REGISTRO DE REVISIONES

Número de Revisión	Fecha	Sección	Cambios Realizados
00	2018/04/16	Todo el documento	Creación de la política
01	2020/07/23	2, 4.3, 4.7, 4.9, 4.11 y glosario	2. Cambio en el área que aprueba la política (antes la Junta Directiva ahora, el Comité de Auditoría), y las responsabilidades de la Dirección de Riesgos y Cumplimiento de la Información. 4.3 Se incluyen los aspectos relacionados de protección sin importar desde donde se accede a la información. 4.7 Se incluye el estudio de seguridad. 4.9 Se modifica el término plan de capacitación por programa de cultura. 4.11 Se incluye el término de Ciberseguridad Glosario, se incluyen definiciones de Seguridad de la Información y Ciberseguridad.
02	2022/04/01	Todo el documento	Cambio en el nombre de la compañía a Investment Vehicle 1 Limited.
03	2022/11/10	Todo el documento	Cambio en la responsabilidad del Comité de Auditoría; cambio en el nombre de la Dirección de Riesgos y Cumplimiento de la Información e inclusión de nuevas responsabilidades; alineación con los criterios de clasificación de la información; actualización de las referencias documentales.
03	2023/10/26	Todo el documento	Se revisó el documento y no se realizaron modificaciones.
03	2024/06/24	Todo el documento	Se revisó el documento y no se realizaron modificaciones.
04	2025/04/30	Todo el documento	Se revisó el documento y no se realizaron modificaciones.
05	2025/10/03	2.2., 2.3., 3.6. 3.10, 3.12 Glosario y documentos referenciados	• Ajustes o nuevas funciones o responsabilidades de la Dirección de Riesgos y cumplimiento y La Organización, sus funcionarios, directores, empleados (directos o subcontratados) y terceros vinculados (proveedores y contratistas). • Cambio del término de colaboradores por empleados

			• Se incluyeron lineamientos o conceptos asociados a: Inteligencia artificial, Sistema de Gestión de seguridad de la Información, Continuidad del negocio, trabajo remoto, protección a la cadena de suministro de terceros, identidad digital, obsolecencia tecnológica. • Actualización de documentos de referencia.

CONTENIDO

1. OBJETIVO Y ALCANCE

1.1 Objetivo

Esta política tiene como objetivo establecer los lineamientos de seguridad de la información y ciberseguridad requeridos para la protección de la información de Investment Vehicle 1 Limited ("la Compañía") y de cualquiera de sus subsidiarias (la "Organización"), frente a situaciones que puedan afectar la Confidencialidad, Integridad y Disponibilidad (como se definen a continuación) de la información de la Organización y que puedan causar impacto financiero, legal, competitivo y/o reputacional en la Organización.

1.2 Alcance

El alcance incluye toda la información y recursos de valor (Tecnologías de información y de las comunicaciones -TICs-, Instalaciones, y Tecnologías operacionales -OTs-) asociados o que pertenezcan a la Organización o que sean gestionados por Terceros vinculados (proveedores y contratistas), independiente del formato, medio, en todas sus formas (digital, manuscrita, hablada, impresa), presentación y/o lugar en el que ésta se encuentre ubicada, incluido el ciberespacio.

2. RESPONSABILIDADES

La Dirección de Riesgos y Cumplimiento de la Información, es el área responsable de formular la Política, divulgarla, revisarla mínimo una vez al año y de mantenerla actualizada; monitorear que se cumpla, en concordancia con la misión y visión de la Organización, y el cumplimiento de las regulaciones aplicables a la Organización, reportando al Comité de Auditoría de la Compañía (el "Comité de Auditoría") los asuntos relevantes sobre Seguridad de la Información y Ciberseguridad.

En el gobierno de Seguridad de la Información y Ciberseguridad participan distintas instancias en todas las compañías descritas en el alcance, las cuales tiene las siguientes responsabilidades:

2.1. Aprobación de política

El Comité de Auditoría es el responsable de ratificar la presente política y sus actualizaciones, hacer seguimiento al perfil de riesgos de la información, promover la cultura de seguridad de la Información y Ciberseguridad, fomentar el cumplimiento de sus lineamientos, asignar los recursos para el cumplimiento, así como hacer seguimiento general al cumplimiento de la presente Política.

La Dirección de Riesgos y Cumplimiento de la Información tiene autoridad para gestionar la revisión de la Política y su presentación al Comité de Auditoría para su ratificación.

2.2. Funciones de la Dirección de Riesgos y Cumplimiento de la Información

- Definir el alcance del programa de Seguridad de la Información y Ciberseguridad para proteger la confidencialidad, integridad y disponibilidad de la información de la compañía,

asegurando el cumplimiento normativo e implementando buenas prácticas y metodologías de reconocido valor técnico aplicables a la industria.

- Propender por la gestión efectiva de los riesgos cibernéticos y de seguridad de la Información, a través de la identificación, análisis, evaluación y tratamiento de estos.
- Definir procesos para la actualización permanente de las novedades de los marcos normativos relacionados con la Seguridad de la Información y Ciberseguridad.
- Soportar en la atención y respuesta de las alertas e incidentes de seguridad de la información y ciberseguridad identificados por los empleados, terceros vinculados y derivado del monitoreo hecho a través de las plataformas de gestión de seguridad de la información que afecten los procesos, recursos tecnológicos y sistemas de la Organización.
- Definir un programa de gestión de la recuperación tecnológica con el fin de garantizar la disponibilidad y continuidad de las operaciones definidas a través del BIA (Business Impact Analysis) como críticas del negocio, ante eventuales interrupciones.
- Con el apoyo de la Dirección Jurídica hacer seguimiento al nivel de cumplimiento de las leyes y normatividad aplicable sobre la Seguridad de la Información y Ciberseguridad.
- Monitorear que se cumpla el programa y Sistema de Gestión de Seguridad de la Información y Ciberseguridad, en concordancia con la misión y visión de la Organización, y el cumplimiento de las regulaciones aplicables a cada una de sus compañías.
- A través de la Dirección Jurídica, establecer y mantener contactos con las autoridades, grupos especiales o de interés pertinentes a la seguridad de la información de seguridad y ciberseguridad.
- Soportar a la Organización en las acciones para la implementación de medidas o controles para el cumplimiento de la presente política.

2.3. La Organización, sus funcionarios, directores, empleados (directos o subcontratados) y terceros vinculados (proveedores y contratistas) que tengan acceso a la información de la organización, ya sea de manera habitual u ocasional, en el desarrollo de sus funciones, son responsables de:

- Conocer y cumplir la presente Política, junto con cualquier manual, procedimiento o instructivo establecidos para la aplicación de esta y mencionados al final del documento.
- La implementación de la Política junto con cualquier manual, procedimiento o instructivo establecidos para la aplicación de esta.
- Asumir la gestión del riesgo del manejo de la información de la Organización y la implementación de las acciones pertinentes para su mitigación.
- Considerar los requisitos de Seguridad de la Información y Ciberseguridad en sus procesos, iniciativas, proyectos y contrataciones.
- Identificar y reportar a la Dirección de Riesgos y Cumplimiento de la Información los eventos potenciales o incidentes que amenacen o puedan poner en riesgo la información corporativa o el cumplimiento de las políticas y/o procedimientos de seguridad de la información.
- Hacer seguimiento al nivel de cumplimiento de las leyes y normatividad aplicable sobre la Seguridad de la información y Ciberseguridad.
- Usar los recursos tecnológicos o la información de la organización, de forma responsable, en ambientes o aplicaciones aprobadas por la CIO (incluye las relacionadas con la IA) y únicamente para propósitos autorizados.
- Identificar y alertar a la Dirección de Riesgos y Cumplimiento de la Información las ciber amenazas y ciber riesgos actuales y emergentes que puedan afectar a la organización.
- Cumplir con las prácticas de la Organización para el uso adecuado y seguro de información o herramientas para la autenticación (contraseñas, código de accesos, MFA, Passwordless).
- Gestionar las identidades digitales y asignar los mínimos privilegios para el acceso a la información en sus diferentes medios y de acuerdo con las responsabilidades; así como

solicitar la eliminación de manera oportuna de las identidades digitales y accesos cuando no son necesarios.

- Los líderes de los procesos deben garantizar que estos cumplan con el principio de segregación de funciones, con el fin de minimizar el riesgo de concentrar las responsabilidades críticas en una sola persona.
- Definir planes de contingencia operativa o tecnológica necesarios para mantener la continuidad de los procesos o servicios críticos de la compañía. Estos deben ser probados periodicamente para mantenerlos efectivos.

3. CONTENIDO

- **Aspectos generales y específicos de la política.**

3.1 La Organización, reconoce que la información es un insumo indispensable para la ejecución de los procesos, la toma de decisiones en el desarrollo de los objetivos del negocio y para el diseño y definición de los productos y servicios que constituyen el factor diferenciador de lo que somos frente a nuestros clientes, empleados y asociados. Reconoce también la importancia de prevenir los riesgos de seguridad de la información y ciberseguridad durante todo su ciclo de vida; tal protección está enmarcada por 3 propiedades:

- **Confidencialidad**: La información no debe ponerse a disposición o ser revelada a individuos, entidades o en procesos no autorizados.
- **Integridad**: Se debe preservar la exactitud, confiabilidad y completitud de la información.
- **Disponibilidad**: La información debe ser accesible y utilizable cuando sea solicitada por un individuo, área o proceso autorizado y en el momento que se requiera.

3.2 Se debe identificar la información y los recursos de valor asociados a la información que la Organización utilice para el desarrollo de sus objetivos de negocio; la información y demás recursos asociados deben tener asignado un responsable, quien debe tomar las decisiones que son pertinentes para su protección, de acuerdo con los requerimientos internos y regulaciones aplicables a cada compañía.

3.3 Toda la información, independientemente del medio en el que se encuentre o ubicación de donde se acceda, debe estar clasificada para establecer su sensibilidad (el nivel de reserva que se debe mantener sobre su contenido) y su criticidad (el nivel de disponibilidad requerido para que no se interrumpan las operaciones del negocio). Es responsabilidad de todos los miembros de la Organización conocer la clasificación de la información que utilizan para el desarrollo de sus actividades; y de los responsables de los procesos de definir los controles para proteger la información de acuerdo con la clasificación que maneje cada Compañía que hace parte de la Organización.

3.4 La Organización identifica como información confidencial o privilegiada, la siguiente información, entre otras, dado que la definición de información confidencial debe hacerse caso por caso:

- Acciones en la bolsa de valores, información estratégica y financiera, información sobre alianzas estratégicas, reportes sobre proyecciones, resultados y/o revelaciones financieras.
- Información relativa a clientes, empleados, accionistas, terceros vinculados, contratistas, proveedores, viajeros, usuarios, inversionistas.
- Información privilegiada por acontecimientos importantes y confidenciales de la empresa.
- Información no pública material. Estos son algunos ejemplos, Información de fusión, proyectos estratégicos, enajenación, cambio en política de dividendos, información de socios comerciales, información sobre accionistas, entre otros.
- Información de negocios que la Organización está obligada a proteger, patentes, invenciones, acuerdos comerciales, contratos, código fuente de desarrollo de software u otra que tenga el potencial para proporcionar ventaja competitiva.
- Las prácticas para optimizar los ingresos, precios, tarifas netas.
- Información de la operación y sus procesos asociados.
- Informes de seguridad, riesgos, cumplimiento, auditoría interna y externa, incidentes operacionales, incidentes de seguridad de la información y ciberseguridad, investigaciones y asuntos legales relacionados con cualquiera de los anteriores.
- Informes de o para organismos reguladores que incluya información confidencial.
- Claves, pines, contraseñas o información de usuarios de red y/o aplicaciones corporativas.
- Información sujeta a leyes de protección de datos personales (incluye dato de tarjetas de pago) en las distintas jurisdicciones en las que la Organización está ubicada o desarrolla su actividad.

La información mencionada anteriormente, y cualquier otra que por su clasificación sea considerada como información confidencial o privilegiada no podrá ser utilizada en beneficio personal de ningún administrador, empleado o tercero vinculado que tenga acceso a la misma, ni para fines distintos de los inicialmente previstos para dicha información.

3.5 Es deber de todos los responsables de los procesos, líderes de proyectos o iniciativas y administradores de contratos, asegurar que los riesgos de la información sean identificados, analizados, evaluados, tratados y monitoreados, de acuerdo con los procedimientos de la Dirección de Riesgos y Cumplimiento de la Información, asegurando que los correspondientes riesgos se mantengan dentro de los niveles de riesgo aceptable por la Organización conforme a lo estipulado en el siguiente documento: MA_AVSG04_054 MANUAL DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN.

3.6 Los recursos de información como: equipos, aplicaciones de negocio, servicios de Internet, Intranet, herramientas colaborativas (correo electrónico, chat, almacenamiento en la nube), entre otros; son provistos a todos los empleados de la Organización para uso exclusivo de la Organización. El acceso y uso de estos, debe ser autorizado por el responsable de cada uno de los recursos y de acuerdo con las responsabilidades de su función. Los recursos de información deben devolverse de inmediato al administrador cuando ya no se necesiten.

3.7 La Organización debe garantizar que sus empleados, cualquier funcionario, gerente o cualquier persona apliquen medidas de seguridad de la información tales como, y sin limitarse a: verificaciones e investigaciones sobre referencias personales, laborales, experiencia laboral, pruebas complementarias, estudio de seguridad, examen de aptitud y conocimientos, de tal manera que apoyen las políticas de seguridad y en cumplimiento de las regulaciones locales.

3.8 Todos los empleados y terceros vinculados se entienden obligados al manejo de la confidencialidad de la información de la Organización independiente que tengan o no firmado un acuerdo de confidencialidad en el momento en que ingresan a la Organización; y son responsables de la reserva de la información inclusive después de finalizada su relación con la Organización.

3.9 La Organización deberá contar con un programa de cultura permanente en Seguridad de la Información y ciberseguridad que permita mantener a todo su personal informado acerca de las políticas, las responsabilidades de seguridad de la información y las continuas amenazas que ponen en riesgo la información que administra y/o procesa.

3.10 Los responsables de los contratos y de la contratación, deben garantizar que las responsabilidades de seguridad de la información de los terceros y su cadena de suministro, que tengan acceso, procesen, almacenen o distribuyan información de valor para la Organización, se encuentren documentadas en los contratos u otros acuerdos de prestación de servicios y deben supervisar su cumplimiento durante toda la vigencia de la relación contractual.

3.11 Es deber de toda La Organización y terceros vinculados reportar cualquier sospecha, condición anormal o violación a las políticas, responsabilidades y procedimientos de Seguridad de la Información y Ciberseguridad que atenten contra la Confidencialidad, Integridad y Disponibilidad de la información de La Organización de manera inmediata a través de los canales establecidos por la Organización.

En el caso de que las situaciones descritas anteriormente, afecten o tengan la posibilidad de afectar o tener algún impacto económico, material, de reputación, legal u operacional para la Organización, deberán ser reportados inmediatamente a la Dirección de Riesgos y Cumplimiento de la Información a través de los canales establecidos por ésta.

La Dirección de Riesgos y Cumplimiento de la Información deberá evaluar los reportes de incidentes y determinar si los mismos cumplen con el criterio de materialidad, caso en el cual deberá informar a la Dirección de Relaciones con el Inversionista para que dé cumplimiento a la Política de Revelación de Información Relevante Financiera y No Financiera para los Accionistas, Mercado, Grupos de Interés y Terceros Interesados.

3.12 La Organización tiene la responsabilidad de implementar lineamientos y medidas técnicas para la protección de la información que se almacena, procesa o transmite; de acuerdo con su clasificación y considerando, pero sin limitarse a:

- Gestión de Riesgos de la Información.
- Identificación y clasificación de activos de información.
- Controles para el almacenamiento y transferencia segura de datos.
- Protección contra amenazas, como software malicioso y/o posibles ataques informáticos.
- Gestión de identidades digitales y control de acceso a la información, las aplicaciones, infraestructura y redes.
- Gestión de seguridad en dispositivos móviles/portátiles propios o personales al servicio de la Organización.
- Uso adecuado de los recursos asignados por la organización (internet, dispositivos tecnológicos corporativos, sitios colaborativos: Sharepoint, Onedrive, Teams, correo, otros).
- Seguridad en redes y telecomunicaciones.
- Seguridad en la adquisición, desarrollo y mantenimiento de recursos tecnológicos (incluyendo sistemas y ambientes de procesamiento, y gestión de la obsolescencia tecnológica).
- Gestión de medios de almacenamiento removible.
- Seguridad en el personal interno y terceros vinculados.
- Gestión de vulnerabilidades técnicas.
- Seguridad en la nube.
- Gestión de logs, eventos e incidentes de seguridad.
- Seguridad física y ambiental en centros de procesamiento de datos o sitios críticos.
- Controles para la instalación, desarrollo y almacenamiento de software.
- Continuidad del negocio, respaldo de información y recuperación de las plataformas tecnológicas en caso de desastres.
- Trabajo remoto o fuera de las instalaciones.
- Uso o desarrollo responsable de las tecnologías de Inteligencia artificial (IA).

3.13 La Dirección de Riesgos y Cumplimiento de la Información, podrá realizar actividades de monitoreo y auditoría en cualquier compañía de la Organización, de manera exclusiva, para determinar el nivel de cumplimiento de los lineamientos establecidos en esta política. Incluyendo terceros y compañías subcontratadas que brinden servicios de gestión, monitoreo, administración de plataformas tecnológicas de Investment Vehicle 1 Limited technology.

- **Regulación legal vigente aplicable a la política.**

3.14 La Organización, su Junta Directiva y su grupo ejecutivo deben comprometerse con el cumplimiento de los requisitos de seguridad de la información establecidos en sus políticas internas de seguridad, así como los solicitados por las leyes y regulaciones aplicables, tales como y sin limitarse a: SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standards), leyes internacionales de protección de datos personales, regulaciones del sector aeronáutico, acuerdos de industria o contractuales, licenciamiento, propiedad intelectual y demás referentes a la Seguridad de la Información y Ciberseguridad.

3.15 En caso de incumplimiento a la Política y/o procedimientos de seguridad establecidos o subsecuentes, la Organización adelantará las acciones legales, administrativas y/o disciplinarias que sean procedentes; de acuerdo con lo previsto en el Reglamento interno de cada una de sus compañías y/o las leyes y regulaciones de seguridad de la información, ciberseguridad y protección de datos personales internacionales y/o locales aplicables.

- **Fecha de efectividad de la política.**

3.16 Esta política entra en vigor a partir del momento de su publicación y se entiende vigente de manera indefinida a menos que se modifique para actualizarla de acuerdo con los cambios en el entorno organizacional, las circunstancias del negocio y/o las condiciones legales. En lo que respecta a terceros vinculados la política entrará a regir cuando se obtengan las autorizaciones correspondientes (firmas de contratos).

- **Prevalencia.**

3.17 En caso de conflicto entre los protocolos de la Junta Directiva, el acuerdo de los Inversionistas y la presente Política, el orden de precedencia de los documentos será el siguiente (i) el acuerdo de los inversionistas, (ii) los protocolos de la Junta Directiva, (iii) la presente Política.

- **Glosario.**

Acuerdo de inversionistas: Acuerdo de los accionistas de la compañía.

Cadena de suministro: En el entorno de la seguridad de la información es el conjunto de procesos, organizaciones, personas, actividades, tecnologías y terceros vinculados (proveedores, socios y contratistas) involucrados en el ciclo de vida de productos, servicios o información, cuyo adecuado funcionamiento, confianza y protección es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información de la organización.

Centro de Procesamiento de Datos (Data Center): Sitio físico o en la nube (virtual) para mantener la infraestructura tecnológica y electrónica, donde se procesa la información necesaria para la ejecución de los procesos de la Organización.

Ciber espacio: Entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física. (Superintendencia Financiera Circular externa 007, 2018)

Ciber seguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad. (Superintendencia Financiera Circular externa 007, 2018)

IA: Inteligencia Artificial.

Identidad: Se refiere a la identificación de personas en las aplicaciones de la organización. Para empleados, la identidad está registrada en SAP SSFF (SuccessFactors) y se reconoce por el número de empleado. En el caso de terceros vinculados, las identidades se registran en el Máster terceros de la herramienta de Gestión de Identidades y se reconocen por el número de identificación; en países donde la legislación de datos personales lo requiera, se empleará otro dato, como licencias de conducción, número tributario u otro identificador permitido. Para crear un usuario en una aplicación, es imprescindible que la identidad esté registrada y activa.

Identidad Digital: Conjunto de información sobre una persona que existe en el entorno digital y que permite identificarla de forma única.

Incidente de ciber seguridad: Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio. (Superintendencia Financiera Circular externa 007, 2018)

Programa de seguridad de la información y ciberseguridad: Conjunto de políticas, estrategias, metodologías, recursos, soluciones tecnológicas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacena, reproduce o procesa en los sistemas informáticos u otros medios de la entidad. (Superintendencia Financiera Circular externa 007, 2018)

Protocolo Junta Directiva: Protocolos de la Junta Directiva de la compañía.

Riesgo (NTC-ISO31000): Efecto de la incertidumbre sobre los objetivos.
NOTA 1: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.
NOTA 2: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.
NOTA 3: Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades

Riesgo de Información (NTC-ISO/IEC 27005): Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

Riesgo de Ciberseguridad (NISTIR 8286 basado en ISO Guide 73 y NIST SP 800-60 Vol. 1 Rev. 1): Un efecto de la incertidumbre en o dentro de un contexto digital. Los riesgos de ciberseguridad se relacionan con la pérdida de confidencialidad, integridad o disponibilidad de información, datos o sistemas de información (o control) y reflejan los posibles impactos adversos en las operaciones de la organización (es decir, misión, funciones, imagen o reputación) y activos, individuos, otras organizaciones y la Nación.

Seguridad de la Información: Conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad u otro medio. (Superintendencia Financiera Circular externa 007, 2018)

Segregación de funciones: Medida que separa las responsabilidades de las distintas actividades involucradas en los procesos críticos de la Compañía.

- **Documentos de referencia:**

Política de continuidad del negocio

MSG-016 Manual General de Seguridad de la Información. Corporativo

MSG-017 Manual de Lineamientos Específicos de Seguridad de la Información – Áreas de Tecnología de la Información

Manual interno para la protección de los datos personales

Manual de Gestión de Riesgos de la Información

Manual del Sistema de Gestión de Seguridad de la Información

Manual Plan de Recuperación ante desastres DRP

IN_SO0113_01 Seguridad Usuarios y Contraseñas

PR_SO0114_02 Procedimiento de atención y respuesta a incidentes de Seguridad de la Información y Ciberseguridad

IN_AVSG04_008 Instructivo para reporte interno y para evaluación de materialidad de Ciberincidentes.

Demás procedimientos e instructivos asociados al marco normativo de la seguridad de la información.