POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

Historial de versiones.

Versión	Fecha	Modificado por	Descripción breve
V0.1	NOV.2024	Auditores Consultores Recad Limitada	Política de Seguridad de la Información y Ciberseguridad
V0.1	NOV.2024	Directores y Abogado	Política de Seguridad de la Información y Ciberseguridad
V0.1.	NOV.2024	Gerente General	Política de Seguridad de la Información y Ciberseguridad

Aprobada por Directorio 30/11/2024

C.4. RIESGO OPERACIONAL

Los intermediarios y custodios de instrumentos financieros, con el objeto de que la entidad desarrolle una adecuada gestión de riesgo operacional, deberán considerar los elementos que se señalan a continuación, adaptándolos de acuerdo a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Las políticas y procedimientos de gestión de riesgo operacional deberán incluir, al menos, los siguientes ámbitos relacionados, descritos en las próximas secciones:

- ✓ seguridad de la información y ciberseguridad,
- ✓ continuidad de negocio; y
- ✓ externalización de servicios.

Los ámbitos mencionados deberán ser considerados por la entidad en los informes que realicen las instancias encargadas de la gestión de riesgos y la auditoría interna, según corresponda. Lo anterior, sin perjuicio del cumplimiento de las normativas aplicables a la entidad que requieren la gestión de sus riesgos operacionales. Las políticas y procedimientos de gestión de riesgo operacional deben estar diseñadas para brindar una seguridad razonable que la entidad pueda desarrollar las operaciones del negocio en forma continua y eficiente, incluso ante la presencia de eventos disruptivos, salvaguardando sus servicios, procesos y activos de información. Estas políticas y procedimientos deben ser establecidas y aprobadas por el directorio, u órgano equivalente, y ser difundidas a todo el personal dentro de la organización. Además, dichas políticas y procedimientos deben establecer los niveles de apetito por riesgo definidos por el directorio u órgano equivalente, que determinará la necesidad de evitar, reducir, transferir o aceptar los riesgos, y acorde con ello, diseñar controles mitigantes.

b) Contar con indicadores claves de medición del riesgo operacional consistentes con la metodología de evaluación y monitoreo de riesgos integrales de la entidad, permitiendo al mismo tiempo establecer niveles de alerta y evaluar la eficacia de los controles adoptados. El detalle de cálculo de estos indicadores deberá ser incluido expresamente en las políticas y procedimientos de gestión de riesgo operacional de la misma entidad.

C.4.1. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

C.4.1.1 DISPOSICIONES GENERALES

En el ámbito de seguridad de la información y ciberseguridad, la gestión de riesgo operacional deberá incluir los siguientes elementos aplicables a todas las entidades adaptándolos de acuerdo a su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

- ➢ Contar con una política de seguridad de la información y ciberseguridad que considere al menos lo siguiente:

- ✓ Procedimientos para la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad, de forma resguardar la disponibilidad, confidencialidad e integridad de los activos de información.
- ✓ Niveles de apetito por riesgo en materia de seguridad de la información y ciberseguridad.
- ✓ Principales funciones y responsabilidades sobre la materia.
- ✓ Procedimientos para la evaluación de los riesgos de seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, servicios, sistemas, emprender nuevas actividades o definir nuevos procesos.
- ✓ Las políticas de seguridad de la información y ciberseguridad formarán parte de las políticas de gestión de

riesgos de la entidad, debiendo ser actualizadas y aprobadas al menos anualmente por el directorio, u órgano equivalente, o con una periodicidad mayor en caso de cambios significativos.

- Contar con una política de tecnologías de información y comunicación (TIC), que considere al menos lo siguiente:

  - ✓ Definición de las líneas de responsabilidad en cuanto a la gestión de los activos de información en la entidad.
  - ✓ Definición de los procesos TIC que aseguren un adecuado diseño, transición, operación de servicio y gestión a través de sus activos de información.
  - ✓ Definición de los procedimientos que se deberán seguir para la adecuada gestión de los procesos TIC.

- Definición del perfil y número necesario de personas con conocimientos o experiencia comprobables en estándares de seguridad de la información y ciberseguridad.

- Establecimiento de los procedimientos para que el personal de la entidad, incluyendo el directorio u órgano equivalente, contribuya a una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad, de conformidad con sus roles y responsabilidades, mediante la implementación de:

  - ✓ Procedimientos de difusión, capacitación y concientización que traten sobre los riesgos, vulnerabilidades y amenazas a la seguridad de la información, la gestión de estos, y las lecciones aprendidas respecto de los incidentes en esta materia, para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de dichos riesgos.
  - ✓ Acuerdos contractuales con los empleados que establezcan sus responsabilidades y las de la entidad en materia de seguridad de la información y ciberseguridad, incluyendo sanciones.

- Generación de acuerdos contractuales para la revocación de derechos de acceso a información y destrucción de activos de información como parte del proceso de cambio de posición o desvinculación de un empleado.

- Auditoría de los procesos de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

- Disposición de procedimientos que le permitan al directorio u órgano equivalente mantenerse informado en forma oportuna y periódica sobre el sistema de gestión de la seguridad de la información y ciberseguridad. Deberá dejarse constancia del reporte de la información de estas materias en las respectivas actas del directorio u órgano equivalente y los comités que se conformen para revisar estas materias.

C.4.1.2 PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La entidad deberá considerar los siguientes procedimientos, y adaptarlos en relación con su modelo de negocios, volumen de operaciones, y número y tipo de clientes:

- Identificación

  - ✓ Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.
  - ✓ Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad.
  - ✓ Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión, clasificados desde una perspectiva de disponibilidad, confidencialidad e integridad.
  - ✓ Implementar un inventario de activos de información que permita conocer las principales características del activo, considerando al menos: hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, estaciones de trabajo, servidores, medios de almacenamiento y documentación física.

- ✓ Actualizar el inventario de activos de información en forma continua, para lo cual los distintos procesos de gestión de riesgo operacional deberán reportar la información que pueda tener efecto en dicho inventario.

➢ Protección y Detección

- ✓ Controles de acceso a las instalaciones e infraestructuras de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.
- ✓ Controles de acceso a los sistemas, de manera de mitigar los riesgos de suplantación o uso indebido por parte de terceros. En el caso de instalaciones, infraestructuras y sistemas críticos, se deberá privilegiar el uso de mecanismos de autenticación multifactor.
- ✓ Implementación de herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios y administradores de sistemas y activos de información, incluyendo usuarios de alto privilegio.
- ✓ Procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, servicios de red, sistemas operativos, bases de datos y aplicaciones de negocios en función de los roles y responsabilidades del personal y sólo lo estrictamente necesario para que éste cumpla sus funciones actuales.
- ✓ Controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por personal interno o externo, así como también los dispositivos Internet de las Cosas (IoT).
- ✓ Mecanismos de control y monitoreo de las condiciones ambientales para la localización segura para los equipos y herramientas, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de incendios y desastres naturales.
- ✓ Procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:

  - Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, anti-spyware y anti-malware, entre otros.
  - Un proceso de gestión de la configuración de los sistemas y activos de información.
  - Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:

➢ Las disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos de los inversionistas, incluyendo acuerdos de no divulgación.

➢ Los procesos de administración de respaldos que aseguren la disponibilidad, confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección E.4.2 siguiente. Los respaldos de la información se debiesen mantener en lo posible en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

➢ Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.

➢ Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.

➢ Respuesta y Recuperación

➢ La entidad deberá contar con procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, considerando:

- ✓ Una instancia de alto nivel definida por el directorio u órgano equivalente encargada de la gestión de incidentes de seguridad de la información y ciberseguridad.
- ✓ Procedimientos de respuesta y recuperación ante incidentes, aprobados por el directorio u órgano equivalente, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y

soporte, los activos de información críticos y las interdependencias con terceros en caso de incidentes. Dichos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección IV.E de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones. Los procedimientos de respuesta y recuperación ante incidentes deberán actualizarse al menos anualmente, cada vez que se registran cambios en los activos de información o se produzcan incidentes que amenacen la seguridad de estos.

✓ Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad, y a esta Comisión, de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección V.E de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.

➢ Procedimientos para el desarrollo, adquisición y actualización de la infraestructura tecnológica de la entidad, que consideren:

✓ Las necesidades de infraestructura tecnológica de la entidad.
✓ Implementación de un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información producto de la introducción de nuevos productos, sistemas y actividades sean efectuadas y monitoreadas de manera segura y controlada.
✓ Como parte de este proceso, previo al paso de producción de un servicio o activo de información se deben realizar pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas, con el propósito de asegurar que no hubiere un impacto adverso en la seguridad de la información y en las operaciones del negocio.
✓ Implementación de un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas que no generen efectos adversos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial
✓ Implementación de un proceso de gestión de actualizaciones de seguridad de software (parches).

➢ La entidad deberá contar con un procedimiento para el mejoramiento continuo de las herramientas, procedimientos y controles de seguridad de la información y ciberseguridad que considere:

✓ Recolectar y analizar información sobre el funcionamiento de activos de información.
✓ Analizar los incidentes de seguridad de la información y ciberseguridad y la efectividad de las medidas adoptadas para resolverlo.
✓ Ejecutar pruebas para identificar amenazas y vulnerabilidades en la seguridad de la información:

- Las pruebas deberán ser realizadas con una periodicidad no mayor a un año, y ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.
- Las pruebas deberán estar basadas en escenarios de riesgo planificados y diseñados para demostrar que los mecanismos y herramientas implementados para preservar la seguridad de la información cumplen adecuadamente con su objetivo, incluyendo ataques cibernéticos.
- Los resultados de las pruebas realizadas deberán ser reportados al directorio u órgano equivalente, incluyendo recomendaciones de mejora en las herramientas, procedimientos y controles.

1. Objeto

En ASESORIAS E INVERSIONES FSJ SPA la Política de Seguridad de la Información y Ciberseguridad establece los principios y directrices que debemos seguir para identificar, clasificar, asignar responsables y proteger adecuadamente los activos de información en nuestra organización, con el objetivo de salvaguardar la integridad de los datos, garantizar la confidencialidad y asegurar la disponibilidad de la información necesaria para cumplir con nuestros objetivos de negocio.
La presente Política de tecnologías de la información y de riesgos de ciberseguridad tiene como objetivo marcar los principios y directrices que den el soporte adecuado para una correcta gestión de la seguridad de la información, de modo que se asegure el adecuado control, rigor y cumplimiento en las actuaciones que se lleven a cabo.

ASESORIAS E INVERSIONES FSJ SPA reconoce la importancia que tiene la seguridad de la información para la correcta realización de sus actividades.
Los activos de información en ASESORIAS E INVERSIONES FSJ SPA abarcan una amplia gama de recursos, como bases de datos de clientes, información financiera, informes de cumplimiento normativo y comunicaciones internas. Entendemos que la correcta gestión de estos activos es fundamental para mantener la confianza de nuestros clientes, cumplir con las regulaciones de libre competencia y garantizar la continuidad de nuestras operaciones.
Por ello ha desarrollado esta política que fija e integra los principios básicos de seguridad con los requisitos operativos en términos de confidencialidad, autenticidad, trazabilidad, integridad, disponibilidad y conservación de la información.

El principal objetivo de esta política es reforzar el compromiso de ASESORIAS E INVERSIONES FSJ SPA con los empleados, empresas, clientes y proveedores, expresado en términos de mejora continua del servicio ofrecido, del cumplimiento de la legislación aplicable, de la mejora de los procesos internos y de la protección de la información manejada dentro del entorno de ASESORIAS E INVERSIONES FSJ SPA.
Nuestra Política establece los lineamientos para identificar y evaluar los activos de información críticos para nuestra empresa, así como para clasificarlos en función de su importancia, sensibilidad y valor. Considera, además, asignar a cada activo de información un responsable de su protección y gestión adecuada, quien velará por su integridad y confidencialidad.

En ASESORIAS E INVERSIONES FSJ SPA nos comprometemos a implementar controles de seguridad adecuados para proteger nuestros activos de información contra amenazas internas y externas, como el acceso no autorizado, la divulgación indebida o la pérdida de datos. A través de esta Política, estableceremos medidas técnicas, físicas y administrativas para salvaguardar la información y promover prácticas seguras en toda la organización.
La gestión adecuada de los activos de información no solo contribuye a la protección de ASESORIAS E INVERSIONES FSJ SPA y nuestros clientes, sino que también refuerza nuestro compromiso con la sostenibilidad, y la legislación vigente, en especial en materia de libre competencia. Al asegurar la disponibilidad de la información necesaria para tomar decisiones informadas, podemos mejorar continuamente nuestros procesos y maximizar nuestra eficiencia operativa.

En resumen, esta Política refuerza nuestra dedicación a la seguridad, integridad y disponibilidad de los activos de información que respaldan nuestras operaciones de Factoring e Intermediación de facturas con distintos Fondos de Inversión.

Se hace por tanto necesario que todas las personas que interaccionen de manera directa o indirecta con ASESORIAS E INVERSIONES FSJ SPA conozcan la política y normativas pertinentes y apliquen sus directrices como tareas propias de las funciones desarrolladas en su vinculación con la misma.

Así pues, la Política de tecnologías de la información y de riesgos de ciberseguridad desarrollada en este documento velará por garantizar la protección de los activos de información de ASESORIAS E INVERSIONES FSJ SPA siendo ésta de aplicación en todas las fases del ciclo de vida de dichos activos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción.

Para la aplicación efectiva de la presente Política y de la Normativa que la desarrolla, ASESORIAS E INVERSIONES FSJ SPA se dotará de los recursos necesarios para su buen desarrollo, tanto en lo referente a las actividades de implantación como de mantenimiento, incluyendo los controles o medidas de seguridad que en cada ámbito se establezcan.

2. Alcance de la Política de Seguridad de la Información y Ciberseguridad de Asesorías e Inversiones FSJ SPA

Esta Política tiene un alcance amplio y se aplica a todas las personas que ocupan un cargo, función o posición en ASESORIAS E INVERSIONES FSJ SPA incluyendo directores, ejecutivos y trabajadores. Además, se aplica a las Filiales y contratistas, proveedores o asesores, así como a los terceros que acceden, utilizan o manejan activos de información de ASESORIAS E INVERSIONES FSJ SPA Resumiendo:

- A todas las sociedades que componen ASESORIAS E INVERSIONES FSJ SPA
- A contratistas y terceros con acceso a los activos de ambos, o bajo su responsabilidad.
- A la información tratada almacenada y custodiada desde cualquier área del grupo.
- A todas las instalaciones, recursos y procesos utilizados para la prestación de servicios, sean estos internos o vinculados con terceros a través de acuerdos o contratos.

Por otra parte, esta Política se extiende a todos los activos de información, tales como computadores, servidores, equipos de red, servicios en la nube, portales y sistemas de propiedad de ASESORIAS E INVERSIONES FSJ SPA dispositivos de almacenamiento extraíbles, discos duros físicos y virtuales, independientemente de su formato o ubicación, que son fundamentales para nuestras operaciones y para cumplir con nuestros compromisos.

Los activos de información incluyen, pero no se limitan a:

- **Datos y registros:**

Esto abarca información recopilada y mantenida en nuestra base de datos de clientes, registros financieros, informes de cumplimiento normativo, operaciones de factoring, liquidaciones de pago, datos personales y cualquier otra información utilizada para respaldar nuestras operaciones y el cumplimiento de las regulaciones y de responsabilidad penal de la persona jurídica, entre otras.

- **Sistemas y aplicaciones:**

Engloba los sistemas informáticos y aplicaciones que utilizamos para gestionar y operar nuestras actividades de Factoring e Intermediación, incluyendo software de seguimiento de inventarios de facturas, y herramientas de análisis de datos, sistemas de gestión y cualquier otro sistema que maneje, almacene o procese información crítica para nuestra organización.

- **Redes y comunicaciones:**

Se refiere a la infraestructura de red utilizada en ASESORIAS E INVERSIONES FSJ SPA incluyendo conexiones internas y externas, dispositivos de red, firewalls y otros componentes necesarios para el intercambio seguro de información dentro de la organización y con entidades externas.

- **Equipos:**

Incluye todos los equipos físicos utilizados para recopilar, almacenar, procesar o transmitir información, como servidores, ordenadores, portátiles, dispositivos móviles, unidades de almacenamiento y cualquier otro dispositivo que albergue datos o se utilice para acceder a ellos.

- **Documentación:**

Esto comprende todos los documentos físicos o electrónicos que contienen información crítica para nuestras operaciones, como manuales de procedimientos, políticas internas, contratos, acuerdos de confidencialidad, otorgamientos, liquidaciones de pago y cualquier documento que sea necesario para la gestión de la información en ASESORIAS E INVERSIONES FSJ SPA

Esta Política se aplica a todos los activos de información, independientemente de su ubicación física o digital, dentro de nuestras instalaciones, en dispositivos móviles o en la nube.
En resumen, esta política tiene como objetivo garantizar una gestión adecuada de todos los activos de información en ASESORIAS E INVERSIONES FSJ SPA abarcando desde los datos y sistemas hasta la infraestructura de red, equipos y documentación.
Al aplicar esta Política, buscamos salvaguardar la información crítica para nuestras operaciones, garantizar el cumplimiento normativo y proteger la confidencialidad, integridad y disponibilidad de nuestros activos de información.
Esta política se ubica dentro del marco jurídico definido por la legislación y normativa vigente, relacionada directa o indirectamente con el tratamiento de la información mediante métodos automatizados y con la seguridad de la información.

3. Principios básicos de la seguridad de la Información y Ciberseguridad

ASESORIAS E INVERSIONES FSJ SPA se rige por los siguientes principios en relación con la seguridad de la información y Ciberseguridad:

- **Confidencialidad**: La ASESORIAS E INVERSIONES FSJ SPA se compromete a tratar toda la información que tengamos de manera confidencial, protegiéndola contra accesos no autorizados o divulgaciones indebidas. Toda la Información Confidencial será utilizada exclusivamente para cumplir el objeto y finalidad para la cual es generada, recopilada o tratada por ASESORIAS E INVERSIONES FSJ SPA debiendo ser guardada como Información Confidencial y no será revelada ni divulgada a terceros sin autorización previa, escrita y expresa de ASESORIAS E INVERSIONES FSJ SPA

- **Integridad:** Se mantendrá la precisión y la integridad de la información a través de controles adecuados para evitar alteraciones no autorizadas o no intencionadas.

- **Disponibilidad:** Se debe garantizar la disponibilidad de la información y los sistemas necesarios para el funcionamiento continuo y eficiente de nuestras operaciones.

- **Cumplimiento legal:** ASESORIAS E INVERSIONES FSJ SPA cumplirá todas las leyes, regulaciones y requisitos contractuales aplicables en relación con la seguridad de la información y Ciberseguridad.

- **Gestión de riesgos:** Se identificarán, evaluarán y mitigarán los riesgos de seguridad de la información a través de un enfoque basado en evaluaciones de riesgos y mejores prácticas. ASESORIAS E INVERSIONES FSJ SPA tendrá una tabla de criterios de aceptación de riesgos, donde se especificará la probabilidad de ocurrencia y cuantificará el impacto de este (limitaciones de servicio, pérdida de datos, continuidad operativa, daños reputacionales, entre otros), asignándole un nivel de riesgo. Todos los riesgos identificados contarán con un responsable del riesgo, quien deberá proponer un plan de tratamiento de los riesgos identificados y asegurar la ejecución del plan para mitigar los mismos. El responsable del riesgo será quien este a cargo de TI.

- **Responsabilidad:** Toda persona que ocupa un cargo, función o posición en ASESORIAS E INVERSIONES FSJ SPA incluyendo directores, ejecutivos principales, trabajadores y todos aquellos que presten servicios a la ASESORIAS E INVERSIONES FSJ SPA como contratistas, o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ASESORIAS E INVERSIONES FSJ SPA son responsables de cumplir con las políticas y procedimientos de seguridad de la información establecidos por ASESORIAS E INVERSIONES FSJ SPA A los socios de la ASESORIAS E INVERSIONES FSJ SPA se les enviará una vez por año, una guía de buenas prácticas de ciberseguridad.

- Adicionalmente se debe:
  - ✓ Aceptar como activos estratégicos la información y los sistemas que la procesan y almacenan, manifestando su determinación en alcanzar los niveles de seguridad necesarios para garantizar su protección, y así mejorar la calidad de los servicios ofrecidos a los empleados o clientes.

- ✓ Garantizar la confidencialidad de la información manejada para la adecuada prestación de los servicios, adaptando las medidas de seguridad al nivel de confidencialidad exigido sobre la información manejada.

- ✓ Garantizar la disponibilidad de la información y de los sistemas que la procesan y almacenan, estableciendo las medidas de prevención, detección y recuperación de carácter organizativo, físico y lógico necesarias.

- ✓ Gestionar los riesgos a los que se ve sometida la información mediante la identificación de posibles amenazas y la adopción de medidas de seguridad apropiadas para tratarlas.

- ✓ Disponer de un entorno de seguridad que garantice el cumplimiento de los requisitos legales aplicables a la información y a los sistemas.

4. Responsabilidades

El Directorio es responsable de que los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de ASESORIAS E INVERSIONES FSJ; mientras que la Alta Dirección tiene la responsabilidad de liderar y respaldar la implementación de la Política de la Seguridad de la Información. Esto implica proporcionar los recursos necesarios, establecer objetivos y supervisar regularmente el desempeño del sistema de gestión de seguridad de la información.
Además, la Alta Dirección debe garantizar que se establezca un marco de gestión de riesgos de seguridad de la información, asignar roles y responsabilidades claras dentro de la organización, y asegurarse de que se realicen revisiones periódicas para evaluar su eficacia y realizar mejoras continuas.

5. Medidas para garantizar la seguridad de la información

Con el fin de garantizar la existencia de un marco global de seguridad de la información que proteja, en la medida de lo posible, frente a dichas amenazas, el Comité de Seguridad de ASESORIAS E INVERSIONES FSJ SPA procederá a adoptar una serie de medidas para prevenir, detectar, reaccionar y recuperarse ante posibles incidentes que afecten a la información.

La seguridad de la información es entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se llevarán a cabo diferentes iniciativas que respalden los esfuerzos ya realizados, de cara a proporcionar una visión general sobre la seguridad de la información a todas las partes interesadas, definir los controles adecuados para proteger los activos y cumplir con los requisitos marcados por la legislación vigente.

En este sentido, se deberá poner en marcha los mecanismos adecuados para prevenir, detectar, reaccionar y recuperarse a los posibles incidentes que puedan afectar a la seguridad de la información. Entre dichos mecanismos se encuentran, entre otros, las siguientes medidas:

- ➢ Prevención

Se tratará de prevenir y evitar la existencia de incidentes que puedan afectar a la seguridad de la información y a los servicios prestados. Para ello, se implantarán las medidas y controles de seguridad necesarios, que serán definidos a través de un proceso formal de análisis y gestión de riesgos.

Dichas medidas y controles, así como las responsabilidades en materia de seguridad de la información y ciberseguridad serán definidos y documentados de manera clara y formal tanto en la Política como en la Normativa de Seguridad de la Información y Ciberseguridad.

Asimismo, y para garantizar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad, a través de cada uno de sus departamentos, deberá:

- ✓ Participar activamente en el ciclo de vida de desarrollo de los sistemas, especialmente en la autorización de los mismos antes de entrar en operación.

- ✓ Realizar evaluaciones periódicas del estado de seguridad de la información y ciberseguridad, solicitando la revisión por parte de terceros para disponer de una evaluación independiente.

➢ Detección y respuesta

Las medidas de prevención no son siempre suficientes ante incidentes de seguridad, por lo que se monitorizará de manera continua el funcionamiento de los sistemas de información de cara a identificar anomalías en su operación.

Ante la detección de un incidente de seguridad de la información y ciberseguridad, se pondrán en marcha los mecanismos de verificación, análisis y comunicación del mismo.

➢ Recuperación

Para aquellos casos en que los incidentes causen un impacto importante, se dispondrá de planes de continuidad de los sistemas, asegurando que se encuentran integrados con los planes generales de continuidad de negocio y actividades de recuperación.

6. Responsables de activos de información:

En ASESORIAS E INVERSIONES FSJ SPA cada activo de información debe tener un responsable designado que sea responsable de su protección y gestión adecuadas. Estos responsables tienen las tareas de:

- ➢ Identificar y clasificar los activos de información bajo su custodia, asegurándose de comprender su importancia y sensibilidad.
- ➢ Establecer controles de seguridad adecuados para proteger los activos de información, basados en las evaluaciones de riesgos y los requisitos de seguridad.
- ➢ Definir los requisitos de acceso y autorización para los activos de información, asegurándose de que sólo se otorguen los privilegios necesarios para la ejecución de sus funciones.
- ➢ Supervisar y revisar regularmente la efectividad de los controles de seguridad implementados y tomar medidas correctivas cuando sea necesario.
- ➢ Colaborar con otros responsables de activos de información y con el equipo de gestión de seguridad de la información para garantizar una gestión coherente y eficaz de los activos de información en toda la organización.

6.1 Trabajadores de ASESORIAS E INVERSIONES FSJ SPA:

Todos tienen responsabilidades en la seguridad de la información y deben cumplir con esta Política y los procedimientos que de ella deriven. Esto incluye:

- ➢ Conocer y cumplir la Política y procedimientos de seguridad de la información de ASESORIAS E INVERSIONES FSJ SPA incluida la clasificación de los activos de la información y el manejo adecuado de la información confidencial.
- ➢ Participar en programas de capacitación y concientización sobre seguridad de la información para comprender los riesgos y las mejores prácticas de seguridad.
- ➢ Informar cualquier incidente de seguridad o vulnerabilidad detectada a los responsables designados (Líder de equipo y responsable de TI) y cooperar en la resolución de dichos incidentes.
- ➢ Utilizar los activos de información de manera responsable y asegurarse de protegerlos contra pérdidas, robos o daños físicos.

6.2 Prestadores de servicios (contratistas, proveedores o asesores).

Es importante establecer medidas de seguridad de la información para los prestadores de servicios que

interactúan con ASESORIAS E INVERSIONES FSJ SPA como contratistas, proveedores o asesores, las que considerarán a lo menos:

- **Acuerdos de Confidencialidad y Cláusulas de Seguridad:** Establecemos acuerdos de confidencialidad que definan claramente la responsabilidad de los prestadores de servicios para proteger la información confidencial y cumplir con las políticas de seguridad de la información de la ASESORIAS E INVERSIONES FSJ SPA

- **Control de Acceso y Autenticación:** Los prestadores de servicios deben acceder solo a los recursos y datos necesarios para llevar a cabo sus funciones. Se debe implementar autenticación segura y control de acceso basado en roles.

- **Capacitación y Sensibilización:** Proporcionamos capacitación sobre las políticas de seguridad de la ASESORIAS E INVERSIONES FSJ SPA y las mejores prácticas para proteger la información confidencial, según el tipo de prestación de servicio.

- **Cifrado y Protección de Datos:** Nos aseguramos de que nuestros datos estén encriptados adecuadamente y protegidos durante la manipulación y almacenamiento de nuestros proveedores.

- **Revocar de Acceso**: Contamos con un procedimiento para revocar el acceso a los prestadores de servicios cuando finalice la relación de servicio.

- **Informe de Brechas e Incidentes**: Contamos con cláusulas en los acuerdos que exija a los prestadores de servicios informar cualquier brecha o incidente de seguridad de manera inmediata.

Estas medidas son personalizadas según las características o naturaleza de nuestros prestadores de servicios con los que trabajamos. La clave es garantizar la protección de la información confidencial y mantener una colaboración segura y confiable.

6.3 Asesores Externos de ASESORIAS E INVERSIONES FSJ SPA (visión futura)

El trabajo seguro con Asesores externos de ASESORIAS E INVERSIONES FSJ SPA implica un enfoque holístico de seguridad de la información. Pese a que nuestros Asesores externos suelen tener sus propias políticas de seguridad, trabajar juntos para establecer estándares compartidos y asegurar la protección de los datos confidenciales es fundamental para mantener la confianza y la integridad en la relación entre las partes.

Las medidas tomadas son las siguientes:

- **Acuerdos de Confidencialidad:** Acuerdos de confidencialidad sólidos con nuestros Asesores Externos antes de compartir cualquier información confidencial. Esto crea una base legal para asegurar que la información no será compartida o utilizada de manera inapropiada.

- **Acceso Controlado:** Otorgamos acceso a la información confidencial solo a las personas que realmente necesitan conocerla. Utilizamos sistemas de autenticación y autorización sólidos para asegurarte de que solo los usuarios autorizados tengan acceso.

- **Encriptación:** Encriptamos los datos confidenciales tanto en tránsito (en proceso de envío en el caso de un correo) como en reposo (guardados en nuestros equipos). Esto ayudará a prevenir que terceros no autorizados accedan a la información incluso si logran interceptarla.

- **Plataformas Seguras:** Utilizamos plataformas y servicios seguros para compartir información confidencial. Esto lo determina nuestro encargado de TI y con el equipo o encargado de Ciberseguridad quien revisa las plataformas y poniendo énfasis en las versiones, actualizaciones, protocolos, estándares, entre otros detalles.

- **Auditorías Regulares:** Realizamos auditorías periódicas para evaluar la seguridad de la información compartida con los asesores externos. Esto nos ayuda a identificar posibles vulnerabilidades o puntos débiles en el sistema.
- **Capacitación y Sensibilización:** Realizamos capacitaciones regular a los empleados y asesores externos sobre las mejores prácticas de seguridad de la información. La sensibilización es fundamental para prevenir amenazas internas y errores accidentales, como se menciona en el en el ítem de "Responsabilidades" en el punto 3 en las responsabilidades de los trabajadores de la ASESORIAS E INVERSIONES FSJ SPA

- **Gestión de Contraseñas:** Damos credenciales de acceso al "Portal Empresa" de forma controlada, asegurándonos de que las contraseñas sean seguras, cambiables periódicamente (2 veces al año), enviando recordatorio y realizando monitoreo a los "Log Access" y votando sesión según tiempo de inactividad máximo 30 min.

- **Control de Versiones:** Utilizamos un sistema de control de versiones para rastrear cambios y asegurar de que solo las versiones autorizadas estén disponibles, almacenando nuestras versiones oficiales en Sharepoint con acceso restringido solo a personal autorizado.

- **Notificación de Brechas**: Contamos con un plan de acción claro en caso de una violación de seguridad. Esto incluye notificar a las partes afectadas y tomar medidas para mitigar los daños.

6.4 Equipo de Gestión de la Seguridad de la Información:

El Gerente de Operaciones encabezará un equipo de Gestión de la Seguridad de la Información encargado de la estrategia de seguridad de la información de la ASESORIAS E INVERSIONES FSJ SPA y de supervisar y monitorear las actividades relacionadas con la Política de Seguridad de la información. Este equipo tiene las siguientes responsabilidades:

- Coordinar la identificación y clasificación de activos de información y asegurarse de que se asignen responsables.
- Establecer controles de seguridad apropiados y evaluar regularmente su efectividad.
- Realizar evaluaciones de riesgos y gestionar las vulnerabilidades y amenazas identificadas.
- Realizar evaluaciones de riesgos y gestionar las vulnerabilidades y amenazas identificadas, implementando medidas de mitigación adecuadas.
- Establecer y mantener políticas y procedimientos de seguridad de la información, asegurándose de que sean consistentes con los requisitos de las distintas normas y otras regulaciones aplicables.

- Supervisar el cumplimiento de las políticas de seguridad de la información y realizar al menos una auditoría interna periódica para identificar debilidades, proponer mejoras continuas, validar si las políticas se están cumpliendo y prepararnos para una auditoría externa.

- Mantenerse actualizado sobre las mejores prácticas y avances en seguridad de la información, y proponer mejoras y actualizaciones según sea necesario.

- Actuar como punto focal para la gestión de incidentes de seguridad de la información, coordinando la respuesta a incidentes, investigando y documentando los incidentes, y tomando medidas correctivas para evitar futuras incidencias.

- Fomentar una cultura de seguridad de la información en toda la organización a través de programas de capacitación al personal que se integre a los distintos equipos de ASESORIAS E INVERSIONES FSJ SPA plan

de concientización y promoción de buenas prácticas de seguridad con actividades, como charlas, correos informativos y evaluaciones. De estas actividades deberá mantener un registro y archivo quedarán con el objeto de poder reutilizar dicho material para inducciones u otras instancias.

- Mantener una comunicación efectiva con la alta dirección y otras unidades y equipos relevantes para garantizar la alineación de estos con las Política de Seguridad de la Información.

El Gerente de Operaciones designará un responsable de la operatoria diaria para asegurar la implementación efectiva de la presente Política.
El equipo de gestión de seguridad de la información desempeña un papel fundamental en la implementación y mantenimiento de un entorno seguro para los activos de información de ASESORIAS E INVERSIONES FSJ SPA Su experiencia y conocimiento en seguridad de la información ayudan a garantizar que se apliquen medidas adecuadas y se tomen acciones proactivas para proteger la confidencialidad, integridad y disponibilidad de los activos de información, y para cumplir con los requisitos de las normas y otras regulaciones pertinentes.

7. Consecuencias del incumplimiento

Toda infracción o incumplimiento a esta política será considerado incumplimiento grave de las obligaciones que impone el contrato de trabajo a los colaboradores de ASESORIAS E INVERSIONES FSJ SPA El incumplimiento de esta política faculta a ASESORIAS E INVERSIONES FSJ SPA a aplicar las sanciones que se contemplan el Reglamento Interno de Higiene, Orden y Seguridad, sin perjuicio de las acciones judiciales que puedan dirigirse contra el transgresor para hacer efectiva su responsabilidad tanto civil como penal.

Toda infracción o incumplimiento de esta Política por parte de los socios de la ASESORIAS E INVERSIONES FSJ SPA puede resultar en medidas disciplinarias contempladas en los estatutos de ASESORIAS E INVERSIONES FSJ SPA determinadas por la Comisión de Ética previa investigación de la Gerencia de Operaciones y el oficial de Cumplimiento, sin perjuicio de las acciones judiciales que puedan dirigirse para hacer efectiva la responsabilidad tanto civil como penal.

Toda infracción o incumplimiento de esta Política por parte todos aquellos que presten servicios a la ASESORIAS E INVERSIONES FSJ SPA como contratistas, gestores de residuos, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ASESORIAS E INVERSIONES FSJ SPA puede resultar en sanciones o consecuencias de acuerdo con lo previsto en los respectivos contratos, sin perjuicio de las acciones judiciales que puedan dirigirse para hacer efectiva la responsabilidad tanto civil como penal.

8. Medidas de Seguridad

- **Acceso y control de la información:**

- ✓ **Identificación y autenticación:** Implementamos mecanismos de identificación y autenticación para garantizar que solo los usuarios autorizados puedan acceder a los activos de información. Esto incluye el uso de contraseñas seguras, autenticación multifactorial y el control de accesos basado en roles.

- ✓ **Control de acceso:** Establecimos políticas y procedimientos para gestionar los permisos de acceso a los activos de información, asegurando que los usuarios tengan los derechos y privilegios adecuados según sus funciones y responsabilidades. Además, se revisarán y actualizarán regularmente los derechos de acceso para evitar privilegios innecesarios o no autorizados.

- ✓ **Gestión de sesiones:** Implementamos controles para gestionar y controlar las sesiones de usuario, incluyendo el cierre automático de sesiones inactivas, el registro de actividad de inicio de sesión y la detección de actividades sospechosas.

- **Protección contra software malicioso:**

- ✓ **Antivirus y antimalware:** Implementamos soluciones antivirus y antimalware actualizadas y eficaces en todos los sistemas y dispositivos utilizados en ASESORIAS E INVERSIONES FSJ SPA Estas soluciones se configurarán para realizar escaneos periódicos, mantener las definiciones de virus actualizadas y generar alertas en caso de detección de amenazas.

- ✓ **Actualizaciones y parches de seguridad:** Mantenemos un programa de gestión de parches y actualizaciones para garantizar que todos los sistemas y aplicaciones utilizados en ASESORIAS E INVERSIONES FSJ SPA estén actualizados con las últimas correcciones de seguridad. Esto incluye la aplicación oportuna de parches críticos y la realización de pruebas de seguridad posteriores a la implementación.

- ✓ **Concientización y capacitación:** Realizamos capacitaciones de manera regular a los trabajadores de ASESORIAS E INVERSIONES FSJ SPA sobre la importancia de la seguridad informática, incluyendo la detección de software malicioso, el manejo seguro de archivos adjuntos y enlaces, y las prácticas recomendadas para evitar infecciones.

- ➢ **Seguridad de la red:**

- ✓ **Perímetro de seguridad:** Implementamos firewalls y dispositivos de seguridad de red para controlar y monitorear el tráfico entrante y saliente, y para prevenir ataques externos no autorizados. Se establecerán políticas de filtrado para permitir únicamente el tráfico legítimo y se realizarán pruebas periódicas de penetración para evaluar la efectividad de las medidas de seguridad.

- ✓ **Detección y prevención de intrusiones:** Utilizamos sistemas de detección y prevención de intrusiones para monitorear y analizar el tráfico de red en busca de actividades sospechosas o maliciosas. Estos sistemas generarán alertas en tiempo real y tomarán medidas preventivas para mitigar cualquier intento de intrusión.

- ✓ **Seguridad inalámbrica**: Implementaremos medidas de seguridad adecuadas para proteger nuestras redes inalámbricas, como el uso de autenticación segura, encriptación de datos y segmentación de redes. También se establecerán políticas y procedimientos para el uso seguro de dispositivos móviles y la conexión a redes externas.

9. Prevención de delitos informáticos

La gestión adecuada de la seguridad de la información y ciberseguridad mejora los procesos corporativos, evita el acceso no autorizado a información sensible de ASESORIAS E INVERSIONES FSJ SPA y sus asociados, y crea un entorno de control que previene conductas delictivas de los colaboradores en el ámbito informático.
En este sentido, todo el que ocupa un cargo, función o posición en ASESORIAS E INVERSIONES FSJ SPA incluyendo directores, ejecutivos principales y trabajadores, además de los Asesores Externos de ASESORIAS E INVERSIONES FSJ SPA y todos aquellos que presten servicios a la ASESORIAS E INVERSIONES FSJ SPA como contratistas, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de ASESORIAS E INVERSIONES FSJ SPA tienen prohibido cometer conductas ilícitas a través de medios informáticos o en contra de sistemas informáticos. Dichas conductas se encuentran sancionadas en la Ley N°21.459, que establece normas sobre delitos informáticos, los cuales se describen a continuación.

- ➢ **Ataque a la integridad de un sistema informático (sabotaje informático):**

Consiste en obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos (art. 1° ley 21.459).

- ➢ **Acceso ilícito:**

Acceder a un sistema informático sin autorización o excediendo la autorización que se posea y superando barreras técnicas o medidas tecnológicas de seguridad. La pena se agrava si el acceso fuere realizado con el ánimo de

apoderarse o usar la información contenida en el sistema informático. También se castiga la divulgación de la información a la cual se accedió de manera ilícita (art. 2° ley 21.459).

- **Interceptación ilícita:**

Interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. También captar, sin contar con la debida autorización, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos (art. 3° ley 21.459).

- **Ataque a la integridad de los datos informáticos (sabotaje de datos):**

Alterar, dañar o suprimir indebidamente datos informáticos, siempre que con ello se cause un daño grave al titular de estos mismos (art. 4° ley 21.459).

- **Falsificación informática:**

Introducir, alterar, dañar o suprimir indebidamente datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (art. 5° ley 21.459).

- **Receptación de datos informáticos:**

Se sanciona al que, conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas de acceso ilícito, interceptación ilícita y falsificación informática (art. 6° ley 21.459).

- **Fraude informático:**

Manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero. Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito (art. 7° ley 21.459).

- **Abuso de los dispositivos:**

Sanciona al que para la perpetración de los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos y delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos (art. 8° ley 21.459).

10. Comunicación de la Política

Para asegurar la efectiva implementación de esta Política, es fundamental que todo el personal esté al tanto de su contenido, además de conocer los aspectos relevantes de la normativa aplicable. Asimismo, es necesario que todos los colaboradores comprometan su adhesión a ésta.

Con el fin de asegurar que todos los colaboradores de la ASESORIAS E INVERSIONES FSJ SPA estén debidamente informados sobre esta materia, además de las disposiciones incorporadas a sus contratos de trabajo y Reglamento Interno de Orden Higiene y Seguridad, ASESORIAS E INVERSIONES FSJ SPA ha dispuesto las siguientes medidas de comunicación:

- La información relacionada a la presente Política estará disponible para todo el personal de ASESORIAS E

INVERSIONES FSJ SPA en sus redes de comunicación internas y externas;

- Difusión sobre buenas prácticas, controles, obligaciones y prohibiciones para prevenir la comisión de delitos; y

- Capacitación regular y continua.

11. Actualización y revisión continua de la Política

Esta Política se revisará y actualizará anualmente o cuando sucedan cambios en ASESORIAS E INVERSIONES FSJ SPA que justifiquen su modificación.

12. Marco Organizativo

La seguridad de los activos de la información es responsabilidad de todos los departamentos de la empresa, así como de todas y cada una de las personas que interaccionen con los mismos.

No obstante, el Directorio tiene atribuida la coordinación, dentro de los límites legales, de las estrategias y directrices generales de gestión del Grupo, operando en interés de todas y cada una de las sociedades que lo integran, correspondiendo, por su parte, al presidente del Directorio y consejero delegado y a los altos directivos de la Sociedad la función de organización y coordinación del Grupo mediante la difusión, implementación y seguimiento de la estrategia y políticas generales establecidas por el Directorio.

Al amparo de lo anterior, el Directorio a través de su Comité de Seguridad y Oficial de Cumplimiento, velará por el seguimiento de los principios y buenas prácticas que se contienen en esta política corporativa por parte de las sociedades integradas en el Grupo.

El Directorio delegará a su vez en el Comité de Seguridad la supervisión y cumplimiento de esta política.

13. Seguimiento y control

ASESORIAS E INVERSIONES FSJ SPA adoptará los mecanismos de control necesarios para asegurar, dentro de una adecuada gestión empresarial, el cumplimiento de la normativa, de los principios y las buenas prácticas enunciadas en esta política. Igualmente, dedicará a tales fines los recursos humanos y materiales adecuados y suficientemente cualificados. Se aprobarán y revisarán periódicamente unas directrices para evaluar y gestionar el riesgo identificado, aplicables a todo el Grupo, que incluirán unos criterios objetivos para clasificar las operaciones en función de su riesgo, así como distintos procedimientos para su aprobación.

14. Control de Distribución

Fecha	Responsable	Canales de distribución
30/12/2024	Oficial de Cumplimiento	Comunicado envío por correo electrónico.

15. Modificaciones

No aplica