar continuamente las redes de Servicios de Valores para identificar riesgos políticos
Fallo en la evaluación y monitoreo de riesgos geopolíticos existentes	▪ Garantizar que los Proveedores de Servicios de Valores y los Clientes tengan acceso adecuado a inteligencia de seguridad y política ▪ Establecer planes de mitigación y contingencia para abordar amenazas emergentes, incluyendo, pero no limitado a, planes de salida ▪ Asegurar que los contratos con clientes distribuyan apropiadamente el riesgo entre el proveedor y el cliente para pérdidas directas e indirectas ▪ Considerar la comunicación rápida y el intercambio de información con pares de la industria, incluyendo células de crisis a nivel sectorial para tratar conflictos y otros eventos geopolíticos
Incumplimiento de cambios regulatorios requeridos como resultado de un riesgo geopolítico o geoeconómico	▪ Asegurar que los acuerdos contractuales con clientes faciliten el cumplimiento basado en riesgo con regímenes de sanciones extranjeras donde exista un nexo jurisdiccional o donde sanciones secundarias sean previsibles ▪ Asignar una responsabilidad clara de gestión para monitorear programas de sanciones potencialmente relevantes y la evaluación asociada (Nota: esto es especialmente importante cuando el cumplimiento de sanciones está subcontratado a funciones del grupo) ▪ Garantizar que las funciones de cumplimiento estén adecuadamente capacitadas en productos de Servicios de Valores

17. Riesgos de Activos Digitales

17.1 Introducción



Los riesgos descritos en los capítulos anteriores de este informe se han centrado en activos mantenidos en un modelo tradicional de Servicios de Valores. Sin embargo, en los últimos cinco años, la industria financiera ha visto la creación y crecimiento de activos digitales, que pueden utilizar diferentes modelos operativos y plataformas tecnológicas.

En este capítulo, el enfoque está en activos digitales que son mantenidos por Clientes y utilizan un proveedor de servicios. No considera la opción de custodia propia, ni analiza activos digitales que normalmente no se mantendrían en un entorno de Servicios de Valores, tales como tokens de vino o tokens no fungibles (NFTs).

El capítulo aborda los principios clave que deben considerarse para mitigar riesgos al prestar servicios sobre activos digitales. Define los dos tipos clave de activos digitales — activos tokenizados y activos digitales nativos — y distingue los riesgos principales de cada uno. Se debe reconocer, sin embargo, que el mercado de activos digitales sigue evolucionando y, por lo tanto, continuará cambiando y desarrollándose. Habrá por ende un requerimiento tanto para Clientes como para Proveedores de Servicios de Valores de evaluar activamente estos desarrollos continuos para mitigar riesgos a medida que cambien.

17.2 Definición

Un activo digital puede definirse, en términos generales, como cualquier activo que se crea y mantiene en forma digital. Desde la perspectiva de la industria de Servicios de Valores, los activos digitales comprenden dos tipos clave:

- Activos Tokenizados
  Los activos tokenizados se crean para representar valores tradicionales que ya se mantienen en un entorno existente de Servicios de Valores. Un activo tokenizado a veces se denomina "gemelo digital" porque es una representación digital de un activo que existe, en forma inmovilizada. Como los activos tokenizados tienen un equivalente real subyacente, no se crean activos nuevos

- Activos Digitales Nativos
  Los activos digitales nativos — a veces conocidos como activos nativos on-chain, activos virtuales o criptoactivos — son activos puramente digitales que solo existen en una plataforma digital. Los activos digitales nativos pueden ser similares a activos que existen en el mundo real o pueden ser nuevos tipos de activos (como criptomonedas y NFTs)

17.3 Panorama de los Activos Digitales

En los últimos diez años, ha habido un cambio lento pero significativo en el panorama financiero. Los modelos tradicionales centralizados para transacciones de dinero y valores, con una fuerte supervisión regulatoria y controles, han sido acompañados por la aparición de activos digitales.

Como ocurre con cualquier novedad, inicialmente hubo preocupaciones sobre los riesgos involucrados en invertir en activos digitales. Sin embargo, más recientemente, esto ha cambiado ya que los reguladores han comprendido este nuevo mundo y comenzaron a implementar nuevas regulaciones, o modificaciones a las existentes, para apoyar su uso. Impulsada por la introducción de regulaciones y altos retornos, la adopción de activos digitales — particularmente la inversión en criptomonedas — ha sido significativa, y se anticipa que el mercado de activos digitales continuará creciendo en el futuro.

17.4 Servicio de Activos Digitales

Al igual que con los activos tradicionales, un Cliente que desee invertir en activos digitales requerirá un proveedor de servicios para mantener y salvaguardar sus activos. Si bien puede ser un Proveedor tradicional de Servicios de Valores quien ofrece este servicio, también existen nuevos participantes — conocidos como VASPs (Proveedores de Servicios de Activos Virtuales).

El servicio de activos digitales dependerá del tipo de activo digital, así como del tipo de modelo operativo y plataforma tecnológica adoptada. A continuación, se destacan las áreas clave a considerar al prestar servicios sobre activos digitales.

17.4.1 Plataforma Tecnológica

Un modelo tradicional de custodia, como se describe en los capítulos anteriores, utiliza un modelo tecnológico que es una plataforma tecnológica privada y centralizada. Los activos tokenizados pueden ser soportados utilizando este modelo tradicional de custodia.

Sin embargo, la mayoría de los activos digitales utilizan diferentes plataformas tecnológicas que aprovechan una base de datos descentralizada y utilizan un libro mayor distribuido — conocido como Tecnología de Libro Mayor Distribuido (DLT). Un DLT es un sistema digital que registra, valida y actualiza transacciones de forma inmutable mientras permite acceso simultáneo a la red desde múltiples ubicaciones. La tecnología permite STP y transparencia entre diferentes organizaciones en tiempo real.

17.4.2 Modelo Operativo

Mientras que los activos tokenizados pueden ser mantenidos por un Proveedor de Servicios de Valores utilizando el modelo operativo tradicional descrito en capítulos anteriores, la mayoría de los activos tokenizados y todos los activos digitales nativos utilizan un modelo diferente conocido como Custodia de Activos Digitales (DAC). Según el informe de Global Digital Finance (GDF), ISSA y Deloitte titulado "Digital Asset Custody Deciphered": "Algunas actividades requeridas para DAC se reconocen en Servicios de Valores tradicionales como roles realizados por un Proveedor de Servicios de Valores. Sin embargo, se reconoce ampliamente que — en relación con activos digitales — pueden ser necesarios nuevos modelos operativos, capacidades y controles para prestar estos servicios efectivamente."

En resumen, los modelos operativos para activos digitales comprenden:

- En lugar de mantener el activo en una cuenta ómnibus o segregada tradicional con un Proveedor de Servicios de Valores, los activos digitales se mantienen en "billeteras" dentro del sistema DLT y el movimiento de los activos digitales de una parte a otra depende de la autorización usando las claves privadas de la billetera del activo.
- Un protocolo de transacción — conocido como contrato inteligente — controla directa y automáticamente la transferencia de activos digitales entre compradores y vendedores basada en condiciones acordadas.
- Los activos digitales y los contratos inteligentes permiten liquidación atómica comprometida, que habilita que la liquidación se acelere o retrase respecto a los marcos temporales acordados por el mercado. El proceso de liquidación para activos digitales es, por lo tanto, flexible y puede ocurrir en cualquier momento del día con liquidación final.

17.4.3 Seguridad de la Información

Se deben implementar controles específicos de acceso físico y de sistema, y controles de segregación para salvaguardar las claves privadas, que deben ser altamente seguros para garantizar la seguridad de la información y limitar las vulnerabilidades ante amenazas como robo o mal uso. Los métodos de seguridad incluyen almacenamiento "caliente" (donde la clave privada está en una ubicación conectada a internet — es decir, menos seguro contra ciberataques pero ventajoso para la rapidez en la finalización de transacciones) o almacenamiento "frío" (donde las claves privadas no están conectadas a internet, por lo que es más seguro aunque más lento para completar el procesamiento de transacciones).

17.4.4 Marcos Regulatorios y Legales

Los marcos regulatorios y legales en torno a los activos digitales aún están evolucionando. Mientras algunas jurisdicciones han creado un marco regulatorio, en muchos mercados esto todavía no existe. Además, las regulaciones se han implementado de diferentes maneras, con algunos mercados creando regulaciones específicas para activos digitales y otros adaptando sus marcos financieros actuales para incorporar estos activos. Cuando se han implementado nuevas regulaciones, tienden a ser únicas para la jurisdicción que tiene supervisión, lo que genera desafíos cuando un Cliente desea invertir en activos digitales en múltiples mercados.

Es por ello crítico que tanto Proveedores de Servicios de Valores consideren aspectos regulatorios tales como:

- Determinar cómo se puede asegurar el título legal y la transferencia de este para DAC (por ejemplo, para valores tradicionales el título legal puede estar registrado a nombre del Proveedor de Servicios de Valores en representación del Cliente, mientras que para activos digitales el Proveedor puede considerarse que tiene la posesión, mientras que el título permanece directamente con el Cliente)
- Cuando ya existe un marco regulatorio para activos digitales, que las regulaciones reflejen que un Proveedor de Servicios de Valores que tiene control sobre claves privadas es conceptualmente similar al modelo tradicional de custodia
- Que las regulaciones de seguridad de activos de la jurisdicción consideren el activo digital como un instrumento financiero (y por lo tanto cubierto por regulaciones de seguridad de activos) o no
- Entender la confluencia entre el Cliente, el Proveedor de Servicios de Valores y la “ubicación” del activo digital y la incertidumbre regulatoria cuando estos difieren

Respecto a plataformas tecnológicas, los reguladores consideran que el estatus regulatorio de un activo o actividad no se ve afectado por el uso de tecnologías alternativas, como DLT, siempre que esto no cambie las características de riesgo del activo o el título legal del activo subyacente.

17.5 Riesgos de Activos Digitales

Para los activos tokenizados, los riesgos son predominantemente los mismos o similares a los riesgos asociados con un modelo tradicional de Servicios de Valores. La principal diferencia y riesgos están ligados a cuando se utiliza un modelo tecnológico diferente. Sin embargo, para los activos digitales nativos existen diferencias clave en torno al modelo operativo, la custodia de los activos, la seguridad así como la confidencialidad. Esto resulta en riesgos diferentes y/o adicionales que deben ser evaluados y mitigados cuando se considera un servicio DAC.

La tabla siguiente proporciona un resumen de los riesgos clave de activos digitales que deben revisar los Proveedores de Servicios de Valores y Clientes cuando consideren activos digitales. Estos riesgos deben considerarse junto con los riesgos descritos en capítulos previos de este informe.

Dada la relativa novedad de los activos digitales, se debe tener en cuenta que la tecnología, los marcos operativos y regulatorios aún están evolucionando y, por lo tanto, los riesgos probablemente cambiarán y podrán emerger riesgos adicionales.

Ilustración 17.5 Tabla de Riesgos de Activos Digitales

Descripción del riesgo	Mitigación del riesgo
Falta de un marco regulatorio para los activos digitales	▪ Asegurar que cualquier jurisdicción donde un Proveedor de Servicios de Valores ofrezca un servicio de activos digitales reconozca la estructura y haya implementado un marco regulatorio ▪ Implementar un monitoreo activo en el Proveedor de Servicios de Valores sobre cambios en regulaciones y leyes relacionadas con activos digitales
Falta de protección de los activos digitales	▪ Asegurar que las regulaciones de seguridad de activos de la jurisdicción consideren el activo digital como un instrumento financiero ▪ Validar que las regulaciones y leyes que rigen la protección de activos digitales estén vigentes en la jurisdicción donde se ofrece el servicio ▪ Garantizar que el Proveedor de Servicios de Valores tenga control sobre las llaves privadas y no un tercero

Descripción del riesgo	Mitigación del riesgo
Diligencia debida insuficiente o incompleta por parte del Proveedor de Servicios de Valores	▪ Evaluar al Proveedor de Servicios de Valores para asegurar que posea las licencias apropiadas para proveer un servicio de Custodia de Activos Digitales (DAC)
Falta de controles operativos o supervisión	▪ Confirmar que los mecanismos de transacción de valores adopten controles de monitoreo para detectar información inusual, sospechosa o sancionada relacionada con activos digitales. ▪ Implementar monitoreo de "Conoce tu transacción" (KYT) y "Conoce tu activo" (KYA) que permita un análisis rápido sobre la validez de las transacciones y la historia del activo.
Información insuficiente y/o seguridad inadecuada de los datos	▪ Implementar una solución de tecnología de registro distribuido (DLT) con características especializadas de seguridad que cubran las llaves de seguridad y contratos inteligentes.
Falta de una solución robusta de tecnología de registro distribuido (DLT)	▪ Realizar una revisión detallada de la tecnología DLT para asegurar que la plataforma cumple con las necesidades del negocio y los requerimientos regulatorios ▪ Implementar la validación de la plataforma durante las pruebas y de manera continua
Proveedor tercero	▪ Asegurar que se realice una debida diligencia detallada de los proveedores terceros, particularmente en lo que respecta a los marcos regulatorios y legales aplicables, la seguridad de los sistemas y la protección de activos

Apéndices

Sección 4: Apéndices

Términos y Definiciones Clave de Alto Nivel

La siguiente tabla proporciona una lista de los términos clave y definiciones utilizados en este informe.

Término	Definición
Activo	También conocido como activo financiero o instrumento financiero, es un activo — usualmente no físico— que tiene valor como reclamo contractual o derecho de propiedad
Ciclo de vida del activo	Un ciclo que refleja las diferentes etapas de un activo, desde su creación, compra, uso y mantenimiento hasta su disposición final
Participante del ciclo de vida del activo	Organizaciones o individuos que proveen o utilizan cualquiera de los componentes descritos en el ciclo de vida de un activo
Gestor de activos	Una organización que actúa en nombre de un inversionista. Puede ser un Gestor de Inversiones (que se enfoca principalmente en inversiones individuales) o un Gestor de Fondos (que trabaja con fondos compuestos por múltiples activos, a menudo adaptados a un sector de mercado específico)
Servicios de activos	La función de dar servicio a los activos de un cliente típicamente incluye: ▪ Eventos corporativos (por ejemplo, aumentos de capital, divisiones de acciones) ▪ Voto por poder ▪ Acciones colectivas ▪ Procesamiento de distribuciones (por ejemplo, dividendos, intereses / redenciones) ▪ Servicios fiscales (por ejemplo, alivio de retención en la fuente o recuperación fiscal)
Agente intermediario (Broker Dealer)	Parte que negocia transacciones financieras en nombre de sus clientes (Broker) o en su propio nombre (Dealer)
Gestión de dinero	La función de proporcionar facilidades de cuentas de dinero para apoyar el movimiento de valores y el dinero relacionado con la prestación de servicios de activos se conoce como gestión de dinero. Estos servicios pueden incluir facilidades de crédito para apoyar la liquidez intradía y capacidades de divisas extranjeras (FX)
Banco Central 4.1-mini	Proveedor de dinero del Banco Central para la liquidación en el Depósito Centralizado de Valores (CSD)

Término	Definición
Contraparte Central (CCP)	Una entidad que actúa como contraparte central para todos los miembros compensadores, con el CCP convirtiéndose en comprador para cada vendedor y vendedor para cada comprador
Depósito Centralizado de Valores (CSD)	Una infraestructura de mercado que mantiene valores y permite que las transacciones de valores se procesen mediante anotaciones electrónicas en cuenta. El CSD típicamente opera un sistema de liquidación de valores y proporciona mantenimiento centralizado de cuentas de valores y/o funciones notariales en un mercado específico
Compensación (Clearing)	Esta función es un paso opcional, entre la negociación y la liquidación, donde ciertas transacciones se procesan conjuntamente, usualmente en un lugar de compensación
Cliente	Un Gestor de Activos o Inversionista que nombra a un Proveedor de Ejecución de Negociaciones y/o Proveedor de Servicios de Valores es conocido como Cliente del Proveedor de Servicios de Valores
Custodio	Una institución financiera autorizada y supervisada por el regulador prudencial de servicios financieros o bancario para proveer Servicios de Valores
Depositario / Banco Depositaria	Una organización designada por ciertos tipos de fondos domiciliados en la UE para supervisar las inversiones realizadas en el fondo
Infraestructura de Mercado Financiero (FMI)	Un proveedor u operador que compensa o liquida valores entre participantes de Servicios de Valores
Administrador de Fondos	Una organización responsable de verificar independientemente los activos de un fondo y valuar el fondo en nombre del Cliente
Participantes de Servicios de Fondos	Las partes involucradas en proveer servicios a un fondo, incluyendo un Administrador de Fondos, Depositario / Banco Depositario y Agente de Transferencia
Custodio Global	Un Custodio que provee servicios respecto a valores negociados en múltiples mercados o jurisdicciones
Inversionista	Un individuo u organización que invierte en activos. Un Inversionista puede ser el dueño real de los activos o un intermediario que los mantiene en nombre de otros inversionistas
Emisor	El creador de un activo es conocido como Emisor
Registrador	Parte responsable de mantener un registro de los inversionistas y la cantidad de valores poseídos para un fondo, bono o emisión de acciones, y garantizar que la cantidad de valores en circulación sea igual a la cantidad emitida
Regulador	La organización que gobierna la operación del mercado financiero para la jurisdicción de su responsabilidad
Custodia	La función de mantener los valores propiedad de un Cliente se denomina Custodia o Safekeeping

Término	Definición
Valores o Broker Principal (Prime Broker)	Una parte que ofrece servicios a fondos de cobertura y otros Clientes profesionales, incluyendo préstamo de valores, ejecución apalancada de operaciones y gestión de dinero
Servicios de Valores	Una combinación de servicios financieros que consiste en la captura de operaciones, compensación y liquidación, así como la custodia y administración de activos en nombre de los Clientes (también a veces denominados servicios posteriores a la operación).
Proveedor de Servicios de Valores	Un término general para los participantes en Servicios de Valores, tales como Custodios, Infraestructuras de Mercado Financiero (FMI) y otros participantes que proveen Servicios de Valores a un Cliente
Liquidación (Settlement)	La función de liquidación se refiere al proceso de transferencia de la propiedad de valores entre contrapartes. La liquidación usualmente se realiza contra dinero, conocido como Entrega contra Pago (Delivery versus Payment, DVP) o Recepción contra Pago (Receipt versus Payment, RVP). Sin embargo, la liquidación también puede ser sin pago
Bolsa de Valores	Un lugar donde los Broker Dealers pueden comprar y vender valores, tales como acciones, bonos y otros instrumentos financieros
Subcustodio	Un Custodio que provee servicios respecto a valores negociados en un mercado o jurisdicción particular
Proveedor Tercero (Third-Party Provider)	Una empresa especializada que ofrece servicios externos a los Proveedores de Servicios de Valores
Captura de Operaciones (Trade Capture)	La función de captura de operaciones o instrucciones es el proceso mediante el cual el Proveedor de Servicios de Valores recibe una instrucción de su Cliente (o participante en ejecución de operaciones) para “liquidar la operación” en su nombre
Agente de Transferencia (Transfer Agent)	Una parte designada por un fondo o el Emisor de un activo para emitir y cancelar unidades de fondos y valores en forma física o desmaterializada, así como reflejar cambios en la propiedad de un activo

Participantes del Grupo de Trabajo

ISSA desea agradecer a las siguientes organizaciones miembros por su participación en este proyecto:

- ABN AMRO
- BNP Paribas S.A
- BNY
- Deutsche WertpapierService Bank AG
- Digital Asset Holding, LLC
- Euroclear
- HSBC Holding Plc
- Intesa Sanpaolo Group / Privredna Banka
- JP Morgan Chase & Co.
- Rand Merchant Bank – Custody Services
- SEB Group
- Standard Chartered Bank
- The Depository Trust & Clearing Corporation