IG4 CAPITAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y TRATAMIENTO DE DATOS PERSONALES

IG4 CAPITAL INVESTIMENTOS LTDA.

("Gestora")

Versión vigente: junio/2022
Versión anterior: julio/2021

Revisión nº:	**Inicio de la vigencia:**
6 (junio/2022)	30/11/2016 y, en su caso, a partir de la obtención de la autorización de la CVM (Comisión de Valores Mobiliarios de Brasil) como gestora de activos

Aprobado por: DocuSigned by: 205EC3047D054CD...

Flávia Andraus Troyano

Director de Cumplimiento

CAPÍTULO I
DEL OBJETIVO

1.1. El presente instrumento tiene por objetivo formalizar la Política de Seguridad de la Información ("Política") adoptada por la Gestora, con carácter permanente, a fin de presentar y diseminar entre los Colaboradores los procedimientos de control utilizados para garantizar la seguridad de la información producida y administrada dentro del ambiente de trabajo de IG4 Capital.

1.2. De este modo, es responsabilidad de todos los Colaboradores garantizar la confidencialidad e integridad de la información producida durante la ejecución del trabajo en la Gestora, siendo fundamental que todos los Colaboradores tengan plena consciencia al respecto de la importancia de cada uno en la garantía de la efectividad de los procedimientos definidos en esta política.

1.3. Es exigido también el comprometimiento en el cumplimiento de esta Política por todos los Colaboradores de IG4 Capital.

1.4. Cualquier colaborador que tenga conocimiento al respecto del incumplimiento de la presente política deberá comunicárselo al Departamento de Compliance, por medio del e-mail compliance@ig4capital.com o efectuar un relato por medio del Canal de Denuncias de la Gestora.

CAPÍTULO II
DE LA AMPLITUD

2.1. Se entiende por "colaboradores", en línea con el concepto definido por el Código de Ética y Conducta de la Gestora: (i) socios y asociados; (ii) funcionarios; (iii) directores; (iv) pasantes; o (v) cualesquiera personas que, en virtud de sus cargos, funciones o posiciones en la Gestora, tengan acceso a la información generada internamente y/o recibida de clientes para el desarrollo de trabajos internos.

2.2. Todos los Colaboradores deben tener consciencia de que toda la información generada internamente o recibida es estrictamente confidencial. La responsabilidad de confidencialidad e integridad de la información tendrá validez incluso después del despido del Colaborador, siendo que el incumplimiento de las disposiciones previstas en esta Política será consideración con infracción grave, susceptible de sanciones administrativas y/o judiciales.

CAPÍTULO III
DE LAS DIRECTRICES Y PROCEDIMIENTOS

3.1. Control de Acceso:

El intercambio de información entre los Colaboradores de la Gestora debe siempre pautarse en el concepto de que el receptor debe ser alguien que necesita recibir tal información para el desempeño de sus actividades y que no está sujeto a ninguna barrera que impida el recibimiento de aquella información. En el caso de dudas el Departamento de Compliance debe ser accionado previamente a la revelación.

Para asegurar el control de Información Confidencial, las siguientes medidas son utilizadas:

(i) login y contraseña para acceso a la red de computadoras individuales para cada Colaborador, así como para acceso a e-mail y dispositivos móviles de uso profesional, siendo tales contraseñas personales e intransferibles;

(ii) prohibición de conexión de equipos en la red de la Gestora que no estén previamente autorizados por el área de informática de la Gestora, no siendo permitido que los Colaboradores utilicen computadoras, discos externos o cualesquiera otros dispositivos no relacionados al desempeño de sus actividades en la Gestora.

(iii) red de información electrónica con la utilización de servidores exclusivos de la Gestora, evitando accesos de terceros;

(iv) mantenimiento de diferentes niveles de acceso a carpetas y archivos electrónicos de acuerdo con las funciones de los Colaboradores, con registro de acceso a tales carpetas y archivos por parte de los Colaboradores con base en la contraseña y login de cada Colaborador, y protección contra adulteraciones y mantenimiento de registros que permitan auditorías e inspecciones;

(v) monitoreo de acceso a sitios, blogs, fotologs y webmails, entre otros, así como los e-mails enviados y recibidos;

(vi) monitoreo, incluso por medio de grabaciones, de llamadas telefónicas realizadas o recibidas por medio de las líneas telefónicas suministradas por la Gestora para la actividad profesional de cada Colaborador; y

(vii) bloqueo de acceso a los sistemas por el departamento de TI, siempre que sea solicitado por el Departamento de Compliance, o en el caso que sea detectado por el departamento de TI algún riesgo para la red o los sistemas de la Gestora.

El Colaborador podrá ser responsabilizado en el caso que le entregue cualesquiera de sus contraseñas a terceros.

El departamento de tecnología de la información ("TI") hará verificaciones semestrales en la red corporativa de la Gestora, para validar el acceso seguro a los recursos disponibles, buen uso de equipos e información común a más de un sector de la Gestora, preservación de Información Confidencial e identificación de las personas que tuvieron o tengan acceso a estas, protección contra adulteraciones y mantenimiento de registros que permitan auditorías e inspecciones. Al final de cada verificación será enviado un e-mail por el área de TI para el Departamento de Compliance reportando la conclusión de los exámenes realizados, incluso eventuales irregularidades o fallas verificadas.

En relación a las copias físicas, documentos conteniendo Información Confidencial deben ser objeto de archivo con acceso restringido y deben ser triturados previamente a su descarte, evitando acceso indebido a tal información, observada las normas relativas a la conservación de documentos por los períodos legales aplicables.

La sede de la Gestora posee segregación física de espacios, de forma que (i) acceso al espacio asignado a la actividad de gestión sea restringido a los respectivos Colaboradores; (ii) reuniones, incluso con no colaboradores, sean realizadas de forma reservada, en salas específicas y segregadas del espacio asignado a la actividad de gestión.

3.2. Backup:

Todos los documentos archivados en las computadoras de la Gestora son objeto de backup diario en la nube con control de las modificaciones promovidas en los archivos, garantizando la seguridad de los respectivos contenidos y eventual responsabilización.

3.3. Copia de archivos e instalaciones:

Todos los programas de computadora utilizados por los Colaboradores deben haber sido previamente autorizados por el responsable del área de TI. Downloads de cualquier naturaleza pueden ser realizados siempre que sea de forma justificada.

La copia de archivos e instalación de programas en computadoras de la Gestora deberá respetar los derechos de propiedad intelectual pertinentes, tales como licencias y patentes.

Está terminantemente prohibido que los Colaboradores hagan copias (físicas o electrónicas) o impriman los archivos utilizados, generados o disponibles en la red y circulen en ambientes externos con estos archivos, salvo si es en favor de la ejecución y del desarrollo de los negocios y de los intereses de la Gestora. En estos casos, el Colaborador que esté en la posesión y guarda del archivo será el responsable directo por su buena conservación, integridad y mantenimiento de su confidencialidad.

Cualquier impresión de documentos debe ser inmediatamente retirada de la máquina impresora, pues puede contener información restringida y confidencial incluso en el ambiente interno de la Gestora. Está prohibido, además, el mantenimiento de estos en mesas, máquinas de fax o copiadoras.

3.4. Descarte de Información:

El descarte de información confidencial debe seguir las siguientes directrices:

(i) el contenido descartado deberá ser borrado y/o los medios deben ser destruidos, imposibilitando su recuperación, de modo que la información no quede vulnerable a acceso no autorizado;

(ii) los documentos físicos que contengan información protegida deben ser triturados inmediatamente después de su uso para evitar su recuperación o lectura;

(iii) la eliminación o la destrucción final de los medios o documentos, realizada por terceros, debe ser documentada.

(iv) dispositivos de memoria y dispositivos de almacenamiento (por ejemplo laptops, dispositivos USB, discos duros portátiles, tablets, smartphones) desactivados por la Gestora deben ser borrados de modo que la información protegida que había en ellos sea irrecuperable.

3.5. Redundancia:

Además de las copias de seguridad anteriores, otros recursos de TI son redundantes. En el caso de avería e indisponibilidad de acceso físico al local de trabajo, el equipo podrá acceder a la información en la nube desde cualquier local.

Para garantizar el funcionamiento de la red y la integridad de los datos, incluso ante la eventual interrupción del suministro de energía eléctrica, todas las estaciones de trabajo y el servidor están conectados a un equipo del tipo no-break, que permite la continuidad del funcionamiento de la red por tiempo suficiente para que los usuarios guarden sus archivos.

3.6. Soporte y Monitoreo:

En el caso de avería de la red o en alguna estación de trabajo, el hecho deberá ser inmediatamente comunicado al área de TI, que asegurará el soporte interno o garantizará que sea accionado el soporte externo necesario.

Los sistemas electrónicos utilizados por la Gestora están sujetos a la revisión y monitoreo en cualquier época sin aviso o permiso, para detectar cualquier irregularidad en la transferencia de información, ya sea interna o externamente.

En este sentido, teniendo en cuenta que la utilización del e-mail se destina exclusivamente para los fines profesionales, como herramienta para el desempeño de las actividades de los Colaboradores, la Gestora también podrá monitorear todo y cualquier cambio, interno o externo, de e-mails de los Colaboradores.

Cualquier sospecha o conocimiento de violación de esta Política o incidente de seguridad de la información debe ser objeto de información al Compliance para que sean tomadas las debidas medidas con relación a la investigación de los hechos, mitigación de eventuales riesgos, implementación de procedimientos correctivos y

responsabilización de los involucrados.

Periódicamente y sin aviso previo, podrán ser realizadas inspecciones en las computadoras para la averiguación de downloads impropios, no autorizados o grabados en locales indebidos.

3.7. Tratamiento de casos de fuga de información confidencial:

En el caso de fuga de información confidencial relacionada a inversionistas, o de cualquier otro Dato Personal o Dato Personal Sensible tratado por la Gestora (regla de Tratamiento de Datos a seguir), aunque sea oriundo de acción involuntaria, la Directora de Compliance notificará a los interesados sobre lo ocurrido. Tratándose de Dato Personal o Dato Personal Sensible, la Autoridad Nacional de Protección de Datos también deberá ser comunicada, además del titular del dato. Esta comunicación respetará los parámetros exigidos por la Ley General de Protección de Datos.

Sin perjuicio, la Gestora accionará su Plan de Recuperación buscando la identificación de la causa que produjo la fuga y responsabilización del causador. Además, será elaborado un Informe acerca de los daños ocurridos, porcentual de las actividades afectadas, impactos financieros, sugiriendo además medidas a ser tomadas para posibilitar que las actividades vuelvan a ser ejecutadas normalmente.

Este Informe será elaborado por la Directora de Compliance y será sometido a la Dirección de la Gestora que promoverá las iniciativas correspondientes para el retorno a la normalidad con la mayor brevedad posible.

3.8. Firewall:

La Gestora hace el uso de la tecnología de Firewall para proteger su red contra amenazas externas.

3.9. Pruebas de Seguridad:

Son realizadas las siguientes pruebas de seguridad para el monitoreo de los sistemas utilizados:

Prueba	**Periodicidad**
Control de dispositivos conectados	Por demanda
Control de acceso	Anual
Pruebas de doble autenticación	Mensual

CAPÍTULO IV
TRATAMIENTO DE DATOS PERSONALES Y SENSIBLES

4.1. La Gestora vela por la observancia, implementación y cumplimiento de reglas, políticas y procedimientos relacionados a la Seguridad de la Información.

4.2. Sin perjuicio de las directrices que aparecen en la Política de Seguridad de la Información anterior y con el objetivo de proteger los derechos fundamentales de libertad y de privacidad, la Gestora adopta reglas y procedimientos para el tratamiento de datos personales y, eventualmente, datos sensibles, incluso en los medios digitales, en línea con la Ley General de Protección de Datos. Para los fines dispuestos en este Código, se consideran:

- "Datos Personales" cualquier información relacionada a persona natural identificada o identificable.

- "Datos Personales Sensibles" los Datos Personales que versen sobre el origen racial o étnico, convicción religiosa, opinión política, filiación a sindicato o a organización de carácter religioso, filosófico o político, dato referente a la salud o a la vida sexual, dato genético o biométrico, cuando estén vinculados a una persona natural.

4.3. Todos los Datos Personales o Datos Personales Sensibles es Información Confidencial y deben ser tratados como tal para los fines de este Código y demás manuales y políticas internas adoptadas por la Gestora.

4.4. El tratamiento de datos personales y de datos sensibles será realizado exclusivamente: (i) para los fines de cumplimiento de obligación regulatoria, en función de las exigencias normativas expedidas por la CVM y auto regulatorias expedidas por ANBIMA; o (ii) para la ejecución de contrato firmado con el cliente. En cualquiera de los casos, solamente será recolectada información de los clientes para finalidades legítimas, buscando la prestación de servicios contratados por el cliente o atención a la regulación y autorregulación, siendo mantenido por la Gestora el registro de las operaciones de tratamiento de datos personales y datos sensibles que realice.

4.5. Siempre que sea necesario el tratamiento de Datos Personales y Datos Sensibles para fines diferentes de aquellos definidos anteriormente, será recolectado el consentimiento del titular, por escrito o por otro medio que demuestre su manifestación de voluntad, para el tratamiento de sus datos, debiendo ser identificadas, expresamente, las finalidades para las cuales se destina. En esta hipótesis, el titular de los datos (personales y sensibles) podrá revocar el consentimiento otorgado en cualquier momento.

4.6. Independiente de la finalidad, el titular del dato personal y/o sensible deberá tener acceso facilitado a la información sobre el tratamiento de sus datos, que deberán ser dispuestas de forma clara, adecuada y ostensiva, indicando:

a. finalidad específica del tratamiento;
b. forma y duración del tratamiento, observados los secretos comercial e industrial;
c. identificación de la Gestora;
d. información de contacto de la Gestora;
e. información acerca del uso compartido de datos por la Gestora y la finalidad;
f. responsabilidades de los agentes que realizarán el tratamiento; y
g. derechos del titular, con mención explícita a sus derechos previstos en el art. 18 de la LGPD.

4.7. El término del tratamiento de datos personales y sensibles ocurrirá finalizada la relación contractual existente entre la Gestora y el cliente o, además, cuando el inversionista no posea más ninguna aplicación en los fondos bajo gestión de la Gestora, conforme sea el caso, pudiendo la Gestora conservar los datos personales y sensibles incluso después del término de su tratamiento para los fines de cumplimiento de obligación legal o regulatoria.

4.8. La Gestora es responsable de garantizar la seguridad de los datos tratados, sin perjuicio del entrenamiento de los Colaboradores con relación a la materia.

CAPÍTULO V
DE LAS DISPOSICIONES GENERALES

5.1. La Interpretación de esta Política debe ser ejecutada por todos los Colaboradores, en conjuntos con las normas y procedimientos que están previstos en el Código de Ética y Conducta de IG4 Capital Investimentos Ltda. y, cuando sea necesario, en consulta al Departamento de Compliance de la Gestora.

5.2. Cualquier infracción o sospecha de infracción de esta Política deberá ser comunicada al Departamento de Compliance, por medio del Canal de Denuncias de IG4 Capital (https://ig4capital.becompliance.com/compliance/canal-denuncias) o por el e-mail compliance@ig4capital.com y deberá ser tratada en los términos y penalidades impuestas por la Gestora.