Primero. Objeto

El propósito de estas políticas es establecer las condiciones y lineamientos para el uso adecuado de la plataforma Sampi Suite Compliance (SSC), asegurando que su operación se realice conforme a los principios de cumplimiento normativo y las mejores prácticas corporativas.

Estas políticas buscan garantizar que la herramienta sea utilizada exclusivamente para la gestión integral de riesgos, controles y contrapartes, en el marco de programas de prevención de lavado de activos, financiación del terrorismo, soborno y corrupción, así como para dar cumplimiento a regulaciones locales e internacionales aplicables.

Asimismo, se pretende proteger la confidencialidad, integridad y disponibilidad de la información cargada en la plataforma, promoviendo un uso ético y responsable por parte de los usuarios autorizados. Todas las acciones realizadas deberán ser trazables y auditables, permitiendo evidenciar la correcta aplicación de las políticas internas y externas.

Finalmente, estas políticas establecen mecanismos de seguridad y control de acceso que previenen usos indebidos, garantizan la transparencia en la gestión y fortalecen la confianza en los procesos de cumplimiento que soporta la herramienta. Esta Política complementa, y no sustituye, la Política de Tratamiento de Datos Personales de Sampi Consultores S.A.S. (en adelante, la "Política de Datos"). En caso de conflicto, prevalecerá la Política de Datos y lo pactado en el contrato y/o Autorización de Tratamiento suscrito con el Cliente.

Segundo Alcance

Las presentes políticas aplican a todos los usuarios autorizados que accedan y operen la plataforma Sampi Suite Compliance (SSC), incluyendo personal interno, consultores externos y cualquier tercero que interactúe con el sistema bajo autorización expresa de la organización.
El alcance comprende todas las funcionalidades del sistema: gestión de riesgos, asignación y seguimiento de controles, administración de perfiles vinculados, monitoreo mediante Entity Watcher, generación de reportes y cualquier módulo adicional incorporado en la suite.

Estas políticas son obligatorias para todas las operaciones realizadas dentro de la plataforma, sin importar el dispositivo, ubicación o modalidad de acceso, y cubren tanto el uso cotidiano como las actividades de configuración, mantenimiento y soporte. Asimismo, se extienden a la protección de datos, trazabilidad de acciones y cumplimiento de normativas aplicables, garantizando que la herramienta se utilice exclusivamente para fines legítimos de prevención y control de riesgos corporativos.

Tercero Relación con la Política de Datos

Las Políticas de Uso de la plataforma Sampi Suite Compliance (SSC) están directamente vinculadas con la Política de Protección de Datos de la organización, dado que la herramienta gestiona información sensible de clientes, proveedores y contrapartes.

El cumplimiento de estas políticas implica que todo tratamiento de datos personales dentro del sistema se realice conforme a la normativa vigente (por ejemplo, Ley 1581 de 2012 en Colombia y estándares internacionales aplicables), garantizando los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Los usuarios deberán asegurarse de que la información cargada en la plataforma sea utilizada únicamente para los fines legítimos definidos en el marco de programas de cumplimiento y prevención de riesgos, evitando cualquier uso indebido, divulgación no autorizada o transferencia no permitida. En consecuencia, la adopción de estas políticas refuerza la responsabilidad compartida entre la organización y los usuarios para proteger los datos, mantener la trazabilidad de las acciones y garantizar la integridad del sistema frente a riesgos tecnológicos y normativos.

Cuarto. Definiciones operativas

1. Alertas Configurables: Notificaciones automáticas generadas por la plataforma ante la detección de riesgos críticos, variaciones en los perfiles de contrapartes o incumplimientos de políticas.

2. API (Interfaz de Programación de Aplicaciones): Conjunto de funciones, protocolos y herramientas que permiten la comunicación entre diferentes sistemas o aplicaciones para intercambiar datos o ejecutar funcionalidades.

3. Autenticación: Proceso mediante el cual la plataforma verifica la identidad de un usuario, servicio o dispositivo antes de otorgar acceso. Incluye métodos como contraseñas, autenticación multifactor (MFA), tokens o certificados digitales.

4. Autorización: Mecanismo que define los permisos y niveles de acceso otorgados a un usuario o proceso, una vez autenticado, según su rol o perfil dentro del sistema.

5. Calificación de Riesgos: Proceso mediante el cual se asigna un puntaje o nivel de riesgo considerando criterios como probabilidad, impacto y materialidad.

6. Cliente: Entidad contratante de la plataforma SSC, responsable de la administración de sus usuarios y del contenido gestionado dentro del sistema.

7. Configuración Mínima Segura: Conjunto de parámetros técnicos obligatorios que debe cumplir cualquier sistema, dispositivo o software para operar bajo condiciones seguras (por ejemplo: cifrado, contraseñas fuertes, parches actualizados).

8. Contenido del Cliente: Toda información, documento, dato o metadato cargado, transmitido o almacenado por el Cliente o sus usuarios dentro de la plataforma SSC.

9. Contraparte: Cliente, proveedor, aliado o cualquier tercero con el que la organización mantiene relaciones comerciales o contractuales y que debe ser evaluado en términos de riesgo.

10. Control: Medida preventiva, detectiva o correctiva implementada para mitigar o reducir la probabilidad e impacto de un riesgo identificado.

11. Controles IA Expert: Funcionalidad basada en inteligencia artificial que sugiere controles preventivos, detectivos o correctivos según el tipo de riesgo y la normativa aplicable.

12. Credenciales: Conjunto de datos utilizados para autenticar y autorizar a un usuario, tales como nombre de usuario, contraseña, MFA, tokens o llaves de API.

13. Cuenta de Usuario: Identificador único asignado a una persona o sistema que permite el acceso a la plataforma, sujeto a los permisos definidos por el Cliente o la organización.

14. Datos Personales: Información que identifica o permite identificar a una persona natural, tratada en la plataforma conforme a la normativa vigente de protección de datos personales.

15. Entity Watcher: Módulo de la plataforma encargado del monitoreo continuo y la verificación automática de contrapartes en listas restrictivas, PEP y otras fuentes oficiales.

16. Fair Use (Uso Justo): Principio que regula el uso razonable y proporcional de los servicios tecnológicos, evitando su explotación excesiva o que afecte la disponibilidad para otros usuarios.

17. Funcionalidades de IA (Inteligencia Artificial): Módulos, servicios o herramientas que utilizan algoritmos de aprendizaje automático, procesamiento de lenguaje natural u otros modelos inteligentes para ejecutar tareas automatizadas o asistidas.

18. Gestión de Incidentes de Seguridad: Conjunto de procedimientos para identificar, contener, mitigar, documentar y notificar eventos que afecten la confidencialidad, integridad o disponibilidad de los sistemas o datos.

19. Integraciones: Conexiones técnicas que permiten que la plataforma interactúe o comparta información con otros sistemas internos o externos mediante APIs, conectores o servicios interoperables.

20. Licenciamiento: Régimen jurídico y técnico que regula los derechos, condiciones y limitaciones sobre el uso del software, herramientas, contenidos o datos proporcionados por la organización o terceros.

21. Logs o Registros: Archivos o bases de datos donde se documentan cronológicamente las actividades, accesos, eventos y transacciones realizadas dentro de la plataforma.

22. Mantenimiento: Actividades programadas o correctivas destinadas a asegurar el funcionamiento continuo, seguro y actualizado de los sistemas o servicios.

23. Mapa de Calor de Riesgo: Representación gráfica que muestra la probabilidad e impacto de los riesgos identificados, facilitando la visualización del nivel de exposición inherente y residual.

24. Matriz de Riesgo Inherente: Herramienta que evalúa el nivel de riesgo antes de la aplicación de controles, considerando factores como probabilidad e impacto.

25. Matriz de Riesgo Residual: Evaluación del nivel de riesgo una vez aplicados los controles, reflejando la efectividad de las medidas implementadas.

26. Monitoreo: Actividad continua de supervisión de los sistemas, redes y servicios con el fin de detectar comportamientos anómalos, vulnerabilidades o incumplimientos de uso.

27. Plataforma Sampi Suite Compliance (SSC): Conjunto de módulos y funcionalidades tecnológicas diseñadas para la gestión integral de riesgos, controles y contrapartes, incluyendo herramientas de análisis, monitoreo, IA y trazabilidad.

28. Política de Uso: Documento que define las condiciones, responsabilidades y limitaciones aplicables al uso de los servicios, recursos tecnológicos e información bajo control de la organización.

29. Perfil Vinculado: Registro digital que contiene información detallada de clientes, proveedores o contrapartes, incluyendo datos básicos, clasificación de riesgo y resultados de screening.

30. Propiedad Intelectual: Derechos legales que protegen la autoría y titularidad de creaciones intelectuales, incluyendo software, marcas, contenido, bases de datos y modelos de IA.

31. Repositorio Documental: Espacio seguro dentro de la plataforma para almacenar documentos relacionados con cumplimiento, evidencias y reportes.

32. Riesgo: Evento potencial que puede afectar negativamente la operación, reputación o cumplimiento normativo de la organización.

33. Screening Automático: Proceso automatizado de verificación de contrapartes en listas restrictivas, PEP y otras fuentes oficiales, realizado por el módulo Entity Watcher.

34. Seguridad de la Información: Disciplina que garantiza la protección de la confidencialidad, integridad y disponibilidad de la información frente a amenazas internas o externas.

35. Servicio: Cualquier módulo, aplicación o funcionalidad tecnológica provista por la organización al Cliente o usuario autorizado bajo los términos de la política.

36. Suspensión o Terminación por Incumplimiento: Medida administrativa o técnica que implica restringir temporal o permanentemente el acceso o uso de los servicios debido al incumplimiento de las condiciones establecidas.

37. Trazabilidad: Capacidad de registrar, almacenar y auditar todas las acciones realizadas por usuarios o sistemas para fines de control, seguridad y cumplimiento normativo.

38. Usuario Autorizado: Persona natural o jurídica que cuenta con credenciales válidas y permisos otorgados por el Cliente o la organización para acceder y operar la plataforma SSC conforme a las políticas establecidas.

39. Vulnerabilidad: Debilidad en un sistema, aplicación o proceso que puede ser explotada para comprometer la seguridad o integridad de la información o de los servicios.

Quinto. Principios de uso

1. Principio de Uso Responsable y Ético. El uso de la SSC debe realizarse de manera ética, transparente y conforme a la legislación vigente, evitando cualquier manipulación, uso indebido o aprovechamiento del sistema para fines distintos a los autorizados por el Cliente o la

organización. Los usuarios deben actuar con integridad, asegurando que la información procesada sea veraz, completa y legítima.

2. Principio de Seguridad y Confidencialidad. Todo acceso y uso de la plataforma deberá realizarse bajo prácticas seguras que protejan la confidencialidad, integridad y disponibilidad de la información. Los usuarios deberán custodiar sus credenciales, cumplir con los controles técnicos y abstenerse de realizar acciones que puedan comprometer la seguridad del sistema o de los datos.

3. Principio de Legalidad y Cumplimiento Normativo. La utilización de la SSC se enmarca en el cumplimiento estricto de las normas legales, contractuales y regulatorias aplicables, incluyendo las relacionadas con la protección de datos personales, prevención del lavado de activos, financiación del terrorismo y demás obligaciones de cumplimiento que soporta la plataforma.

4. Principio de Integridad de la Información y Trazabilidad. Toda operación realizada en la SSC deberá garantizar la exactitud, completitud y trazabilidad de la información registrada. Los usuarios deben evitar la alteración, eliminación o registro de datos falsos, y permitir la auditoría y seguimiento de las acciones para mantener la transparencia operativa.

5. Principio de Limitación y Propósito de Uso. El acceso y uso de la plataforma, sus módulos e integraciones deberán limitarse estrictamente a los fines autorizados por la organización o el Cliente. Está prohibido el uso para actividades no relacionadas con la gestión de riesgos, cumplimiento o control de contrapartes, así como la extracción o reutilización de información con propósitos externos o no autorizados.

Sexto. Cuentas, acceso y autenticación

1. Creación y asignación de cuentas: Cada Usuario Autorizado deberá contar con una cuenta individual y no transferible, asignada por el Cliente o por la organización administradora de la SSC. La creación de cuentas estará sujeta a los procedimientos internos de aprobación y registro definidos por la entidad responsable del servicio. Las cuentas deberán vincularse a una identidad verificable y a un rol determinado dentro de la organización, garantizando la correcta segregación de funciones.

2. Uso personal e intransferible: Las cuentas y credenciales de acceso son de uso estrictamente personal. Queda prohibido compartir, transferir o delegar el uso de credenciales a terceros, aun dentro de la misma organización. Cualquier acción realizada bajo una cuenta se presumirá efectuada por el titular de la misma, siendo este responsable de las operaciones ejecutadas en la plataforma.

3. Autenticación y medidas de seguridad: El acceso a la SSC requerirá procesos de autenticación segura, que podrán incluir contraseñas robustas, autenticación multifactor (MFA), tokens de acceso u otros mecanismos equivalentes. La organización podrá exigir el cumplimiento de políticas de contraseñas seguras, como longitud mínima, complejidad, caducidad periódica y renovación obligatoria. El Usuario Autorizado deberá garantizar la confidencialidad de sus credenciales y notificar de inmediato cualquier sospecha de acceso indebido o pérdida de control sobre ellas.

4. Roles, permisos y niveles de acceso: La asignación de permisos se realizará bajo el principio de mínimo privilegio, otorgando a cada usuario únicamente los accesos estrictamente

necesarios para el desempeño de sus funciones. Los niveles de acceso podrán ser revisados, modificados o revocados en cualquier momento por motivos de seguridad, cambios de rol o incumplimiento de la política.

5. Suspensión, revocación y eliminación de cuentas: La organización o el Cliente podrán suspender temporal o definitivamente una cuenta cuando:

a) Se detecte uso indebido, intento de acceso no autorizado o incumplimiento de la política.
b) El usuario deje de tener relación contractual o laboral con el Cliente; o
c) existan razones de seguridad, mantenimiento o investigación de incidentes.
d) La eliminación de cuentas deberá realizarse conforme a los procedimientos de gestión de identidad y acceso (IAM) establecidos, preservando la trazabilidad y los registros de auditoría.
e) Responsabilidad del Cliente y del Usuario Autorizado El Cliente es responsable de la administración y control de las cuentas de sus usuarios, así como de asegurar que el acceso a la SSC se mantenga conforme a los principios de seguridad y confidencialidad. Cada Usuario Autorizado asume la obligación de custodiar sus credenciales y cumplir con los protocolos de autenticación establecidos.

Séptima Seguridad y configuración mínima

1. Principio de seguridad integral: La seguridad de la plataforma SSC, sus datos y usuarios es una responsabilidad compartida entre la organización, el Cliente y los Usuarios Autorizados. Toda operación deberá realizarse observando los principios de confidencialidad, integridad, disponibilidad y trazabilidad de la información. El incumplimiento de las medidas de seguridad podrá dar lugar a la suspensión o revocación del acceso, sin perjuicio de las acciones legales o contractuales aplicables.

2. Configuración mínima obligatoria de seguridad: Todo dispositivo, navegador, red o entorno desde el cual se acceda a la SSC deberá cumplir con una configuración técnica mínima que garantice un nivel adecuado de protección, incluyendo, entre otros:

- Sistema operativo actualizado y libre de software malicioso.
- Navegadores en versiones soportadas y con parches de seguridad vigentes.
- Cifrado de comunicaciones mediante protocolo HTTPS/TLS.
- Bloqueo automático de sesión tras períodos de inactividad.
- Contraseñas robustas conforme a los parámetros definidos por la organización.
- Activación obligatoria de autenticación multifactor (MFA) cuando esté disponible.
- Antivirus y firewall activos con actualizaciones automáticas habilitadas.
- La organización podrá actualizar o ampliar estos requisitos según las mejores prácticas o normas de seguridad de la información vigentes.

3. Protección de datos y cifrado: Toda información transmitida o almacenada en la SSC deberá estar protegida mediante mecanismos de cifrado y controles de acceso adecuados. Los datos personales y sensibles serán tratados conforme a la normativa aplicable de protección de datos personales, limitando su acceso únicamente a personal autorizado y para los fines expresamente permitidos.

4. Actualizaciones, parches y mantenimiento preventivo: La organización garantizará la aplicación oportuna de actualizaciones, parches de seguridad y mejoras técnicas necesarias

para mantener la integridad y disponibilidad del sistema. El Cliente y los Usuarios Autorizados deberán abstenerse de interferir, deshabilitar o eludir dichas actualizaciones. Los mantenimientos programados podrán implicar breves interrupciones del servicio, las cuales serán notificadas conforme a los canales oficiales de comunicación.

5. Gestión de dispositivos y entornos de acceso: El Cliente es responsable de asegurar que los equipos y redes desde los cuales sus usuarios acceden a la plataforma cumplan con las políticas internas de seguridad y los requisitos técnicos definidos. No se permite el acceso desde dispositivos o entornos no controlados, comprometidos o que utilicen configuraciones inseguras (por ejemplo, redes Wi-Fi públicas o equipos sin control de antivirus).

6. Monitoreo y detección de incidentes: La SSC cuenta con mecanismos de monitoreo continuo y detección de comportamientos anómalos para prevenir accesos no autorizados, filtraciones o vulneraciones. La organización podrá registrar, analizar y conservar trazas de auditoría (logs) con fines de seguridad, cumplimiento y respuesta ante incidentes. Cualquier anomalía o sospecha de brecha de seguridad deberá ser reportada de inmediato al canal oficial de soporte o al contacto designado por el Cliente.

7. Responsabilidad del Usuario Autorizado: Cada Usuario Autorizado deberá:

- Mantener la confidencialidad de su cuenta y credenciales.
- No instalar, modificar ni manipular software que interfiera con el funcionamiento de la SSC.
- Notificar de inmediato cualquier intento de acceso indebido o comportamiento sospechoso.
- Cumplir con los lineamientos técnicos de seguridad definidos por el Cliente y la organización.

Octavo. Uso aceptable y prácticas prohibidas

1. Principio general de uso aceptable: El uso de la Plataforma Sampi Suite Compliance (SSC) deberá efectuarse exclusivamente para los fines autorizados relacionados con la gestión de riesgos, cumplimiento, controles y contrapartes, conforme a las funciones, licencias y roles asignados a cada Usuario Autorizado. Toda actividad dentro de la SSC deberá respetar las políticas internas del Cliente, los términos contractuales, las leyes aplicables y los principios de ética, seguridad y confidencialidad.

2. Usos aceptables:

a) Se consideran usos aceptables de la plataforma aquellos que:
b) Contribuyan a la gestión legítima de riesgos, cumplimiento normativo y monitoreo de contrapartes.
c) Garanticen la veracidad, exactitud y trazabilidad de la información registrada o consultada.
d) Se realicen respetando las normas de seguridad establecidas, los niveles de acceso autorizados y las medidas de protección de datos.
e) Promuevan la eficiencia, integridad y transparencia en los procesos gestionados mediante la SSC.
f) Cumplan con las condiciones de licenciamiento, propiedad intelectual y uso justo (Fair Use) de los servicios tecnológicos provistos.

3. Prácticas prohibidas: Queda estrictamente prohibido el uso de la SSC, total o parcial, para cualquiera de los siguientes fines o conductas:

a) Intentar acceder, sin autorización, a cuentas, módulos, bases de datos o información de otros usuarios o del sistema.
b) Modificar, eliminar, copiar o interceptar información sin la debida autorización.
c) Suplantar la identidad de otro usuario o utilizar credenciales ajenas.
d) Instalar, distribuir o ejecutar software malicioso, scripts o herramientas diseñadas para alterar el funcionamiento de la plataforma.
e) Realizar pruebas de penetración, ingeniería inversa o cualquier acción que comprometa la integridad técnica de la SSC sin autorización previa y expresa de la organización.
f) Generar tráfico automatizado, ataques de denegación de servicio (DoS) o cualquier otra acción que afecte la disponibilidad del servicio.
g) Exportar, compartir o divulgar información contenida en la SSC sin la debida autorización del Cliente o de la organización.
h) Utilizar los datos procesados en la plataforma para fines distintos a los establecidos por la política o la relación contractual.
i) Alterar, falsificar o eliminar registros, evidencias o trazas de auditoría.
j) Violar derechos de propiedad intelectual, licencias de software o políticas de confidencialidad.
k) Utilizar la plataforma para actividades contrarias a la ley, incluyendo lavado de activos, fraude, manipulación de información o acceso no autorizado a datos personales.
l) Infringir la normativa de protección de datos personales o las políticas internas de cumplimiento.
m) Realizar acciones que deterioren la seguridad, estabilidad o reputación de la SSC o de la organización titular.
n) Usar el sistema para difundir contenido inapropiado, ofensivo, discriminatorio o que contravenga principios éticos o corporativos.
o) Uso de scripts o bots para realizar operaciones masivas fuera de los límites establecidos.
p) Intentos de eludir mecanismos de control de carga o autenticación.
q) Compartir credenciales para incrementar el volumen de operaciones más allá del permitido.
r) Copiar, reproducir, descompilar, modificar, traducir, adaptar, distribuir o crear obras derivadas de la SSC o de cualquiera de sus componentes.
s) Realizar ingeniería inversa, pruebas de penetración no autorizadas, o intentos de obtención del código fuente o de su lógica interna.
t) Utilizar la plataforma con fines distintos a los autorizados, o para prestar servicios a terceros sin consentimiento previo y escrito de la organización.
u) Eludir mecanismos de licenciamiento, autenticación o seguridad implementados en la SSC.

4. Monitoreo y verificación de cumplimiento: La organización y el Cliente se reservan el derecho de monitorear las actividades realizadas en la plataforma para garantizar el cumplimiento de esta política, así como para investigar y documentar cualquier conducta irregular. El uso de la SSC implica la aceptación de tales medidas de auditoría y monitoreo bajo los principios de legalidad, necesidad y proporcionalidad.

5. Consecuencias del incumplimiento: El incumplimiento de las disposiciones establecidas en esta sección podrá generar la suspensión temporal o definitiva del acceso, la revocación de licencias de uso, y la adopción de medidas disciplinarias y/o legales según la gravedad de la

infracción. La organización se reserva el derecho de reportar los incidentes que constituyan violaciones de ley a las autoridades competentes.

Novena. Propiedad intelectual y licenciamiento

1. Titularidad de derechos: La Plataforma Sampi Suite Compliance (SSC), incluyendo sus módulos, funcionalidades, interfaces, código fuente, estructuras de datos, diseños, modelos de inteligencia artificial, bases de conocimiento, documentación técnica y manuales de usuario, es de propiedad exclusiva de SAMPI CONSULTORES S.A.S., con NIT. 901661063, organización titular, quien conserva todos los derechos de propiedad intelectual, industrial y de autoría. Ninguna disposición de la presente política otorga al Cliente o a los Usuarios Autorizados derecho de propiedad, titularidad o participación sobre la SSC ni sobre sus componentes, salvo las licencias limitadas de uso aquí descritas.

2. Licencia de uso otorgada al Client: La organización concede al Cliente una licencia limitada, no exclusiva, intransferible, revocable y de alcance territorial definido, para acceder y utilizar la SSC con el único propósito de gestionar riesgos, controles, contrapartes y demás procesos asociados a sus actividades de cumplimiento. Dicha licencia:

a) Derecho de uso por subscripción.
b) Se encuentra condicionada al cumplimiento de los términos contractuales, técnicos y de seguridad establecidos por la organización.
c) Será válida únicamente durante el periodo de vigencia del contrato o suscripción correspondiente.

El Cliente conserva la titularidad y los derechos sobre el contenido que cargue, gestione o procese dentro de la SSC, incluyendo documentos, datos, registros, reportes y metadatos ("Contenido del Cliente"). La organización únicamente accederá o procesará dicho contenido en los siguientes casos:

a. Para la prestación y mantenimiento del servicio.
b. Para la mejora continua, monitoreo o soporte técnico autorizado.
c. Para el cumplimiento de obligaciones legales o regulatorias aplicables.

4. Condiciones de uso y licenciamiento: El Cliente declara que posee las autorizaciones necesarias para el tratamiento y uso de dicho contenido conforme a la ley y exime a la organización de cualquier responsabilidad derivada de su origen, exactitud o licitud. Cualquier desarrollo, módulo, mejora, personalización, funcionalidad adicional o actualización que sea incorporada a la SSC —ya sea por solicitud del Cliente o como evolución tecnológica propia— será de propiedad exclusiva de la organización, aun cuando haya sido financiada o co–diseñada por el Cliente, salvo pacto contractual expreso en contrario. La SSC puede incorporar o interoperar con componentes, bibliotecas o servicios de terceros licenciados bajo sus propios términos.

El Cliente y los Usuarios Autorizados aceptan cumplir con dichas condiciones y reconocen que su incumplimiento puede generar la suspensión del acceso o responsabilidades frente a los titulares de dichos derechos. La licencia otorgada al Cliente estará vigente durante el periodo contractual. Al término o rescisión del contrato, el acceso será revocado, y el Cliente deberá cesar todo uso de la SSC y de los materiales asociados. La organización conservará, por el tiempo estrictamente necesario, las trazas, registros y respaldos que sean requeridos para fines de

cumplimiento, auditoría o soporte a obligaciones legales. La organización podrá aplicar medidas técnicas y legales para proteger sus derechos sobre la SSC, incluyendo monitoreo, auditoría, restricciones de acceso y acciones judiciales o administrativas en caso de infracción. El uso de la SSC implica el reconocimiento expreso de estos derechos y la obligación de respetar las limitaciones establecidas en materia de propiedad intelectual y licenciamiento.

Decima. Integraciones y APIs. Las APIs (Application Programming Interfaces) son interfaces que permiten la comunicación segura entre la plataforma Sampi Suite Compliance (SSC) y sistemas externos, facilitando la interoperabilidad y el intercambio controlado de datos. Las integraciones se realizan bajo protocolos estandarizados (REST, HTTPS) y mecanismos de autenticación robustos (tokens, OAuth). Esta política regula el uso de APIs para conexión con sistemas internos del cliente (ERP, CRM, bases de datos). Integración con servicios externos (listas restrictivas, proveedores de screening, módulos de IA). Automatización de procesos mediante endpoints documentados. El cliente es responsable de la correcta configuración de sus integraciones y del cumplimiento de las políticas de seguridad en sus sistemas conectados.

Decimo Primero. Límites de uso y Fair Use Los límites de uso y la política de Fair Use establecen las condiciones técnicas y operativas que regulan la utilización de la plataforma Sampi Suite Compliance (SSC), garantizando un acceso equitativo, estable y seguro para todos los usuarios. El principio de Uso Justo (Fair Use) establece que todos los Clientes y Usuarios Autorizados deben utilizar los recursos tecnológicos, capacidad de procesamiento, almacenamiento, consultas automáticas y servicios en la nube de manera razonable, proporcional y equitativa.

Parámetros de Fair Use (ejemplos): La organización podrá establecer límites razonables en el volumen de procesamiento, número de usuarios simultáneos, frecuencia de consultas, tamaño de almacenamiento, transacciones por API o capacidad de integración, según el plan contratado y las condiciones técnicas del servicio.Dichos límites estarán definidos en la documentación técnica o en los acuerdos de nivel de servicio (SLA) y podrán ajustarse en función de la evolución tecnológica o contractual, como:

- Número máximo de consultas API por hora/día según el plan contratado.
- Tamaño máximo de archivos cargados en el Repositorio Documental (ej. 50 MB por archivo).
- Límite de perfiles vinculados por cuenta según la licencia.
- Restricciones en la frecuencia de screening automático para evitar saturación de listas externas.

Responsabilidad: El Cliente es responsable de garantizar que el uso de la SSC por parte de sus Usuarios Autorizados se mantenga dentro de los límites permitidos y conforme al principio de Uso Justo. Cualquier acción que suponga abuso, saturación del sistema o utilización indebida de recursos podrá considerarse un incumplimiento grave de la política de uso y del contrato de servicio, tales como. alertas, suspensión temporal del servicio o terminación del contrato, según la gravedad y reincidencia.

Decimo Segundo. Monitoreo y registros

El monitoreo y registro son procesos esenciales para garantizar la trazabilidad, transparencia y seguridad en el uso de la plataforma Sampi Suite Compliance (SSC). Incluyen la recopilación, almacenamiento y análisis de datos relacionados con las actividades realizadas por los usuarios

y los sistemas integrados. El monitoreo podrá realizarse de forma continua y automatizada, utilizando herramientas de auditoría y análisis de comportamiento (por ejemplo, detección de anomalías o correlación de eventos), conforme a las normas de seguridad y protección de datos aplicables. El monitoreo y registro aplican a todos los componentes de la SSC, incluyendo:

- Todas las acciones ejecutadas en la plataforma (creación, modificación, eliminación de riesgos, controles, perfiles y documentos).
- Accesos
- Autenticaciones y cambios en configuraciones.
- Interacciones con APIs e integraciones externas.
- Alertas generadas por el sistema, incluidas las relacionadas con riesgos críticos y screening automático.

Decimo Tercero Disponibilidad y mantenimiento

1. Disponibilidad del Servicio: La plataforma **Sampi Suite Compliance (SSC)** está diseñada para operar bajo estándares de alta disponibilidad, garantizando el acceso continuo y confiable a sus funcionalidades. La organización se compromete a mantener un nivel de disponibilidad conforme a los acuerdos de nivel de servicio (SLA) establecidos contractualmente, incluyendo:

- Disponibilidad mínima del servicio del **60%** mensual, excluyendo mantenimientos programados.
- Infraestructura alojada en entornos seguros y redundantes, con respaldo automático de datos.
- Monitoreo continuo de la plataforma para detectar y mitigar incidentes que puedan afectar la disponibilidad.

2. Mantenimiento Preventivo y Correctivo: La organización realizará actividades de mantenimiento técnico con el fin de preservar la estabilidad, seguridad y rendimiento de la SSC. Estas actividades incluyen:

- **Mantenimiento preventivo:** Aplicación periódica de actualizaciones, parches de seguridad, mejoras de rendimiento y ajustes de configuración.
- **Mantenimiento correctivo:** Intervenciones técnicas para resolver errores, vulnerabilidades o fallos detectados en la operación del sistema.

Los mantenimientos programados serán comunicados con al menos **48 horas de antelación**, indicando el alcance, duración estimada y posibles afectaciones al servicio. En casos de mantenimiento urgente o correctivo, se notificará a través de los canales oficiales tan pronto como sea posible.

3. Responsabilidad del Cliente y Usuarios Autorizados. El Cliente y sus Usuarios Autorizados deberán:

- Garantizar que los dispositivos y redes desde los cuales se accede a la SSC cumplan con los requisitos técnicos y de seguridad definidos.
- No interferir, deshabilitar ni obstaculizar los procesos de mantenimiento, actualizaciones o monitoreo del sistema.
- Reportar de manera inmediata cualquier incidente, falla o comportamiento anómalo al canal oficial de soporte.

Décimo Cuarto. Soporte Técnico y Atención al Cliente

1. Alcance del Soporte Técnico: La organización proveerá servicios de soporte técnico para garantizar el funcionamiento adecuado de la plataforma Sampi Suite Compliance (SSC), destinado exclusivamente para la resolución de incidentes técnicos relacionados con el acceso, operación o configuración de la plataforma, atención a consultas funcionales sobre el uso de módulos, reportes, controles y herramientas de IA., asistencia en la integración de APIs, configuración de alertas y personalización de funcionalidades según el plan contratado.

2. Canales de Atención: El soporte técnico estará disponible a través de los canales oficiales definidos por la organización, tales como:

- Correo electrónico: ruben.zapata@sampiconsultores.com
- Línea telefónica directa: 3057891389.
- Portal de soporte en línea en la pagina de soporte de www.sampiconsultores.com con base de conocimiento y manuales de usuario.

Los canales estarán activos en horarios hábiles definidos contractualmente, y podrán incluir atención prioritaria según el nivel de criticidad del incidente reportado.

3. Niveles de Servicio (SLA): La organización se compromete a mantener trazabilidad de cada solicitud, garantizando seguimiento, cierre documentado y retroalimentación al Cliente. El soporte técnico se regirá por acuerdos de nivel de servicio (SLA) que establecen:

- Tiempos de respuesta según la severidad del incidente (crítico, alto, medio, bajo).
- Tiempos de resolución estimados para cada tipo de solicitud.
- Escalamiento técnico en caso de requerimientos complejos o fallas persistentes.

4. Responsabilidades del Cliente y Usuarios Autorizados: Para facilitar una atención efectiva, el Cliente y sus Usuarios Autorizados deberán:

- Reportar los incidentes de forma clara, incluyendo evidencia, descripción del problema y pasos realizados.
- No realizar intervenciones técnicas no autorizadas que puedan alterar el funcionamiento de la SSC.
- Colaborar con el equipo de soporte en la validación de soluciones y pruebas de corrección.

5. Actualizaciones y Comunicaciones: Toda actualización técnica, mantenimiento programado o cambio relevante en la plataforma será comunicado por el canal oficial de soporte, incluyendo:

- Fecha y hora estimada de intervención.
- Módulos afectados y duración prevista.
- Recomendaciones para mitigar impactos operativos.

Décimo Quinto. Gestión de Incidentes de Seguridad

Se entiende por incidente de seguridad cualquier evento que comprometa, o tenga el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información, los sistemas o los servicios provistos por la plataforma Sampi Suite Compliance (SSC). Esto incluye accesos no autorizados, pérdida de datos, fallos técnicos, vulnerabilidades explotadas,

comportamientos anómalos o cualquier actividad que infrinja las políticas de seguridad establecidas.

1. Procedimientos de Gestión: La organización implementará un conjunto de procedimientos estructurados para la gestión de incidentes, que incluyen:

- Identificación: Detección temprana de eventos mediante monitoreo continuo, alertas automáticas y reportes de usuarios.
- Contención: Acciones inmediatas para limitar el alcance del incidente y evitar su propagación.
- Mitigación: Aplicación de medidas técnicas y operativas para reducir el impacto del incidente.
- Resolución: Corrección de la causa raíz y restauración de los servicios afectados.
- Documentación: Registro detallado del incidente, acciones tomadas, análisis forense y lecciones aprendidas.
- Notificación: Comunicación al Cliente y, cuando aplique, a las autoridades competentes conforme a la normativa vigente.

2.. Responsabilidades: La organización es responsable de coordinar la respuesta ante incidentes, mantener los protocolos actualizados y garantizar la trazabilidad de las acciones. Por su parte El Cliente deberá reportar de forma inmediata cualquier sospecha o evidencia de incidente a través del canal oficial de soporte y los autorizados deberán colaborar en la investigación, abstenerse de realizar acciones que agraven el incidente y seguir las instrucciones del equipo técnico.

3.. Comunicación y Transparencia: En caso de incidentes que afecten la operación del Cliente o la seguridad de los datos, la organización se compromete a:

- Informar oportunamente sobre la naturaleza del incidente, su impacto y las medidas adoptadas.
- Mantener la confidencialidad de la información involucrada, salvo obligación legal de divulgación.

Décimo Sexto. Funcionalidades de Inteligencia Artificial (IA)

La plataforma Sampi Suite Compliance (SSC) incorpora funcionalidades de Inteligencia Artificial (IA) con el objetivo de fortalecer la gestión de riesgos, el cumplimiento normativo y la toma de decisiones estratégicas. Estas herramientas están diseñadas para asistir a los usuarios en la identificación, evaluación y mitigación de riesgos relacionados con LA/FT, corrupción, fraude y otros delitos financieros. Las funcionalidades de IA incluyen, pero no se limitan a:

- Análisis automatizado de riesgos: Evaluación de probabilidades e impactos con base en datos históricos, sectoriales y comportamientos registrados.
- Generación de controles inteligentes: Sugerencia de controles específicos según el tipo de riesgo, área involucrada y nivel de vulnerabilidad.
- Mapas de calor y matrices de riesgo residual: Visualización dinámica del estado de los riesgos y efectividad de los controles.
- Alertas tempranas: Identificación de señales de alerta mediante patrones de comportamiento, listas restrictivas y datos transaccionales.

- Clasificación automática de contrapartes: Segmentación de clientes y proveedores según nivel de riesgo, sector económico y ubicación.
- Asistente legal inteligente: Apoyo en la redacción de estrategias de mitigación, cláusulas contractuales y recomendaciones normativas.
- Carga y visualización de controles IA Expert: Acceso rápido a controles recomendados por el sistema, con posibilidad de personalización.

3. Uso Responsable y Limitaciones
- Las funcionalidades de IA son herramientas de apoyo y no sustituyen el juicio profesional ni la validación humana.
- El Cliente es responsable de revisar, validar y complementar las recomendaciones generadas por la IA antes de su implementación.
- La organización no se hace responsable por decisiones tomadas exclusivamente con base en los resultados de la IA sin revisión técnica o legal.

4. Actualización y Mejora Continua: Las funcionalidades de IA serán actualizadas periódicamente para incorporar mejoras técnicas, nuevos modelos de análisis y ajustes conforme a cambios regulatorios. El Cliente será informado de estas actualizaciones mediante los canales oficiales.

5. Privacidad y Seguridad de Datos Toda información procesada por los módulos de IA será tratada conforme a las políticas de privacidad y seguridad de la plataforma, garantizando la confidencialidad, integridad y trazabilidad de los datos utilizados.

Décimo Séptimo. Contenido del Cliente

Se entiende por **Contenido del Cliente** toda la información, documentación, datos, registros, formularios, reportes, configuraciones, listas de contrapartes, matrices de riesgo, controles, evidencias y demás elementos que el Cliente ingrese, cargue, procese o gestione dentro de la plataforma Sampi Suite Compliance (SSC), en particular deberá:

- El Cliente es el único responsable de la veracidad, legalidad, integridad y actualización del contenido que incorpora en la plataforma.
- La organización no se responsabiliza por errores, omisiones o falsedades en el contenido proporcionado por el Cliente.
- El Cliente deberá garantizar que el contenido no infringe derechos de terceros ni disposiciones legales vigentes.
- El Cliente podrá conservar, modificar o eliminar su contenido conforme a sus necesidades operativas.
- La organización podrá conservar copias de seguridad del contenido por motivos técnicos, legales o de auditoría, conforme a los plazos definidos en la política de retención de datos.
- El Cliente podrá registrar información detallada de sus contrapartes (clientes, proveedores, socios), incluyendo datos de identificación, sector, ubicación, activos, reportes y segmentación de riesgo.
- La plataforma permite la visualización, edición y análisis de estas contrapartes mediante formularios, tablas y mapas de calor.

19. Suspensión y terminación por incumplimiento SSC podrá suspender o restringir el acceso cuando existan indicios de uso ilícito, violaciones graves de esta Política, riesgo para la seguridad/estabilidad, fraude o por orden de autoridad. De ser razonable, se ofrecerá ventana de remediación.

Décimo Octavo. Cambios a la Política

La organización se reserva el derecho de modificar, actualizar o complementar esta Política de Uso en cualquier momento, con el fin de adaptarla a cambios normativos, mejoras tecnológicas, evolución de los servicios o necesidades operativas. Toda modificación será comunicada al Cliente por los canales oficiales establecidos, indicando la fecha de entrada en vigor, el alcance de los cambios y las implicaciones para los usuarios autorizados. El uso continuado de la plataforma Sampi Suite Compliance (SSC) después de la publicación de los cambios se considerará como aceptación expresa de los mismos.

El Cliente podrá solicitar aclaraciones o expresar observaciones sobre las modificaciones propuestas, dentro de los plazos definidos en la comunicación oficial. En caso de que los cambios afecten condiciones contractuales esenciales, se podrá acordar su incorporación mediante adenda o ajuste contractual. La versión vigente de la Política de Uso estará disponible en el portal oficial de la organización o en el entorno de administración de la SSC.

Décimo Noveno. Ley y Jurisdicción Aplicable

Esta Política de Uso se rige por las leyes de la República de Colombia, incluyendo, pero sin limitarse a, las disposiciones sobre protección de datos personales, propiedad intelectual, comercio electrónico y cumplimiento normativo. En caso de conflicto, controversia o interpretación relacionada con el uso de la plataforma SSC, las partes acuerdan someterse a la jurisdicción de los jueces de la ciudad de Bogotá D.C., renunciando expresamente a cualquier otro fuero que pudiera corresponderles por razón de su domicilio presente o futuro.

Sin perjuicio de lo anterior, las partes podrán optar por mecanismos alternativos de solución de controversias, tales como la conciliación o el arbitraje, conforme a lo pactado en el contrato principal o en acuerdos específicos. La interpretación de esta política deberá realizarse en armonía con el contrato de prestación de servicios, la Política de Tratamiento de Datos Personales y demás documentos vinculantes suscritos entre el Cliente y la organización.

Vigencia y Aceptación

La presente Política de Uso entra en vigor a partir de la fecha de su publicación y permanecerá vigente mientras el Cliente mantenga una relación contractual activa con la organización. Su aceptación es condición necesaria para el acceso y utilización de la plataforma SSC, y se entiende como aceptada al momento de la firma del contrato principal, la activación del servicio o el uso continuado de la solución. La organización y el Cliente reconocen que esta política forma parte integral del marco contractual que regula la prestación del servicio, y que su cumplimiento es esencial para garantizar la seguridad, eficiencia y legalidad en el uso de la plataforma. Cualquier disposición no prevista en este documento será interpretada conforme a los principios de buena fe, equidad y cumplimiento normativo aplicable.