Racional SpA

Manual de Gestión de Riesgos y Control Interno

6 de julio de 2026

Antecedentes Generales

Racional SpA (en adelante, la "Sociedad" o "Racional"), es una sociedad por acciones, que se constituyó mediante escritura pública de fecha 28 de diciembre de 2018 en la notaría de don René Benavente Cash, inscrita a fojas 478, N°249, en el Registro de Comercio del Conservador de Bienes Raíces de Santiago, correspondiente al año 2019, y publicada en el Diario Oficial de fecha 7 de enero del mismo año.

La Sociedad se encuentra inscrita en el Registro de Prestadores de Servicios Financieros que lleva la Comisión para el Mercado Financiero (en adelante, la "CMF"), bajo el N°17.

Objetivo

El objeto de este Manual de Gestión de Riesgos y Control Interno (en adelante, el "Manual") es definir los mecanismos necesarios para la identificación y cuantificación de los riesgos relevantes, a través de políticas de gestión de riesgos y procedimientos de control interno en las actividades de la Sociedad. En el caso de identificar riesgos significativos en el desarrollo de las actividades, se establecerán estrategias específicas de mitigación y planes de contingencia.

Este documento cumple con las siguientes funciones:

- Identificar las áreas potenciales de riesgo y los responsables de los procesos críticos;
- Proporcionar la base metodológica para la realización de análisis constantes con el fin de generar herramientas que permitan medir, evaluar o identificar nuevos riesgos;
- Permitir la reducción de la ocurrencia de eventos de riesgo; y
- Establecer las directrices para mantener informada de manera constante a la alta administración de la Sociedad respecto de los riesgos.

Las disposiciones del presente Manual serán aplicables, sin excepción, a la Sociedad en la prestación de sus servicios, sus colaboradores, directores y partícipes.

Alcance

El presente documento tiene como propósito conformar el marco formal para la administración y supervisión de la gestión de riesgos, basado en las mejores prácticas de administración y control interno, sin perjuicio de las normas impartidas por la CMF.

Referencias

- Ley No. 18.045 sobre mercado de valores.
- Ley No. 18.046 sobre sociedades anónimas.
- Ley No. 19.913 sobre prevención de lavado de activos.
- Ley No. 19.628 sobre protección de los datos personales.
- Ley N°21.663, Ley Marco de Ciberseguridad, en lo que resulte aplicable a la Sociedad.
- Ley N°21.521 que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros (“Ley Fintec”).
- Norma de Carácter General N°502 de la Comisión para el Mercado Financiero, modificada por las Normas de Carácter General N°524 y N°559, o aquella normativa que la modifique o reemplace (la “NCG 502”). Las referencias de este Manual y de los demás documentos del marco normativo interno a la NCG 502 se entienden hechas a su texto vigente.
- Norma de Carácter General N°530 de la CMF, sobre el Manual de Sistema de Información Fintec (MSI Fintec) y los archivos FINTEC.
- Ley N°21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, conforme a su entrada en vigencia.
- Normativa dictada por la Unidad de Análisis Financiero, en aquellos servicios respecto de los cuales Racional tenga la calidad de sujeto obligado.
- Política de Contratación y Remuneración de la Sociedad, que desarrolla la Sección IV.D.1 letras f) y g) de la NCG 502, sobre contratación de personal idóneo y remuneración que previene conflictos de interés. Dicha Política forma parte integrante del sistema de gestión de riesgos y control interno y debe interpretarse en forma armónica con el presente Manual.

Definiciones.

“Enrutamiento de Órdenes” es el servicio de canalización de órdenes recibidas de terceros para la compra o venta de valores de oferta pública o instrumentos financieros a sistemas alternativos de transacción, intermediarios de valores o corredores de bolsas de productos.

“Conflicto de Interés” significa cualquier hecho que pueda afectar o influir en la independencia u objetividad en el actuar de Racional y/o las Personas Obligadas que pueda interferir en sus decisiones u obligaciones para con los Usuarios.

“Instrumentos Financieros” significa todo título, contrato, documento o bien incorporal, nacional o extranjero, diseñado, empleado o estructurado con la finalidad de generar rentas monetarias, o dar cuenta de una deuda insoluta, incluyendo valores de oferta pública inscritos o no en el Registro de Valores y de Valores Extranjeros de la Ley N°18.045, divisas, contratos derivados, contratos por diferencia, facturas y criptoactivos, entre otros, independiente de si su soporte es físico o electrónico.

“Personas Obligadas” significa Racional, sus directores, gerentes, administradores, colaboradores, y su personal a cargo del algoritmo a través del cual se realiza el servicio de Enrutamiento de Órdenes a nombre de Racional.

“Registro” significa el Registro de Prestadores de Servicios Financieros que lleva la Comisión para el Mercado Financiero.

“Usuario” o “Cliente” significa la persona natural o jurídica a la cual Racional presta servicios de Asesoría de Inversión y/o Enrutamiento de Órdenes.

“Directorio” es el órgano que aprueba las políticas, los manuales, el plan anual de gestión de riesgos, el apetito de riesgo y los cambios materiales; supervisa su cumplimiento y deja constancia de sus acuerdos en acta.

“Gerencia General” es el órgano que implementa los acuerdos del Directorio, asigna los recursos necesarios y asegura la operación diaria de la Sociedad.

“ECCI” es el Encargado de Cumplimiento y Control Interno, quien ejerce la función de gestión de riesgos y cumplimiento, monitorea los controles y reporta directamente al Directorio.

“Responsable de Tecnología y Operaciones” corresponde al Head of Engineering o a quien formalmente se designe, y ejecuta los controles tecnológicos y operativos. Las referencias contenidas en este Manual a “Gerente de Tecnología”, “Gerencia de Tecnología”, “Head of Engineering”, “encargado de infraestructura” o “Tecnología y Operaciones” se entienden efectuadas a esta misma función.

“Finanzas” es el área responsable del control del patrimonio ajustado, de las garantías y del reporte FINTEC02.

“Revisor Independiente” es la persona distinta del ejecutor del control o del reporte, encargada de verificar su correcta ejecución.

“Orden” significa la instrucción de compra o venta de valores de oferta pública o instrumentos financieros impartida por un Cliente y recibida por Racional para su transmisión a un Corredor Asociado.

“Corredor Asociado” significa el intermediario de valores, corredor de bolsa, corredor de bolsa de productos, operador regulado o sistema alternativo de transacción, en Chile o en el extranjero, al cual Racional transmite las Órdenes de sus Clientes para su ejecución.

“Evidencia” significa los registros íntegros, fechados y trazables que acrediten la ejecución de una actividad o control, incluyendo actas, aprobaciones, tickets, logs, reportes, conciliaciones, resultados de pruebas, respaldos de comunicaciones y planes de remediación. Toda la Evidencia se conserva en el repositorio designado por un plazo mínimo de cinco años contados desde su generación, o por el mayor plazo que exija la normativa aplicable, y queda a disposición de la CMF cuando ésta lo requiera. Este es el plazo único de conservación aplicable a todo el marco normativo interno de la Sociedad, y los demás documentos que lo integran se remiten a él.

Aspectos Organizacionales de la Gestión de Riesgos y Control Interno.

Con el objeto de realizar una eficaz definición, administración y control de los riesgos identificados derivados del desarrollo de las actividades de la Sociedad, se ha diseñado la estructura organizacional que a continuación se detalla.

Directorio.

Dentro de sus responsabilidades están, revisar, aprobar y, cuando corresponda, actualizar las políticas y los procedimientos de gestión de riesgos y control interno para la Sociedad, al menos una vez al año o con la frecuencia necesaria en caso de que se produzcan cambios significativos en las políticas y los procedimientos establecidos, dejando evidencia de ello. Para estos efectos, deberá dar cumplimiento a los principios y elementos de gestión de riesgos que se señalan a continuación:

a) Establecer la misión, visión y objetivos estratégicos, teniendo en consideración las responsabilidades que el marco regulatorio vigente establece para la Sociedad.

b) Aprobar políticas de gestión de riesgos que sean coherentes con los objetivos estratégicos y el marco regulatorio.

c) Revisar las políticas, al menos anualmente, y actualizarlas en caso de que se produzcan cambios significativos tales como introducción de nuevos productos o servicios, o cambios en la regulación aplicable a la Sociedad.

d) Evaluar periódicamente la suficiencia de recursos de las instancias encargadas de la gestión de riesgos.

e) Establecer una estructura organizacional adecuada para la gestión de riesgos de la Sociedad.

f) Establecer políticas de contratación de empleados que aseguren que Racional disponga de personal con la debida experiencia para desempeñar sus funciones, y velar porque se cuente con el recurso humano calificado para la gestión de riesgos.

g) Implementar políticas de remuneración y compensación para quienes presten servicios para la Sociedad, las cuales considerarán al menos la forma o mecanismo mediante el que se prevendrá y verificará que con las remuneraciones y compensaciones no se produzcan o exacerben conflictos de intereses por parte de quienes gestionan recursos de Racional y de quienes asesoran o mantienen relaciones comerciales con Clientes.

h) El Directorio deberá evaluar la pertinencia de conformar un Comité de Gestión de Riesgos o una instancia similar que le permita tratar y monitorear aspectos relevantes de los negocios, referidos a materias tales como conflictos de intereses, seguridad de la información, entre otros. Los fundamentos considerados por el Directorio para evaluar la conformación de comités o instancias similares deberán estar debidamente documentados.

i) Asegurar que las actas o documentación equivalente den cuenta de las principales temáticas tratadas en las sesiones del Directorio y los comités -en caso de que se creen-, así como las políticas y los procedimientos mencionados previamente. Todo el material que se elabore o presente al Directorio o los comités -en caso de que se creen-, deberá estar debidamente documentado y archivado de conformidad a las normas generales aplicables en la materia, y estar permanentemente disponible para su examen a solicitud de la CMF.

Encargado de Cumplimiento y Control Interno.

El encargado de cumplimiento y control interno (en adelante, el "ECCI") será designado y removido por el Directorio, al cual reportará funcional y directamente. Deberá contar con acceso irrestricto a la información necesaria, con acceso autónomo al Directorio —pudiendo requerir ser oído sin la presencia de la Gerencia General— y con recursos suficientes. Conforme a la tabla de proporcionalidad de la Sección IV de la NCG 502, y atendida la clasificación de la Sociedad, la función de gestión de riesgos puede ser ejercida de manera no especializada por un integrante de la alta administración, con reporte directo al Directorio. A la fecha de este Manual esa es la situación de la Sociedad: quien ejerce como ECCI desempeña simultáneamente un cargo ejecutivo en el área de Tecnología. Dicha concurrencia está expresamente permitida por la norma en la medida que existan controles compensatorios, los que se encuentran regulados en el Control 5 y en el Anexo C de la Política de Contratación de Personal y de Remuneraciones, a los que este Manual se remite y que forman parte integrante de él. El ECCI ejercerá la función de gestión de riesgos y cumplimiento, monitoreará la eficacia de los controles y actuará como contraparte de la CMF en estas materias, sin reemplazar a los responsables de primera línea en la ejecución de sus controles.

El ECCI tiene las siguientes funciones:

1. Es el responsable de asegurar la elaboración de las políticas y procedimientos por parte de las áreas generadoras de riesgos, y de su exactitud, integridad y actualización;
2. Monitorear el cumplimiento de las políticas y procedimientos de gestión de riesgos y control interno, permanentemente, y de los controles definidos en dichas políticas y procedimientos;
3. Adoptar medidas que permitan garantizar el debido cumplimiento de las disposiciones contenidas en las leyes y normativas, y en lo específico, en lo relativo al debido manejo de materias como, por ejemplo, actividades prohibidas, conflictos de intereses, eventualidad de fraude, y otros delitos o infracciones.
4. Emitir un informe, al menos con una periodicidad semestral, al Directorio, en que se documenten las instancias de incumplimientos detectados, causas que lo originaron, medidas adoptadas y efectividad de dichas medidas;
5. Proponer cambios en las políticas y en los procedimientos de gestión de riesgos según corresponda;
6. Elaborar un plan anual que se refiera a la naturaleza, alcance y oportunidad de las actividades que la función de gestión de riesgos desarrollará. El plan será aprobado por el Directorio y será actualizado según corresponda, conforme lo indica la NCG 502.

Asesoría Legal Externa.

Racional cuenta con asesoría legal externa que dentro de sus responsabilidades está el asesorar al ECCI y a la Sociedad en general, en temas relacionados con la gestión y mitigación del riesgo jurídico, así como en la interpretación de nuevas exigencias normativas que apliquen a Racional.

Dentro de sus responsabilidades se encuentra el exigir y velar por el cumplimiento de la normativa vigente que rige a la Sociedad, además de colaborar en la identificación de riesgos, cambios regulatorios y determinar medidas preventivas y correctivas para un correcto control en la prestación de los servi-

cios de la Sociedad.

Segregación de Funciones

Con el objeto de resguardar una adecuada gestión de riesgos y control interno, la Sociedad mantiene una separación entre las funciones operativas o generadoras de riesgo y las funciones de control. Las áreas operativas son responsables de la ejecución de las actividades propias del servicio de enrutamiento de órdenes —tales como la recepción, canalización y confirmación de órdenes de los Clientes—, mientras que la función de control, radicada en el Encargado de Cumplimiento y Control Interno (ECCI), no participa en la ejecución de las operaciones que le corresponde controlar, salvo en la medida en que quien la ejerce desempeñe simultáneamente un cargo ejecutivo. En ese caso, el ECCI se abstiene de actuar como revisor independiente respecto de las materias individualizadas en el Anexo C de la Política de Contratación de Personal y de Remuneraciones, las que son revisadas por la persona designada al efecto en dicho Anexo.

La función de control es ejercida por el ECCI, quien es designado por el Directorio, le reporta directamente y mantiene acceso autónomo a éste, conforme a lo señalado en los numerales vi.ii y X del presente Manual. En el ejercicio de esta función, el ECCI cuenta además con el apoyo de la asesoría legal externa referida en el numeral vi.iii.

De este modo, ninguna persona ejerce sin contrapeso la ejecución y el control de un mismo proceso crítico. Allí donde ambas funciones concurren en una misma persona, la revisión independiente recae en el tercero designado en el Anexo C de la Política de Contratación de Personal y de Remuneraciones, el ECCI conserva reporte directo y acceso autónomo al Directorio, y el Directorio verifica anualmente la suficiencia de dichos controles dejando constancia de su conclusión en el acta respectiva.

Sin perjuicio de lo anterior, y en aplicación del principio de proporcionalidad y flexibilidad descrito en el numeral viii.xii, atendida la naturaleza, escala y complejidad de las operaciones de la Sociedad, en aquellos casos en que no resulte posible una separación total de funciones, se implementarán controles compensatorios debidamente documentados y aprobados por el Directorio, tales como revisiones cruzadas, autorizaciones de un nivel jerárquico superior y monitoreo por parte del ECCI. La Sociedad evaluará periódicamente la suficiencia de esta estructura organizacional y de los controles compensatorios adoptados, dejando evidencia de dicha evaluación.

Las áreas operativas y tecnológicas son responsables de ejecutar los procesos y controles de primera línea. El ECCI, como segunda línea, supervisa y evalúa su cumplimiento y efectividad, sin asumir la ejecución ordinaria de los controles que le corresponde revisar. Cuando quien ejerce el ECCI desempeñe además un cargo ejecutivo de primera línea, la separación entre ambas líneas no se obtiene por la persona sino por la materia: respecto de las materias individualizadas en el Anexo C de la Política de Contratación de Personal y de Remuneraciones, la revisión de segunda línea recae en el revisor allí designado y no en el ECCI.

El Directorio o la Gerencia General, según corresponda, designará formalmente un titular para cada cargo crítico, indicando sus facultades, responsabilidades, accesos, incompatibilidades y mecanismo de reemplazo. Las designaciones deberán constar por escrito y mantenerse permanentemente actualizadas.

Se considerarán cargos críticos, al menos, los siguientes:

Gerente General.

Encargado de Cumplimiento y Control Interno (ECCI).

Responsable de Tecnología y Operaciones.

Responsable de infraestructura y accesos.

Responsable de la relación operativa con los intermediarios y Corredores Asociados (servicio de Enrutamiento de Órdenes).

1. Responsable de los reportes a la CMF y de los reportes de incidentes.
2. Responsable del servicio de asesoría de inversión y quienes formulen recomendaciones personalizadas a clientes (servicio de Asesoría de Inversión).

Esta lista es común a los documentos del marco normativo interno de la Sociedad; los cargos que se indican como propios de un servicio determinado sólo son exigibles respecto de ese servicio.

Cada control establecido en el presente Manual y en las políticas y procedimientos que lo complementan deberá indicar, a lo menos, su responsable de ejecución, su revisor, su periodicidad, la Evidencia que lo acredita, el repositorio en que dicha Evidencia se conserva, el umbral que activa una excepción y el mecanismo de escalamiento aplicable.

Función de Gestión de Riesgos

La gestión de riesgos es una función esencial en Racional, diseñada para garantizar la identificación, evaluación, mitigación y monitoreo continuo de los riesgos que puedan afectar las operaciones de la Sociedad. Este proceso es realizado asegurando la operación segura, eficiente y alineada con el marco regulatorio aplicable.

Conforme a lo establecido en la NCG 502, la función de gestión de riesgos es la instancia responsable del monitoreo de los controles definidos en las políticas y procedimientos de gestión de riesgos y control interno de la Sociedad, la que deberá reportar directamente al Directorio de Racional.

Para lo anterior, la Sociedad procedió a identificar los riesgos y estableció políticas y procedimientos, estrategias de mitigación de riesgos y planes de contingencia consecuentes con estos. Los desarrollos de estas acciones se detallan en las secciones VIII y IX siguientes, donde se describen, de forma general, las políticas y procedimientos con las que realizan la gestión de riesgos y control interno, y las estrategias de mitigación y planes de contingencia con los que cuenta la Sociedad.

El objetivo principal de contar con políticas y procedimientos de gestión de riesgos y control interno formalizados es la minimización de los riesgos que pueden afectar los objetivos de la organización.

Políticas y Procedimientos de Gestión de Riesgo y Control Interno

A continuación, se describen las políticas y se hace referencia a los procedimientos que regulan los distintos aspectos en relación con el servicio de Enrutamiento de Órdenes.

Políticas y procedimientos de Conflictos de Interés.

1. Objetivo

La presente política de conflictos de interés tiene como objetivo identificar, regular y gestionar las situaciones que configuran un potencial conflicto de interés, sobre todo aquellas que pudieren originarse con ocasión de la prestación de los servicios de Enrutamiento de Órdenes por parte de Racional y que pudieren, potencial o efectivamente, perjudicar a sus Clientes.

2. Definición de conflicto de interés

Se entenderá por "Conflicto de Interés" cualquier hecho que pueda afectar o influir en la independencia u objetividad en el actuar de Racional y/o las Personas Obligadas, que pueda interferir en sus decisiones u obligaciones para con los Usuarios.

3. Principios

Frente a cualquier Conflicto de Interés que pudiese surgir, Racional y las Personas Obligadas deberán actuar siempre en el mejor interés del Cliente afectado y de conformidad con los siguientes principios:

1. Interés superior del Cliente: el interés del Cliente debe siempre primar por sobre el de Racional o por sobre el interés personal de las Personas Obligadas y las personas relacionadas con estas últimas, salvo con el consentimiento expreso de parte del Cliente.
2. Igualdad de trato hacia los Clientes, salvo que un Cliente consienta expresamente en una situación que privilegie a otro Cliente, en su desmedro.
3. Información y transparencia: este principio ve reflejado tanto en la obligación de las Personas Obligadas de informar a Racional en caso de existir un posible Conflicto de Interés que no pueda resolverse en conformidad con estos principios, como en la obligación de informar a los Clientes de Racional cuando no sea posible resolver un Conflicto de Interés en conformidad con estos principios, de forma de obtener su debido consentimiento u otra solución aceptable.
4. Prevención: principio que se ve reflejado en la obligación de adoptar las medidas que razonablemente sirvan para evitar los conflictos de interés según los casos y circunstancias determinadas.

4. Ámbito de aplicación

La presente política y procedimiento se aplica a todas las Personas Obligadas, incluyendo a aquellas actividades externalizadas que involucren la prestación de servicios de Enrutamiento de Órdenes y otros productos o servicios relacionados.

5. Procedimiento

El objetivo del procedimiento es poder identificar, gestionar y supervisar adecuadamente los potenciales Conflictos de Interés que surjan con ocasión de la prestación del servicio de Enrutamiento de Órdenes u otros servicios relacionados. Este procedimiento está conformado por las siguientes actividades:

1. Identificación de Conflictos de Interés: en términos generales, identificamos que los Conflictos de Interés pueden surgir en los casos donde, en el contexto de la prestación del servicio de Enrutamiento de Órdenes, se presenta una situación en la cual Racional y/o las Personas Obligadas, que están en una posición de confianza o fiduciaria respecto de un Usuario, presentan intereses individuales opuestos a los de dicho Usuario.

   Para identificar los potenciales Conflictos de Interés, el ECCI, con la colaboración de la Gerencia General y del Responsable de Tecnología y Operaciones, será responsable de implementar herramientas y acciones tales como formularios de conflictos de interés, revisión de relaciones personales y profesionales de las Personas Obligadas, y análisis de órdenes ejecutadas.

   Asimismo, se realizarán análisis de riesgos para detectar potenciales Conflictos de Interés.

   En particular, Racional identifica como potencial fuente de Conflictos de Interés su propio modelo de negocios y sus fuentes de ingreso, en la medida que la estructura de comisiones, remuneraciones, incentivos o cualquier beneficio económico que Racional perciba, directa o indirectamente, de terceros o de las entidades a las cuales se canalizan las órdenes, pudiere influir en las decisiones de enrutamiento de las órdenes de los Clientes. Las áreas específicas de atención identificadas por la Sociedad —entre ellas la retribución que Racional percibe del intermediario receptor al que canaliza las órdenes y las barreras de información lógicas y tecnológicas que segregan sistemas, accesos y bases de datos respecto de éste— se encuentran individualizadas en el Manual de Gobernanza Corporativa y detalladas en el manual de procedimientos operativos, a los que este Manual se remite.

1. Manejo de Conflictos de Interés: los potenciales conflictos de interés que surjan y se identifiquen por parte de los empleados y las Personas Obligadas deberán ser reportados al Gerente General de la Sociedad y al ECCI, mediante los canales identificados para estos efectos, pudiendo incluir email, plataformas de mensajería como Slack, documentos, u otros. Mientras se revisen por parte del Gerente General y ECCI de manera conjunta, no se deberán tomar decisiones que pudieran estar afectas a Conflictos de Interés. Cada nuevo Conflicto de Interés identificado será registrado por el ECCI en el Registro de Conflictos de Intereses Identificados, con indicación de la decisión adoptada y de su seguimiento, y se evaluarán los mecanismos de resolución de conflictos de interés particulares y/o generales según aplique. El ECCI mantiene dicho Registro, informa los conflictos materiales al Directorio y reporta a éste sobre su gestión.
2. Prevención y monitoreo de Conflictos de Interés: A nivel de controles, las políticas, procedimientos y mecanismos de Racional para prestar el servicio de Enrutamiento de Órdenes no se modificarán hasta que sean aprobadas por el Gerente General y Directorio, y en el día a día la canalización de las órdenes se realiza de manera 100% automatizada, sin inputs manuales que varíen en estos plazos.

   Cualquier cambio en relación con la canalización de órdenes será debidamente respaldado y documentado en su respectivo proceso. Existe una serie de controles asociados al servicio de Enrutamiento de Órdenes, partiendo por los de los cambios relevantes que pudiera haber, un sistema de permisos asociados a la infraestructura en la nube de Racional, y más.

Como medida de prevención, la canalización de las órdenes se efectúa conforme a criterios objetivos, previamente definidos y aplicados de manera uniforme, en el mejor interés del Cliente, sin que el modelo de negocios de Racional, sus fuentes de ingreso o su relación con las entidades de destino incidan en la decisión de enrutamiento en desmedro del interés del Cliente. Toda relación de Racional con las entidades a las cuales se canalizan las órdenes que pudiere configurar un Conflicto de Interés será identificada, gestionada y, cuando corresponda, informada al Cliente conforme a los principios establecidos en esta política.

En el desarrollo, implementación y/o supervisión del código asociado al algoritmo que contiene el modelo automatizado para canalizar órdenes, en relación en particular a la infraestructura, lenguaje y/o *frameworks*, seguridad y otros, participará también el Responsable de Tecnología y Operaciones, además de la Gerencia General.

6. Revisión de políticas y procedimientos

Las políticas y procedimientos serán revisadas y actualizadas por el Directorio, al menos una vez al año, o cuando existan cambios significativos.

Políticas y procedimientos de Confidencialidad de la Información.

1. Objetivo

El objetivo de esta política es garantizar la protección de la información confidencial relacionada con las órdenes pendientes de ejecución de los Usuarios, asegurando que dicha información se maneje conforme a los principios de privacidad establecidos por la legislación vigente, en particular la Ley N°19.628 sobre protección de datos personales. Racional se compromete a proteger los datos personales, su privacidad y la información reservada, evitando el acceso o divulgación no autorizada.

En este contexto, la Sociedad tendrá especial resguardo y cuidado en el tratamiento de los datos personales[1],considerando para cada caso el consentimiento del Usuario u otra base de licitud que sea aplicable conforme lo indica la Ley N°19.628.

Las Personas Obligadas deberán guardar estricta confidencialidad respecto de la información personal y de las operaciones de cada Usuario. Para tales efectos, deberán abstenerse de entregar a terceros la información del Usuario que obre en su poder, y se limitarán a utilizar la información correspondiente sólo para los propósitos relacionados con el servicio de Enrutamiento de Órdenes.

Racional se obliga a que la información personal y de las operaciones de cada Usuario estén guardados de un modo seguro, manteniendo la información almacenada de manera digital y bajo un estricto control. El acceso a la información de los Usuarios, de sus inversiones y operaciones estará limitado a las personas autorizadas para tales efectos por Racional.

La obligación de confidencialidad es sin perjuicio de las órdenes o resoluciones emitidas por alguna autoridad judicial o administrativa, con facultades suficientes, al amparo de las cuales se le requiera a Racional el envío de información de los Usuarios.

2. Definición

Se entenderá por “Información Confidencial”, cualquier documento, informe, base de datos, correo electrónico, conversación y cualquier otra clase de comunicación verbal o escrita proveniente de la Sociedad y sus Usuarios, así como la información relativa a terceros, de carácter legal, económico o financiero, referidos a aspectos relevantes de la marcha de los negocios de la Sociedad y/o sus Usuarios, que pueda impactar en ellos, directa y/o indirectamente.

3. Principios de tratamiento de Información Confidencial

La Sociedad se compromete con los siguientes principios, respecto del manejo de Información Confidencial relacionada con las operaciones de ésta, así como la relativa a terceros, con quienes mantiene una relación comercial:

1. Resguardar la confidencialidad de la información de sus Usuarios y, sobre todo, la información relativa a las órdenes pendientes de ejecución de dichos Usuarios.
2. Resguardar la confidencialidad de la información de sus contrapartes comerciales.
3. Establecer mecanismos de control, para evitar el uso de información confidencial y/o privilegiada por parte de sus colaboradores y otras personas que puedan tener acceso a ella.
4. Actuar con lealtad, en el uso que haga de la Información Confidencial de sus Clientes y contrapartes comerciales.
5. Cumplimiento interno: exigir a sus colaboradores, proveedores y terceros, cualquiera que sea éstos y que implique con ellos un intercambio de información, la aplicación de estos principios.
6. Registro de NDAs: llevar un Registro de los “NDA” (non disclosure agreement) suscritos por la Sociedad y otras empresas relacionadas, junto a la persona responsable interna de Racional en recibir dicha información, y la duración del acuerdo;
7. Registro y reporte: Llevar los registros exigidos por la ley y las normas de la CMF, respecto de personas con acceso a información privilegiada y de personas relacionadas a la Sociedad, y deberá informar oportunamente las operaciones de éstas a la CMF, cuando así lo exige la norma; y
8. Tratamiento de datos personales conforme a la ley: Realizar tratamiento de datos personales conforme lo define la Ley N°19.628, siempre que el titular de los mismos consienta expresamente en ello u otra base de licitud establecida en la Ley N°19.628 lo permita.

4. Ámbito de aplicación

Esta política y procedimiento se aplica a las Personas Obligadas de la Sociedad, así como a cualquier tercero que tenga acceso a Información Confidencial en el contexto de la prestación de los servicios de Enrutamiento de Órdenes y otros servicios relacionados.

5. Procedimiento

El procedimiento relativo al manejo de Información Confidencial y el tratamiento de datos personales consiste en que toda la información relacionada a los Usuarios y a sus operaciones queda guardada de forma automática en una infraestructura en la nube de Google. Esta información se almacena utilizando técnicas avanzadas de cifrado y seguridad para garantizar la protección de los datos personales y de la Información Confidencial contra el acceso y la divulgación no autorizadas.

En este contexto, solamente tienen acceso con credenciales de seguridad las personas que correspondan, quienes son determinadas por el Responsable de Tecnología y Operaciones en función de sus roles y responsabilidades dentro de la Sociedad. Además, se cuenta con un sistema de respaldos automático diario en la infraestructura de la nube de Google para evitar cualquier posible pérdida de los datos.

Asimismo, se establecen cláusulas de confidencialidad en los contratos que suscribe Racional con las personas que tienen acceso a la Información Confidencial, sean Personas Obligadas, proveedores u otros.

El responsable de mantener la seguridad de la infraestructura y datos de los Usuarios es el Responsable de Tecnología y Operaciones, supervisado por la Gerencia General. Esto implica que el Responsable de Tecnología y Operaciones se encarga de la implementación de las medidas de seguridad, la administración de los accesos y la supervisión del sistema de respaldos. La actividad de guardar y proteger la información es supervisada por el Gerente General, quien se asegura de que se cumplan todas las políticas y procedimientos de seguridad establecidas.

Para documentar el cumplimiento de estas actividades, se mantiene un registro detallado de todas las acciones realizadas, incluyendo accesos a la información, cambios en la configuración de seguridad, y la realización de respaldos. Estos registros son revisados periódicamente y/o según corresponda para verificar su conformidad con las políticas y procedimientos de la Sociedad y las normativas vigentes.

Dado que el servicio de la nube con Google es externalizado, el responsable dentro de la Sociedad es también el Responsable de Tecnología y Operaciones. Este se encarga de la gestión del contrato y de asegurar que el proveedor cumpla con todos los requisitos de seguridad, privacidad y protección de datos establecidos por Racional. Cualquier cambio relevante en estos temas debe ser aprobado por el Gerente General y/o Directorio, según corresponda.

6. Revisión de políticas y procedimientos

Las políticas y procedimientos serán revisadas y actualizadas por el Directorio, al menos una vez al año, o cuando existan cambios significativos.

Políticas y procedimientos de Información al Inversionista

1. Objetivo

El objetivo de esta política es asegurar que todos los Usuarios y el público general reciban información veraz, suficiente, clara y oportuna relativa a los servicios de Enrutamiento de Órdenes que ofrece Racional y otros servicios relacionados, conforme a lo dispuesto en la Ley N°21.521.

En este contexto, Racional se compromete a proporcionar información veraz, suficiente, clara, y oportuna a los Usuarios, asegurando que comprendan las características, condiciones, riesgos y costos de los servicios.

2. Principios

1. Veracidad y Exactitud: Toda la información proporcionada debe ser precisa, veraz y no inducir a error o confusión.
2. Oportunidad**:** La información debe ser entregada en un tiempo adecuado para que los inversionistas puedan tomar decisiones informadas.
3. Accesibilidad: La información debe ser clara, comprensible y fácilmente accesible para todos los inversionistas, sin distinción.
4. Periodicidad: Se deberá garantizar que la información se entregue de acuerdo con los plazos establecidos en la ley, en la normativa aplicable y en los procedimientos internos de la Sociedad.
5. Cumplimiento Normativo: La información entregada debe cumplir con lo dispuesto en el artículo 28 de la Ley N°21.521 y cualquier otra normativa aplicable.

3. Ámbito de aplicación

Esta política y procedimiento se aplica a todas las personas involucradas en la relación con los Usuarios, incluyendo a las Personas Obligadas de la Sociedad, así como a cualquier tercero que interactúe con los Usuarios en el contexto de la prestación de los servicios de Enrutamiento de Órdenes y otros servicios relacionados.

4. Información que debe ser conocida, periodicidad y mecanismos de divulgación

La información proporcionada por Racional será expresada en un lenguaje sencillo, evitando tecnicismos innecesarios y adaptándose a las características de los Usuarios y del público general receptor. Asimismo, su contenido será revisado periódicamente para garantizar su vigencia, veracidad y precisión.

Con respecto a la suficiencia y oportunidad, de conformidad con la normativa aplicable, Racional pondrá a disposición de los Usuarios y del público general, la siguiente información en la periodicidad que se indica a continuación:

1. Información para el público general

   Racional pondrá a disposición del público en todo momento y debidamente actualizada la siguiente información:

1. *Descripción general de la estructura de comisiones o remuneraciones que recibe Racional,* esto es, señalar si cobra a los Usuarios por canalizar órdenes o percibe una retribución del intermediario o sistema al que canaliza la orden, o del colocador o emisor de los instrumentos objeto de la orden; y si esa comisión o remuneración es fija o variable, el monto o porcentaje, y la forma de su determinación.

A la fecha de esta versión, y conforme al Contrato General de Servicios al Cliente, su Anexo A y los Términos y Condiciones del Plan Racional Pro, la estructura que se divulga es la siguiente: Racional no cobra al Usuario comisiones por transacción ni por el enrutamiento en ningún plan; el Plan Free incluye hasta diez transacciones mensuales de compra y venta de acciones sin costo y el Plan Pro, cuyo precio es el único cobro directo al Usuario, incluye transacciones ilimitadas y funcionalidades premium; Racional percibe del intermediario receptor un porcentaje fijo de la comisión de custodia que éste cobra al Usuario sobre los activos custodiados y un porcentaje fijo del spread cambiario aplicado en la compra y venta de dólares, cuyo nivel depende del plan del Usuario; y podría percibir de administradoras de fondos una remuneración por distribución, que se informará al Usuario en caso de existir. Toda modificación de esta estructura se refleja en la Información Legal antes de su entrada en vigencia.

1. *La existencia de conflictos de intereses* que emanen del modelo de negocios o sus fuentes de ingresos y cómo los gestiona. En este contexto, en caso de aplicar, se detallarán las medidas adoptadas para mitigarlos y prevenir que afecten a los Usuarios. Estos conflictos serán gestionados de forma transparente y documentada, garantizando que los intereses de los Clientes prevalezcan.
2. *Descripción de las políticas de gestión de riesgo operacional y los niveles de servicio comprometidos* en cuanto a disponibilidad, desempeño y continuidad.
3. *Forma y oportunidad en que serán informados los incidentes* que comprometan la disponibilidad y seguridad de la información.
4. *Identificación de las garantías que la Sociedad haya constituido* para indemnizar los perjuicios que se puedan producir a los Usuarios, así como la descripción de la forma o mecanismos de ejecución y asignación de esas garantías.
5. Información para los Usuarios

Racional pondrá a disposición del Usuario previo a, o con posterioridad a, canalizar la orden, la siguiente información:

1. *Previo a la canalización de órdenes:* En caso de aplicar, Racional informará a los Clientes sobre los conflictos de intereses que se susciten entre Racional y el Cliente en particular y cómo pueden afectarlo si no se resolvieren adecuadamente.

1. *Con posterioridad a la canalización de órdenes:* Racional informará a los Clientes el hecho de que se recibió y canalizó la orden, así como la confirmación de su recepción y eventual ejecución por parte del intermediario, sistema alternativo de transacción o tercero al que se hubiere derivado esa orden.

No será necesario entregar la información a que se refieren las letras a) y b) del párrafo anterior, en caso de Usuarios que tengan la calidad de Inversionista Institucional, conforme al artículo 4° bis letra e) de la Ley N° 18.045, o de Inversionista Calificado, de entre los señalados en los números 2, 3 y 4 de la Sección II de la Norma de Carácter General N° 216 de la Comisión, que es la norma que define esta última categoría.

En cuanto a los mecanismos de divulgación y entrega de información, toda la información aplicable se encontrará disponible en el sitio web y en la aplicación móvil de Racional conforme a la periodicidad indicada precedentemente, utilizando formatos interactivos y didácticos para facilitar su comprensión.

5. Procedimiento de control de cumplimiento

La supervisión y control del cumplimiento de esta política estará a cargo del ECCI, quien verificará la veracidad, suficiencia, claridad y accesibilidad oportuna de la información proporcionada a los Usuarios y al público general.

Para estos efectos, el ECCI revisará la veracidad y exactitud de toda la información divulgada en el sitio web y la aplicación móvil de Racional para asegurarse de que no contenga errores que puedan inducir a los Usuarios a tomar decisiones incorrectas. Asimismo, revisará que toda la información exigida por la normativa aplicable y la demás que Racional estime conveniente, esté siendo entregada de manera oportuna a los Usuarios y al público general a través de los referidos canales.

Adicionalmente, realizará una evaluación anual de la efectividad de la información entregada sobre la base de estudios o análisis que permitan definir si está siendo leída y comprendida por los receptores. A modo de ejemplo, podrá revisar las consultas o reclamos recibidas y utilizar los resultados de este análisis para mejorar y ajustar el proceso de elaboración y entrega de la información.

6. Revisión de políticas y procedimientos

Las políticas y procedimientos serán revisadas y actualizadas por el Directorio, al menos una vez al año, o cuando existan cambios significativos.

Políticas y procedimientos de cumplimiento de requisitos legales y normativos de funcionamiento

1. Objetivo

El propósito de esta política es garantizar que la Sociedad cumpla en todo momento con los requisitos legales y normativos necesarios para operar como entidad regulada, asegurando que todas las actividades realizadas se desarrollen conforme a la regulación aplicable. Esta política establece las medidas necesarias para monitorear y garantizar el cumplimiento de dichos requisitos, y los procedimientos para gestionar adecuadamente cualquier evento de incumplimiento.

2. Principios

Racional se compromete con una serie de principios generales que constituirán los pilares fundamentales del actuar de la organización frente al cumplimiento de la regulación, políticas y procedimientos. A continuación, se puede encontrar un listado de los principales principios:

1. Cumplimiento de la legislación: Todos los colaboradores deben cumplir rigurosamente con la legislación vigente en el desempeño de sus funciones y representación de la Sociedad. Racional se compromete a participar únicamente en actividades legítimas, manteniendo altos estándares de calidad, transparencia y competencia justa.

2. Cumplimiento de requisitos legales y normativos: Racional debe cumplir con todas las leyes, regulaciones y normativas aplicables que la habiliten para funcionar y operar legalmente en calidad de enrutador de órdenes. Esta obligación se extiende a todas las Personas Obligadas.
3. Monitoreo y verificación del cumplimiento de los requisitos de funcionamiento: Racional debe establecer mecanismos de monitoreo continuo para asegurar que se cumplan los requisitos específicos de funcionamiento regulados.
4. Informar a las autoridades competentes: En caso de incumplimiento a los requisitos legales y normativos de funcionamiento, la Sociedad deberá informar oportunamente a la Comisión para el Mercado Financiero.
5. Cumplimiento de las políticas y procedimientos: Los colaboradores deben adherirse a los procedimientos y políticas establecidas por la Sociedad en el ejercicio de sus funciones.
6. Gestión de incumplimientos: Racional debe definir procedimientos para el caso de que se presenten eventos de incumplimiento en los requisitos legales y normativos de funcionamiento.
7. Deber de denunciar: Todo colaborador que tenga conocimiento de posibles infracciones éticas y normativas graves dentro de la organización, y/o de incumplimientos a los requisitos legales y normativos de funcionamiento, tiene la obligación de reportarlo internamente a través del canal de denuncia proporcionado por la Sociedad.
8. Prevenir el Uso de Información Privilegiada: se prohíbe el uso indebido de información privilegiada. Los colaboradores deben abstenerse de beneficiarse de esta información y reportar cualquier uso indebido.
9. Prevención del Lavado de Dinero: Racional se abstendrá de establecer relaciones con individuos o entidades sospechosas de actividades ilegales.
10. Prevención del Fraude: Racional adopta una política de tolerancia cero frente al fraude interno y externo. Se promueve la transparencia y se implementan controles para mitigar el riesgo de fraude en todas las operaciones y relaciones comerciales.
11. Manipulación de Precios: La Sociedad prohíbe cualquier práctica de asociada a la concertación de precios o tasas con otro partícipe de la industria.
12. Compromiso: Todos los colaboradores deben comprometerse a cumplir y promover los procesos establecidos en materia de políticas y procedimientos de la Sociedad.

3. Ámbito de aplicación

Esta política se aplica a las Personas Obligadas, y también a los proveedores y terceros que se relacionan con la Sociedad para la prestación de servicios que pueden estar afectos a los requisitos legales y normativos de funcionamiento.

4. Procedimiento

El objetivo de este procedimiento es definir las acciones necesarias para monitorear, verificar y garantizar que la Sociedad cumpla con los requisitos legales y normativos específicos para operar como entidad regulada. Además, se establece el proceso para gestionar y remediar cualquier evento de incumpli-

miento en dichos requisitos.

En este contexto, las acciones principales consisten en: (i) la identificación de los requisitos legales y normativos de funcionamiento aplicables a la Sociedad, (ii) el registro de los requisitos identificados y la designación de los responsables de cumplimiento, (iii) los controles preventivos de incumplimiento; y (iv) el monitoreo de los controles preventivos implementados.

1. Identificación de requisitos legales y normativos aplicables y registro

   El ECCI será el encargado de identificar y mantener actualizados los requisitos legales y normativos aplicables que permitan a la Sociedad operar dentro del marco regulatorio.

   Para estos efectos, realizará una revisión exhaustiva de las leyes y regulaciones que rigen la actividad de la Sociedad, incluidas normativas específicas, oficios, y cualquier otra normativa relacionada que resulte aplicable.

1. Registro de los requisitos legales y normativos identificados y designación de responsables de cumplimiento

   Luego de haber identificado los requisitos legales y normativos de funcionamiento aplicables a la Sociedad, Racional implementará una Matriz de Cumplimiento Normativo (“Matriz”) con el objetivo de mantener un registro exhaustivo de todos los requisitos y emitir recordatorios en fechas específicas. Este documento deberá cumplir con las siguientes características:

1. Incluir las fechas límites o periodicidad de cumplimiento para cada requisito legal o normativo aplicable a la Sociedad.
2. Designar a los responsables encargados de materializar el cumplimiento de cada requisito legal o normativo.
3. Estar accesible para todas las áreas y colaboradores involucrados en el cumplimiento de estos requisitos.

   La responsabilidad de elaborar y mantener actualizada la Matriz de Cumplimiento Normativo recae en el ECCI.

   En este contexto, el ECCI deberá elaborar un borrador de la Matriz que incluya los requisitos legales y normativos identificados, sus plazos o su periodicidad, los responsables de su ejecución y, si es necesario, fechas de recordatorio. Este borrador será validado por las áreas y colaboradores pertinentes involucrados en el cumplimiento de las exigencias.

   Una vez validado, el ECCI deberá integrar los plazos o la periodicidad aplicable en la Matriz, específicamente, en un calendario corporativo accesible a todos los responsables del cumplimiento de los requisitos legales y normativos de funcionamiento.

   Además, el ECCI será responsable de generar recordatorios oportunos antes de las fechas de los plazos o de la periodicidad aplicable para el cumplimiento de los requisitos. En la fecha máxima de cumplimiento, el ECCI verificará que se haya cumplido con el requisito respectivo solicitan-

do al responsable de la ejecución la evidencia correspondiente como, por ejemplo, comprobantes de envío a la CMF, capturas de pantalla o registros relevantes. Esta evidencia deberá ser registrada en el repositorio designado para tal fin.

Por último, anualmente, durante el cierre de cada año calendario, el ECCI realizará un levantamiento de todos los requisitos legales y normativos de funcionamiento aplicables a la Sociedad que estarán vigentes durante el próximo año, actualizando la Matriz en dichos términos.

1. Controles preventivos de incumplimiento legal o normativo

   Los controles preventivos de incumplimiento abarcan todas las áreas, procesos o actividades de la Sociedad que están expuestas a posibles incumplimientos legales o normativos. A continuación, se detallan los controles implementados:

1. Revisión por Revisor Independiente:

   Cada requisito legal o normativo que implique la generación y envío de información a una entidad externa debe ser revisada por un colaborador designado como "Revisor Independiente". Este rol será diferente al del "Ejecutor", quien es responsable de elaborar el reporte de información. Por otro lado, el "Emisor", quien es el encargado de la emisión definitiva de la información, puede ser una persona distinta al Revisor o Ejecutor.

1. Monitoreo continuo de cumplimiento por el ECCI:

   El ECCI monitoreará periódicamente, según el calendario de requisitos legales o normativos contenido en la Matriz, el cumplimiento oportuno de los referidos requisitos. Para estos efectos, realizará revisiones periódicas y análisis de los procesos operativos para asegurar que la Sociedad cumpla con todos los requisitos legales y normativos de funcionamiento en todo momento.

   Se mantendrán registros detallados de los informes de revisión y cualquier otra documentación relacionada con el monitoreo del cumplimiento.

1. Asignación de Informes Eventuales:

   El ECCI coordinará con las jefaturas para asignar los informes de requisitos legales o normativos que puedan surgir eventualmente y que no estén sujetos a un calendario específico. Los responsables designados serán responsables de reportar cualquier evento especificado por la legislación o normativa y llevar a cabo las tareas correspondientes.

1. Asesoría Legal o Técnica:

   La Sociedad buscará apoyo en asesoría legal o técnica para todas las cuestiones relacionadas con el cumplimiento normativo, especialmente en el contexto de la supervisión por parte de la CMF u otros organismos fiscalizadores.

1. Monitoreo de los controles preventivos implementados

   El encargado de la Función de Gestión de Riesgos verificará periódicamente que los controles establecidos para la prevención del riesgo normativo y legal operen según su diseño, mediante la ejecución de actividades de monitoreo internas.

El objetivo de este monitoreo es identificar deficiencias o combinaciones de deficiencias en los controles que puedan afectar significativamente la operación del modelo de prevención.

Las actividades de monitoreo evaluarán la aplicación y eficacia de los controles, identificando las áreas o procesos con mayor exposición a fraudes, delitos o incumplimientos, y propondrán al Directorio posibles mejoras. Anualmente, el encargado de la Función de Gestión de Riesgos presentará una planificación de actividades de monitoreo, alineada con los procesos críticos y los controles de riesgos establecidos en la Matriz de Cumplimiento Normativo.

5. Procedimiento en caso de verificarse evento de incumplimiento en los requisitos legales y normativos de funcionamiento

En caso de que se detecte un evento de incumplimiento de los requisitos legales o normativos de funcionamiento, el ECCI deberá investigar el evento, evaluar sus implicancias y tomar las acciones correctivas necesarias. Las acciones correctivas podrán incluir modificaciones en los procedimientos, implementación de controles preventivos adicionales, entre otras.

En este contexto, los incumplimientos serán evaluados por el ECCI y se informarán a la CMF cuando la normativa aplicable, una instrucción de dicha autoridad o la naturaleza del incumplimiento así lo exija. Asimismo, serán reportados al Gerente General y/o Directorio de la Sociedad, y serán documentados en un informe detallado que incluirá la descripción del incumplimiento, la evaluación de su impacto y las acciones correctivas tomadas.

6. Revisión de políticas y procedimientos

Las políticas y procedimientos serán revisadas y actualizadas por el Directorio, al menos una vez al año, o cuando existan cambios significativos.

Lineamientos de seguridad de la información y ciberseguridad.

La seguridad de la información y la ciberseguridad son pilares estratégicos para Racional, siendo esencial para garantizar la protección de los datos, la continuidad operativa y el cumplimiento normativo.

La política de seguridad de la información y ciberseguridad tiene como objetivo establecer un marco que permita identificar, proteger y responder de manera efectiva a amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos de la Sociedad y de sus Usuarios.

Esta política aplica a todas las áreas, colaboradores, sistemas tecnológicos y procesos de Racional que impliquen el manejo de información propia o de terceros. Además, abarca los servicios externalizados relacionados con la gestión de datos y ciberseguridad, asegurando que los proveedores cumplan con los estándares definidos.

En este contexto, Racional y todas sus políticas y procedimientos de gestión de riesgos y control interno deberán observar los siguientes lineamientos en términos de seguridad de la información y ciberseguridad:

1. Capacitación Periódica del Personal

La Sociedad realizará capacitaciones periódicas para todo el personal, con el fin de asegurar que estén conscientes de los riesgos de seguridad de la información y ciberseguridad. Estas capacitaciones tienen como objetivo principal que el personal contribuya de manera efectiva a la adecuada gestión de dichos riesgos, fomentando una cultura organizacional orientada a la seguridad.

1. Resguardo de la Información de los Clientes

Para estos efectos, Racional implementará las siguientes medidas:

- 1. Inventario y Clasificación de Activos de Información: La Sociedad implementará y mantendrá un inventario actualizado de los activos de información. Este inventario incluirá una clasificación detallada de los activos, considerando dimensiones clave como la disponibilidad, confidencialidad e integridad de los mismos.
  2. Inventario de Servicios Relacionados con Activos de Información: Se llevará un registro de los servicios relacionados con los activos de información, asegurando que todos los servicios estén identificados y documentados para facilitar su gestión y protección.
  3. Controles de Acceso: La Sociedad establecerá controles de acceso a las instalaciones, infraestructuras de negocios y sistemas de información. Estos controles serán revisados y actualizados periódicamente para garantizar su eficacia.
  4. Herramientas de Registro, Control y Monitoreo: Se implementarán herramientas avanzadas de registro, control y monitoreo de la actividad de los usuarios que utilizan los sistemas de información. Esto permitirá detectar y responder oportunamente a cualquier actividad inusual o no autorizada.

1. Implementación de Controles para Mitigar Riesgos del Uso de Dispositivos Móviles y Acceso Remoto, y de Herramientas de Gestión de Ciberseguridad

La Sociedad adoptará controles específicos para mitigar los riesgos asociados al uso de dispositivos móviles y el acceso remoto del personal. Asimismo, implementará herramientas de gestión de ciberseguridad como, por ejemplo, programas de gestión de parches de *software* y *firmware*, protección de redes mediante *firewalls*, sistemas de prevención de intrusos, elevación de privilegios, gestión de identidades y acceso físico y lógico, y mecanismos de control de identidad para evitar la suplantación.

1. Gestión de Condiciones Ambientales

Racional establecerá medidas para gestionar adecuadamente las condiciones ambientales a efectos de que sus equipos y herramientas estén ubicados en una localización segura. Esto incluye asegurar que los equipos estén protegidos contra factores ambientales adversos que puedan comprometer su funcionamiento y seguridad.

1. Procedimientos de Identificación de Amenazas de Ciberseguridad

La Sociedad implementará procedimientos para la identificación temprana de amenazas de ciberseguridad, tales como phishing, malware, y la inyección de código malicioso, entre otras. Estos procedimientos incluirán la actualización constante de las técnicas de detección y la capacitación del personal en la identificación y manejo de estas amenazas.

1. Procedimientos de Respuesta y Recuperación ante Incidentes Operacionales

    Racional implementará procedimientos de respuesta y recuperación ante incidentes operacionales, los que deberán considerar la recuperación oportuna de funciones críticas; los procesos de respaldo y soporte; los activos críticos de información previamente definidos; y la interdependencia con terceros.

El Responsable de Tecnología y Operaciones, en coordinación con el ECCI, es responsable de implementar los lineamientos de seguridad de la información y ciberseguridad.

El ECCI es el encargado de evaluar periódicamente los controles establecidos en la materia y de reportar al Directorio los resultados de estas evaluaciones.

El Directorio revisará anualmente los lineamientos de seguridad de la información y ciberseguridad, y los actualizará cada vez que lo requieran cambios regulatorios o tecnológicos.

Procedimiento de Enrutamiento de Órdenes y Trazabilidad.

Tecnología y Operaciones mantendrá un procedimiento documentado que cubra, de extremo a extremo, la recepción, validación, registro de fecha y hora, transmisión, acuse de recibo, rechazo, cancelación, corrección, estado, ejecución informada por el Corredor Asociado y cierre de cada Orden. El procedimiento deberá impedir alteraciones no autorizadas y permitir reconstruir íntegramente la trazabilidad de cada Orden.

El procedimiento comprenderá, al menos, las siguientes materias:

- Validaciones previas a la transmisión de la Orden, incluyendo verificación de identidad del Cliente, integridad y consistencia de los parámetros de la Orden y controles de razonabilidad.
- Registro de fecha y hora de recepción, transmisión y cierre de cada Orden, con fuente horaria confiable.
- Identificación única de la Orden, que permita su seguimiento en todos los sistemas involucrados.
- Acuse de recibo o rechazo por parte del intermediario o Corredor Asociado, y registro del motivo del rechazo.
- Tratamiento de órdenes duplicadas, incluyendo mecanismos de detección y supresión.
- Cancelaciones de Órdenes y, cuando proceda, su reemplazo mediante cancelación y nueva Orden, con registro del solicitante, la causa, la autorización y la hora.
- Caídas de API, latencias anómalas o indisponibilidad del intermediario o Corredor Asociado, con los mecanismos alternativos y de contención aplicables.
- Comunicación al Cliente respecto de la recepción, transmisión, rechazo, cancelación o corrección de su Orden.
- Cierre de la Orden y conservación de la Evidencia correspondiente en el repositorio designado.

La ejecución de este procedimiento corresponde a Tecnología y Operaciones, en su calidad de primera línea. El ECCI, como segunda línea, monitoreará su cumplimiento y evaluará su efectividad, sin asumir la ejecución ordinaria de los controles que le corresponde revisar. Concurriendo ambas funciones en

una misma persona, la revisión de los controles señalados en el Anexo C de la Política de Contratación de Personal y de Remuneraciones recae en el revisor allí designado.

Conciliación de Órdenes.

Racional conciliará periódicamente las Órdenes recibidas y transmitidas con los acuses, rechazos y estados informados por cada Corredor Asociado. Toda diferencia deberá registrarse, investigarse, resolverse dentro del plazo definido y escalarse según su impacto. Tecnología y Operaciones ejecutará la conciliación; un Revisor Independiente verificará sus resultados; y el ECCI monitoreará el cumplimiento y las excepciones.

La conciliación se efectuará con periodicidad diaria respecto de la totalidad de las Órdenes del día hábil anterior y, tratándose de Órdenes críticas o de eventos de indisponibilidad, con periodicidad intradía conforme lo determine Tecnología y Operaciones. Las diferencias que no puedan resolverse dentro del día hábil siguiente serán escaladas a la Gerencia General y, si su impacto lo amerita, al Directorio.

La Evidencia de cada conciliación reportes de origen, reportes del Corredor Asociado, partidas conciliatorias, resolución de diferencias y visto bueno del Revisor Independiente se conservará en el repositorio designado y estará permanentemente disponible para su examen a solicitud de la CMF.

Algoritmo de Enrutamiento y Control de Cambios.

El enrutamiento de las Órdenes se realiza de manera automatizada. El enrutamiento se rige por criterios objetivos previamente aprobados y aplicados de manera uniforme conforme a las instrucciones del Cliente, sin favorecer a un Corredor Asociado por ingresos, incentivos o relaciones comerciales. A la fecha la regla de canalización es determinada y no una selección dinámica entre alternativas: la Orden se transmite al intermediario con el que el Cliente mantiene contrato vigente, conforme a la Parte III de la Política de Gestión de Terceros. Racional no asume obligaciones de mejor ejecución, que corresponden a quien ejecuta la Orden.

Todo cambio material en el algoritmo, en sus reglas de decisión o en los criterios objetivos de enrutamiento exigirá, previamente a su liberación a producción:

- Solicitud formal de cambio, con identificación del solicitante, el objetivo y el alcance.
- Evaluación de riesgos y de conflictos de interés asociados al cambio.
- Pruebas documentadas en ambiente distinto del productivo, con criterios de aceptación definidos.
- Aprobación de la Gerencia General y del Directorio.
- Segregación entre quien desarrolla y quien despliega el cambio.
- Plan de reversa que permita restituir la versión anterior.
- Registro de la versión liberada, con fecha, hora, responsable y contenido del cambio.

El ECCI verificará el cumplimiento de este control de cambios y reportará al Directorio las excepciones detectadas. Se prohíbe modificar reglas de enrutamiento o eludir los controles descritos sin la autorización previa aquí exigida.

Capacidad Operacional y Pruebas.

Tecnología y Operaciones realizará y documentará, al menos anualmente y ante cambios materiales, pruebas de capacidad, disponibilidad, estrés, recuperación y continuidad sobre los componentes críticos del servicio de Enrutamiento. Las pruebas deberán considerar el volumen actual y proyectado, las dependencias con terceros, criterios de aceptación, resultados, desviaciones y planes de remediación. El ECCI verificará su ejecución y reportará sus conclusiones al Directorio.

La exigencia de un informe de un tercero independiente sobre capacidad operacional no constituye una obligación propia de Racional por el solo hecho de prestar el servicio de Enrutamiento de Órdenes. La Sociedad sí debe acreditar y mantener su capacidad operacional conforme al primer y segundo párrafo de la Sección VI de la NCG 502 y a su Sección II.E letra d). La exigencia de informe de tercero, en cambio, está contenida en el último párrafo de la Sección VI, en su texto fijado por la Sección I letra F de la NCG N° 524, y se encuentra circunscrita a quienes presten servicios de intermediación o custodia de instrumentos financieros y se clasifiquen en el Bloque 2 o 3, calidad que la Sociedad no tiene. Racional evaluará su procedencia únicamente si en el futuro presta alguno de dichos servicios, dejando constancia de dicha evaluación.

Continuidad Operacional.

Racional mantendrá vigentes, aprobados y operativos un Plan de Continuidad de Negocio, un Plan de Recuperación ante Desastres y el correspondiente Análisis de Impacto en el Negocio. Estos instrumentos serán revisados y probados al menos anualmente y ante cambios materiales.

Dichos instrumentos comprenderán, al menos:

- Análisis de Impacto en el Negocio (BIA).
- Identificación de los procesos críticos, incluido el ciclo completo de Enrutamiento de Órdenes.
- Definición de RTO (Recovery Time Objective) y RPO (Recovery Point Objective) por proceso crítico.
- Identificación de las dependencias con terceros, incluidos proveedores de infraestructura y Corredores Asociados.
- Política de respaldos y procedimientos de restauración, con pruebas de restauración efectivas.
- Responsables de cada actividad de continuidad y recuperación.
- Mecanismos alternativos de operación ante indisponibilidad de los sistemas o de los intermediarios.
- Protocolos de comunicación interna, a la CMF y a los Clientes.
- Informe de resultados de cada prueba, con desviaciones identificadas.
- Plan de remediación y seguimiento de los hallazgos hasta su cierre.

Tecnología y Operaciones ejecuta y documenta estas actividades; el ECCI verifica su ejecución y efectividad; y el Directorio conoce y aprueba anualmente los planes y los resultados de las pruebas, dejando constancia en acta.

Patrimonio Ajustado y Garantías.

Mientras Racional se encuentre clasificada en el Bloque 2 para el servicio de Enrutamiento de Órdenes, mantendrá permanentemente patrimonio ajustado y/o garantías por un monto no inferior a UF 500. Finanzas será responsable del cálculo y control de suficiencia; el ECCI efectuará un monitoreo independiente y coordinará el reporte FINTEC02.

La garantía deberá renovarse antes de su vencimiento, con alertas a 90, 60, 30, 15 y 5 días conforme al Procedimiento de Control y Renovación de la Garantía, responsable definido y evidencia de vigencia y cobertura disponible para la CMF.

Tras la NCG N° 524, la clasificación del servicio de enrutamiento de órdenes en la Tabla 4 de la Sección IV.D.4 (Bloque 2, 100 o más clientes activos en Chile) determina tanto las exigencias organizacionales y de gestión de riesgos de la Sección IV.D como, por remisión de la Sección V.A, la exigencia de patrimonio o garantía de la Sección V. Se trata de una única clasificación con dos efectos, y no de dos criterios independientes. El ECCI monitoreará mensualmente ambos parámetros y reportará al Directorio cualquier aproximación o superación de umbrales.

Aplicación del Principio de Proporcionalidad y Flexibilidad

Racional adopta el principio de proporcionalidad en el diseño y aplicación de sus políticas y procedimientos. Este enfoque asegura que las medidas implementadas sean adecuadas a la naturaleza, escala y complejidad de las operaciones de la Sociedad, optimizando recursos y garantizando un cumplimiento normativo efectivo. Esto, con el objeto de ajustar las políticas, procedimientos y controles a las características específicas de la Sociedad, considerando factores como el tamaño de la organización, el volumen de operaciones y el número o tipo de clientes.

El principio de proporcionalidad se aplica transversalmente en todas las políticas y procedimientos de la Sociedad.

Plan de Gestión de Riesgos: Estrategias de Mitigación de Riesgos, Planes de Contingencia y Riesgo Operacional.

El encargado de la función de gestión de riesgos de la Sociedad es el responsable de elaborar un plan de gestión de riesgos que incluya las estrategias de mitigación de riesgos y la planificación de contingencias en relación con los principales riesgos de Racional, los que como mínimo deben contemplar los riesgos provenientes de conflictos de intereses y los riesgos de seguridad de la información y ciberseguridad.

El plan de gestión de riesgos abarca todas las áreas operativas, tecnológicas y de control interno de la Sociedad. En este contexto, la elaboración de las estrategias de mitigación de riesgos y la planificación de contingencias en relación con los principales riesgos, considerará lo siguiente:

1. Identificación de procesos en los que se descomponen las actividades efectuadas por Racional y los responsables de dichos procesos para identificar riesgos potenciales. Esto incluye el uso de herramientas como mapas de procesos y de riesgos, y matrices de identificación de eventos, con especial atención en riesgos operativos, tecnológicos y regulatorios.

2. Identificación de los riesgos inherentes a los que se expone la Sociedad en el desarrollo de sus actividades.
3. Medición de los riesgos inherentes identificados en las actividades efectuadas por la Sociedad. En este contexto, los riesgos identificados son clasificados según su impacto y probabilidad mediante una matriz que permite priorizar las acciones correctivas. Los niveles de riesgo se clasifican como Bajo, Medio, Alto y Crítico. Esta clasificación considerará factores financieros, reputacionales y operativos.
4. Definición de los mecanismos de control para mitigar los riesgos inherentes identificados.

   En este contexto, la Sociedad implementa controles internos preventivos y correctivos que incluyen:

• Controles tecnológicos como autenticación multifactor y cifrado de datos.

• Procedimientos operativos documentados.

• Monitoreo de actividades críticas mediante indicadores clave de riesgo.

   Adicionalmente, en caso de la materialización de un riesgo identificado, la Sociedad dispone de planes de contingencia que garantizan:

• La recuperación de datos a través de respaldos automáticos.

• La continuidad operativa mediante sistemas redundantes.

• Protocolos de respuesta inmediata frente a incidentes de ciberseguridad.

1. Procedimientos de información y comunicación de la gestión de riesgos que asegure que la información relevante acerca de la efectividad de los controles mitigantes y el cumplimiento de los niveles de apetito por riesgo llegue al Directorio y a todas las partes interesadas.
2. Programa de mejoramiento continuo de la gestión de riesgos, con el objeto de evaluar la necesidad de realizar cambios frente a nuevos escenarios económicos y financieros que vaya enfrentando la Sociedad, cambios del perfil de riesgo y producto de la implementación o cambios en los estándares o mejores prácticas internacionales.

Este plan será monitoreado continuamente por parte de la función de gestión de riesgos para asegurar su efectividad y controlar su cumplimiento. En esta línea, también monitoreará la correcta ejecución de las estrategias de mitigación de riesgos y de los planes de contingencia relacionados a los eventos asociados a los riesgos que surjan de las actividades de la Sociedad.

Anualmente, se realiza una revisión integral del plan de gestión de riesgos, incorporando los cambios operativos, tecnológicos o regulatorios que se hubiesen producido. Asimismo, el Directorio deberá aprobar el plan de gestión de riesgos al menos de forma anual a efectos de que se reflejen los cambios significativos experimentados en la estrategia de negocios de la Sociedad o los cambios en las condiciones de mercado.

Función de Control

Encargado de Cumplimiento y Control Interno.

El ECCI es el responsable de la función de control de la Sociedad. Esta responsabilidad implica la realización de diversas actividades para monitorear el cumplimiento de las políticas, los planes, procedimientos y controles que la Sociedad defina.

El ECCI deberá desarrollar, implementar y mantener un sistema de control que permita verificar que los empleados de la Sociedad conozcan y cumplan con las políticas y procedimientos aprobados por ésta. Para estos efectos deberá contar con la identificación de las personas de todos los niveles jerárquicos que se encargan de administrar las funciones de gestión de riesgos y control de manera cotidiana, indicando sus respectivas responsabilidades.

Sin perjuicio de los informes, el ECCI deberá elaborar, cuando corresponda, informes dirigidos al Directorio dando cuenta y documentando las instancias de incumplimiento de límites y controles, y las acciones adoptadas ante tales circunstancias.

En el ejercicio de sus funciones, el ECCI deberá coordinar y/o realizar evaluaciones periódicas de las materias objeto de la Sociedad. Deberá, además, de acuerdo a un calendario de monitoreos, realizar monitoreo de la ejecución de los controles y pruebas periódicas a los mecanismos de control, con el fin de verificar su funcionamiento y definir revisiones y ajustes, de ser pertinentes.

Manejo de excepciones.

En caso de cualquier situación de excepción a lo establecido en el presente Manual, es necesario analizar la situación que la amerita o provoca, con el objetivo de determinar la estructura de control interno, la naturaleza, causa y efectos de la autorización. Lo anterior, sin perjuicio del procedimiento de aprobación de excepciones establecidas en las políticas y/o manuales de procedimientos aplicables.

Para cumplir lo anterior se deberá:

1. Definir si la excepción es crítica o no.
2. Determinar la naturaleza y causa de cada excepción, considerando si es intencional o no intencional.
3. Evaluar el peor efecto posible que tiene cada excepción.
4. Decidir qué excepciones críticas son consistentes o inconsistentes para valorar el nivel del control de riesgo.
5. Determinar el efecto de las excepciones en la Sociedad.
6. Buscar medidas de mitigación o control.

Las excepciones a lo establecido en el presente Manual o a los procedimientos establecidos que no hayan sido calificadas como críticas deberán ser aprobadas por el Gerente General de la Sociedad. Las excepciones calificadas como críticas conforme al análisis precedente deberán ser aprobadas por el Directorio, dejándose constancia en acta. Cuando la urgencia de la situación no permita esperar a la próxima sesión, el Gerente General podrá autorizarlas provisionalmente, debiendo someterlas a ratificación del Directorio en la sesión siguiente. En todos los casos, la solicitud, su fundamento, la evaluación

efectuada conforme a lo señalado precedentemente y la decisión adoptada se registrarán por escrito y se remitirán al ECCI, quien mantendrá el registro de excepciones y dará cuenta de ellas en su informe semestral al Directorio.

Otras Disposiciones

Lo establecido en el presente Manual tiene por objeto complementar la normativa que regula las materias aquí tratadas, por lo cual la Sociedad y sus colaboradores deberán dar cumplimiento a las normas que se relacionen con lo establecido en este Manual. Asimismo, en caso de existir oposición entre lo dispuesto por la normativa aplicable y el presente Manual, primará la disposición legal o reglamentaria correspondiente.

Actualización

En el caso que cualquier disposición del presente Manual sea modificada, ésta deberá ser puesta en conocimiento de las personas que corresponda dentro del plazo de 5 días hábiles a partir de la fecha en que el Directorio acuerde la referida modificación. Junto con lo anterior, se deberá emitir un texto refundido del Manual el cual deberá estar a disposición de todos los funcionarios que corresponda, ya sea por medio escrito o electrónico.

El presente Manual deberá ser revisado por parte del Directorio al menos una vez al año y cada vez que se presenten circunstancias que así lo ameriten.

El control de versiones del presente Manual será mantenido por el Encargado de Cumplimiento y Control Interno (ECCI), quien registrará cada modificación en la tabla de Control de Versiones contenida en el numeral XIV, dejando constancia de la versión, la descripción del cambio y la fecha de aprobación por el Directorio. La revisión anual será planificada conforme a un calendario definido por el ECCI, y la documentación de respaldo de cada revisión y actualización, incluyendo las actas de aprobación, las versiones anteriores del Manual y la evidencia de su difusión, se conservará en un repositorio único, permanentemente disponible para su examen a solicitud de la CMF.

Difusión y Capacitación

Racional reconoce que una adecuada capacitación y la difusión efectiva de sus políticas y procedimientos son fundamentales para fortalecer la cultura organizacional, prevenir riesgos y garantizar el cumplimiento normativo.

En este contexto, como parte integrante del sistema de gestión de riesgos de la Sociedad, se planificarán programas de entrenamiento y capacitación, destinados a sensibilizar y educar al personal, en el uso de controles, detección y reporte de riesgos operacionales, financieros y/o normativos en sus actividades diarias, con objeto de que cada colaborador contribuya a disminuir la ocurrencia de eventos de riesgo y minimizar de esta forma, su impacto en el negocio.

Para apoyar lo anterior, se mantendrá constantemente publicado y actualizado este documento, que incluye las políticas y los procedimientos definidos para realizar la gestión de riesgos, así como también cualquier otro documento que tenga relación con los procesos de la Sociedad, los cuales deban ser co-

nocidos y aplicados por toda la organización.

Control de Versiones

Versión	Descripción de Cambio	Fecha
1.0	**Emisión inicial del Manual**	**24 de julio de 2024**
2.0	**Actualización integral al texto de la NCG 502 modificado por la NCG 524 (enrutamiento de órdenes), incorporación de los controles compensatorios del ECCI y remisión a la Política de Contratación y Remuneraciones. Aprobada por el Directorio.**	**6 de julio de 2026**

1. La definición legal está detallada en la ley N°19.628 sobre protección de datos personales. ↑