1. OBJETIVO

Establecer los lineamientos referentes a la seguridad de la información en las relaciones con los proveedores que garantice la protección de los activos de la organización que sean accesibles por terceros.

2. ALCANCE

Estas normas son de obligatorio cumplimiento por parte de todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica del Grupo MOK.

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Aceptación del riesgo: Decisión de asumir el riesgo.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una compañía autorizada.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Periférico: dispositivo electrónico físico que se conecta o acopla a una computadora u otro dispositivo informático, pero no forma parte del núcleo básico.

Proveedor: es una empresa o persona física que proporciona bienes, servicios o recursos a otras personas o empresas.

Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Valoración del riesgo: proceso global de análisis y evaluación del riesgo.

4. DIRECTRICES

4.1 Relaciones con los Proveedores.

GRUPO MOK vela por mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes o que son procesados, comunicados o dirigidos a estos.

4.1.1 Seguridad de la Información en las relaciones con los proveedores.

- El Grupo MOK debe elaborar modelos de Acuerdos de Confidencialidad. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.
- El Grupo MOK velará por las condiciones de comunicación segura mediante mensajería autorizada, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- La transmisión y/o transferencia de información podrá tener requisitos de cifrado de acuerdo con la Política de criptografía y/o requisitos del negocio dentro de la relación contractual.
- Las partes garantizarán un nivel adecuado de seguridad para evitar fuga, robo, o uso de información confidencial o patentada y acepta que protegerán la información confidencial y reservada de cada una, realizando el debido almacenamiento de esta, por la parte receptora.
- El área de TI y Riesgos mitigará los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la compañía.
- El área de Riesgos y Seguridad de la Información, evaluará y aprobará los accesos a la información de la compañía requeridos por terceras partes.

- El área de TI y Riesgos identificará, evaluará y monitoreará los riesgos relacionados con terceras partes a los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología.
- Las personas responsables de contratos con terceros se asegurarán de divulgar las políticas, normas y procedimientos de seguridad de la información de la compañía que apliquen, así como velar por que el acceso a la información y a los recursos de almacenamiento o procesamiento se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.
- En los contratos o acuerdos con proveedores será necesario incluir una cláusula de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las Políticas de Seguridad de la Información.
- A todos los proveedores se les compartirá y/o informará las políticas corporativas de seguridad de la información de **GRUPO MOK** y estos implementaran medidas para cumplirla.
- El área de Seguridad de la Información de **GRUPO MOK** realizará capacitaciones o informar a los proveedores de la empresa en temas de seguridad de la información.

4.1.2 Gestión de la prestación de servicios de proveedores:

- **GRUPO MOK** velara por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.
- El área de TI verificará en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la compañía.
- El área de TI verificará las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia terceros.

- El área de TI, y los supervisores de contratos con terceros, monitoreará periódicamente, el Acuerdo de intercambio de información y los requisitos de seguridad de la información de parte de los proveedores de servicios.
- Los responsables de los contratos con terceros, con el apoyo del área de TI, administrará los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.
- Los responsables de contratos con terceros, con el apoyo del área de TI, administrará los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos, igualmente se verificará la aparición de nuevos riesgos.

4.1.3 Seguridad en los Acuerdos con los Proveedores.

Las condiciones de seguridad de la información quedarán reflejadas en los contratos firmados con los proveedores por parte de Grupo MOK y en un apartado específico para ello. Los documentos sobre los acuerdos para la seguridad de la información estarán firmados por ambas partes.

Este es un listado de requisitos de seguridad que el Grupo MOK puede exigirles a sus proveedores según el tipo de servicio prestado:

- **Responsable de seguridad:** en calidad de contratante, el Grupo MOK le podrá solicitar siempre y cuando sea necesario a su proveedor la designación de un responsable de seguridad quien servirá de interlocutor para cualquier tema de seguridad y el responsable de que se cumplan los controles pactados entre las partes.

- **Control de Personal:** el Grupo MOK se reservará el derecho de requerir a sus proveedores que le mantenga informado de cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado. En caso de ser necesario, se definirá como y cuando se realizarán las comunicaciones.

  Nota: Los proveedores que tengan algún tipo de relación con Grupo MOK incluirán como requisito en sus políticas que todo el personal que ha sido dado de baja le sea revocado los permisos de acceso tanto a las instalaciones como a los sistemas de información.

- **Requisitos Legales:** Grupo MOK verificará que todos los proveedores cumplan con los requisitos legales sobre el negocio enmarcados en la seguridad de la información del estado colombiano, entre ella la información de derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional. Esto quedará especificado en los contratos que la empresa tenga con sus proveedores independiente del tipo de servicio prestado.

- **Uso de Activos:** Grupo MOK garantizará el uso correcto de sus activos donde los proveedores se comprometen al uso de activos para la finalidad prevista y que tomaran las medidas de control que se establezcan para evitar el daño o revelación de la información y los accesos no autorizados.

- **Revisiones de controles de Seguridad:**
  - El personal de Seguridad de la Información de **GRUPO MOK** generará, ejecutará y monitoreará revisiones periódicas a los proveedores que presten servicios relacionados con los sistemas de información.
  - Grupo MOK establecerá condiciones para la realización de revisiones de puntos de control de seguridad en las instalaciones de los proveedores.

- Grupo MOK garantizará los recursos necesarios para la realización de evaluaciones y/o revisiones de puntos de control con el fin de garantizar la regularidad de la verificación al personal, procedimientos y controles dependientes del proveedor que intervengan en la prestación de servicios.
- La vigilancia y supervisión del cumplimiento de los contratos, estará a cargo del funcionario que sea designado por GRUPO MOK. En desarrollo de la labor de supervisión, el podrá efectuar en cualquier momento, por escrito o verbalmente, requerimiento o sugerencias para que EL PROVEEDOR actúe preventiva o correctivamente, con la finalidad de que los contratos se ejecuten de conformidad con los términos establecidos en el mismo.

  Nota: La anterior cláusula se aplicará de manera exclusiva a los proveedores críticos, sean personas naturales o jurídicas.

- **Control de Procedimientos:** Se generarán cláusulas específicas, con el fin de que el proveedor mantenga procesos de seguridad en todas las actividades desarrolladas que involucren al Grupo MOK y sus clientes.

  a) **Procesos de devolución o destrucción de la información a la finalización del acuerdo:** Se debe proteger la difusión de información confidencial una vez se dé por finalizado el contrato con el proveedor, por lo cual se realizará la respectiva devolución o destrucción de la información digital y/o física que le fue entrega al contratista. Lo anterior, ayudará a salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información que administre en el marco del objeto del contrato suscrito con Grupo MOK.

  b) **Planes de formación en seguridad de la información:** Se establecerá un programa de capacitación de proveedores para mantener la concientización sobre seguridad de la información. Esto se realizará por medio del envío de capsulas, a través de una comunicación externa emitida por Grupo MOK.

c) **Procedimientos de control de cambios:** Se podrá controlar la implementación de cambios en los procesos de los proveedores utilizando procedimientos formales de control de cambios. Estos procedimientos podrán ser documentados y por tal motivo es necesario cumplirlos para minimizar la corrupción de los sistemas de información y que no se vea afectada la prestación del servicio por parte del proveedor. La inclusión de sistemas o procesos nuevos importantes en los sistemas ya existentes seguirán un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Estos procesos podrían incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios

También es necesario garantizar que la seguridad y los procesos de control existentes no se ponen en peligro permitiendo una prestación normal del servicio por parte de los proveedores. Los procedimientos de control pueden incluir:

- La garantía de que los cambios son realizados por las personas autorizadas.
- El mantenimiento de los niveles de servicio estipulados en el contrato.
- La revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.
- En caso de ser un cambio que afecte aplicativos utilizados por el proveedor para la prestación del servicio, se identificará todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.

- La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.
- La garantía de que las partes interesadas acepten los cambios antes de la implementación.
- La garantía de que la documentación del proceso este actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.
- La programación de revisiones de seguridad que incluya todos los cambios realizados en la prestación del servicio por parte del proveedor.
- El mantenimiento de una versión de control para todas las actualizaciones de software.
- La garantía de que los procedimientos y procesos se cambian en función de una necesidad con el objeto de mantener su idoneidad. Lo anterior estará debidamente documentado.
- La garantía de que la implementación de los cambios en los procesos de los proveedores tiene lugar oportuno y no perturba los procesos del negocio involucrados.

d) Procesos de tratamiento de incidencias u no conformidades: El tratamiento de las incidencias u no conformidades permite garantizar la disponibilidad de los servicios prestados por los proveedores y los mecanismos de revisión y resolución de interrupciones y degradaciones que se presenten en la prestación de los servicios, para garantizar la misma según los acuerdos establecidos con los clientes.

Por norma general, en los procesos productivos o de prestación de servicio existirán tres fuentes de no conformidades que podrían originar el correspondiente informe:

- **Incidencias con proveedores:** Entregas de material en mal estado o incumplimiento de plazos establecidos.
- **Incidencias en controles internos:** Errores detectados en la propia organización durante los controles realizados durante el desarrollo del proceso productivo o de prestación del servicio.
- **Reclamaciones de clientes:** Productos o servicios defectuosos que han superado los controles de la organización y que han sido detectados por el cliente.

El Grupo MOK cuenta con un documento **(GRI-PD-004 Procedimiento de Gestión de eventos e incidentes SI)** en el cual se detalla el paso a seguir en caso de presentarse incidencias u no conformidades con alcance a las partes interesadas. Lo anterior, podrá quedar especificado a través de una cláusula en los convenios y/o contratos firmados por Grupo MOK y sus proveedores según el servicio prestado.

e) Procesos de escalado en la resolución de incidencias: Cuando ocurra una incidencia u no conformidad, el Grupo MOK la escalará según las actividades previamente definidas en la cláusula 8 del **GRI-PD-004 Procedimiento de Gestión de eventos e incidentes SI** para de esta forma darle solución.

f) Procesos de actualización de software y programas de seguridad: Grupo MOK cuenta con cláusulas específicas sobre el control de software operacional en los convenios con proveedores o partes interesadas, las cuales aseguran que las áreas de TI, Riesgos y Seguridad de la Información validarán los riesgos que genera la migración hacia nuevas versiones del software operativo. Es necesario asegurar el correcto funcionamiento de los sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Adicionalmente, el área de TI puede ejecutar un plan de actualizaciones para el software, aplicaciones y librerías de programas, así como un informe de dichos parches y/o actualizaciones, que llevarán a cabo el personal de la Mesa de Servicios, con generación y revisión de los informes de forma semanal y es aplicable a las partes interesadas. Para mayor información véase **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**

g) Planes de emergencia y de recuperación de desastres (Plan de continuidad del negocio): Grupo MOK tiene establecido mediante cláusulas en los contratos o convenios firmados con los proveedores que se maneje un BCP (Plan de Continuidad de Negocio) que permita asegurar los ANS (Acuerdos de Nivel de Servicio) estipulados inicialmente en los contratos para así no afectar la prestación del servicio.

- **Control de Software Malicioso (Virus):** Se tienen requisitos establecidos para el control de virus y software malicioso de equipos y soportes que se conectan a la red de Grupo MOK. Al igual que se controla la obligación de mantener los antivirus actualizados. El Grupo MOK asegurará que sus proveedores han tomado medidas de control y establecido políticas para los usuarios sobre el uso de redes, emails y aplicaciones que prevengan el software malicioso. Lo anterior, se encuentra establecido en **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**

- **Uso del Software:** El Grupo MOK tiene cláusulas sobre el uso de software autorizado, la prohibición de software privado o quienes son las personas autorizados para la instalación de software gratuito, las cuales están pactadas en las Políticas Corporativas de Seguridad de la Información, en donde la compañía asegurará que todo el software que se ejecuta en el Grupo MOK y es utilizado por los proveedores este protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software libre de distribución y uso. Los empleados y partes interesadas cumplirán con las leyes de derechos de autor y acuerdos de licenciamiento de software, es

ilegal duplicar software sin la autorización del propietario de los derechos de autor bajo licencia otorgada. Véase en **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**

- **Gestión de Incidentes:** El Grupo MOK gestionará el manejo de incidentes y contingencias asociadas con el acceso a los sistemas de información por parte de los proveedores, incluidas las responsabilidades tanto de la compañía como de los proveedores. De igual forma, se asegurará que los eventos e incidentes de seguridad de la información que se presentan en los activos de información de la compañía y tengan relación con las partes interesadas sean comunicados y atendidos oportunamente, aplicando los procesos definidos con el fin de tomar oportunamente las acciones correctivas.

  El área de TI contará con un diagrama de red para tener la ubicación rápida de los recursos existentes. Para mayor información véase en **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**

- **Desarrollo de Software:** Grupo MOK estableció cláusulas para controlar el desarrollo de software por parte de los proveedores, estas están disponibles en la sección de Requisitos de Seguridad de los sistemas de información disponible en las Políticas Corporativas de Seguridad de la Información. **(Ver documento).**

- **Equipos Informáticos:** En el Grupo MOK no existe el acceso a los activos informáticos por parte de proveedores y si se diera el caso, se debe realizar bajo expresa autorización del área de TI con condiciones específicas.

- **Autenticación:** El Grupo MOK estableció una política para el uso general de sus contraseñas. Esta política establece los parámetros y lineamientos diseñados en torno a la calidad de las contraseñas que deben ser tenidas en cuenta por todos los funcionarios, proveedores y partes interesadas que tengan acceso a los sistemas de información del Grupo MOK como estrategia de mitigación del riesgo y seguridad de la información.

El contratista será el responsable de los daños causados por el incumplimiento de las normas de gestión de contraseñas contenidas en este apartado y de las responsabilidades legales establecidas por el Grupo MOK. Véase el documento **GI-PLT-003 Política General de Contraseñas.**

- **Uso y Conexión de Redes Informáticas:** Grupo MOK velará por la protección de las redes de datos y los recursos de red, mediante controles de acceso lógicos que evita el acceso no autorizado, debido a esto se tiene una Política de Control de Acceso que establece las pautas para la conexión y transmisión de datos cuando sea aplicable al proveedor. Véase el documento **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**

- **Obligaciones del personal:** A continuación, se especifican las obligaciones a las que están sujetas las personas que prestan servicio dentro de los acuerdos firmados con los proveedores:

    - Cumplirán con las obligaciones de seguridad de la compañía. Ver documento **(CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.)**
    - Conocerán y seguirán las recomendaciones de los planes de emergencia y de respuesta ante los incidentes de seguridad de la información del Grupo MOK. Ver documento **PCN-A-001 BIA GRUPO MOK.**
    - Grupo MOK estableció cláusulas obligatorias de cumplimiento en la gestión de identificaciones y credenciales de acceso a los sistemas de información por parte de terceros. Por tal motivo se ha dispuesto la **GI-PLT-003 Política General de Contraseñas** y la **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**
    - En el caso donde los proveedores tengan la necesidad de trabajar en sitio (instalaciones de Grupo MOK), deberán cumplir con la política de escritorio limpio que la compañía tenía establecida según las recomendaciones de la norma ISO 27001.

- El área de TI asegurará que los sistemas de información adquiridos y desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual. Ver las **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**
- Grupo MOK tiene establecido una política de protección de datos personales que menciona las obligaciones de los proveedores y el tratamiento que debe darse a los datos según la ley.
- El Grupo MOK estableció una serie de cláusulas sobre la responsabilidad de los activos de información, la custodia, su finalidad y la devolución al momento de finalizar el vínculo comercial con los proveedores. Esta información se encuentra definida en los contratos realizados con terceras partes y en las **CO-SI-PLT-001 Políticas Corporativas de Seguridad de la Información.**
- **GRUPO MOK**, con el apoyo del personal de Seguridad de la Información y Protección de Datos, establecerán acuerdos de confidencialidad y no divulgación con las terceras partes con quienes se realice dicho intercambio durante y después de la finalización de la relación contractual.

- **Obligaciones sobre las instalaciones:** Se establecerán requisitos para la seguridad en el trabajo en las instalaciones de Grupo MOK tales como:

  - Durante la visita de terceros a las instalaciones deberán portar en todo momento el carnet de visitante en un lugar visible.
  - Cumplir con los controles de acceso de acuerdo a lo establecido en la Política de Control de Acceso Físico.
  - Los lineamientos de comportamientos no permitidos están definidos en la Política de Control de Acceso Físico.
  - Cumplir con las políticas de buen uso de las instalaciones.

4.1.4 Cadena de suministro de tecnologías de la información y comunicación.

El área de TI y Riesgos identificará, evaluará y monitoreará los riesgos relacionados con terceras partes a los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología. Grupo MOK verificará que los acuerdos con proveedores incluyan requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación y el proveedor será el responsable de tratar estos riesgos aplicables a su cadena de suministro.

Se incluirán los siguientes temas en los acuerdos con los proveedores, concernientes a la seguridad de la cadena de suministro:

- Determinar los requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología de la información y de comunicaciones, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores.
- Implementar evaluación de seguridad en la cadena de suministro para proveedores que manejen información crítica.
- Exigir para los servicios de tecnología de información y de comunicaciones, que los proveedores divulguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro, si los proveedores contratan externamente partes del servicio de tecnología de la información y comunicaciones que suministran al Grupo MOK.
- Requerir que los proveedores divulguen prácticas de seguridad adecuadas a lo largo de la cadena de suministro, para los servicios y/o productos de tecnología de información y comunicaciones, si estos servicios y/o productos incluyen componentes comprados a otros proveedores.

- Grupo MOK implementará un proceso de seguimiento y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos de seguridad establecidos.
- Es necesario ejecutar un proceso para identificar los componentes de los productos o servicios que son críticos para mantener la funcionalidad, y, por tanto, requieren una mayor atención y escrutinio cuando se construyen por fuera del Grupo MOK, especialmente si el proveedor en de clasificación tipo A contrata externamente aspectos de componentes de productos o servicios a otros proveedores.
- Se definirán reglas para compartir información concerniente a la cadena de suministro y cualquier problema y compromisos entre el Grupo MOK y los proveedores por medio de correo electrónico o llamadas en caso de ser necesario.
- Llevar a cabo procesos específicos para la gestión del ciclo de vida y la disponibilidad de componentes de tecnología de información y de comunicación, y de los riesgos de seguridad asociados. Esto incluye la gestión de riesgos de componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o ya no suministran estos componentes debido a que se han hecho avances en la tecnología.

4.2 Gestión de la entrega del servicio por terceras partes.

Grupo MOK velará por mantener un nivel apropiado de seguridad de la información y la entrega del servicio acorde con los convenios realizados con sus terceras partes. A parte de establecer los requisitos de seguridad, se procurará por mantenerlos a lo largo del tiempo, verificar que se cumplan, por lo cual será necesario controlar los servicios prestados y los cambios que se puedan presentar en los mismos.

4.2.1 Seguimiento y revisión de los servicios de proveedores

Realizar un seguimiento y revisión con regularidad de la prestación de servicios de los proveedores con los que Grupo MOK tenga vínculos comerciales, que abarque:

- Garantizar que los términos y condiciones de seguridad de la información de los convenios se cumplan, y que los incidentes y problemas de seguridad de la información se gestionan de forma adecuada.
- Definir un proceso de relacionamiento para la gestión del servicio que se presente entre el Grupo MOK y el proveedor con el fin de:

    - Velar por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, Grupo MOK velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.
    - Examinar los reportes de servicio diseñados por el proveedor, para así agendar reuniones de avance regulares, según lo determinado en los acuerdos.
    - Programar revisiones periódicas a los proveedores, de la mano con el análisis de reportes de auditores independientes, solo si se encuentran disponibles, y acciones sobre las cuestiones precisadas.
    - Proporcionar información sobre incidentes o eventos de seguridad de la información para posteriormente analizarla según se exija en los convenios firmados.
    - Verificar los rastros de revisiones del proveedor, los reportes de eventos de seguridad de la información, problemas operacionales, falla e interrupciones vinculadas con el servicio prestado.
    - Solucionar y gestionar cualquier problema encontrado.

- Verificar los aspectos de seguridad de la información de las relaciones que tengan nuestros proveedores con sus propios proveedores.
- Grupo MOK asegurará que el proveedor siempre mantenga una capacidad de servicio suficiente a través de planes ejecutables destinados a mantener los niveles de continuidad del servicio acordado previamente en los convenios, después de fallas en el servicio o desastres que se puedan presentar.

4.2.2 Gestión de cambios en los servicios de los proveedores.

Gestionar los cambios en el suministro de servicios por parte de los proveedores teniendo en cuenta la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir nuevas necesidades de seguridad si así se estima oportuno. Esto puede incluir el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad que ya existan en el momento. Se tendrá presente la criticidad de la información, al igual que los sistemas y procesos del Grupo MOK que se encuentren involucrados.

Al realizar estos cambios se podrá implementar una revaloración de los riesgos de seguridad de la información, por lo cual se establecerá una cláusula en los contratos que permita notificar a Grupo MOK cualquier cambio en los servicios prestados por el proveedor. Los siguientes son aspectos a tener presente:

Los cambios hechos por el Grupo MOK para implementar:

- El desarrollo de nuevas aplicaciones y sistemas involucrados con los cambios.
- Cambios efectuados en los convenios con proveedores.
- Mejoras que se puedan presentar a los servicios que se ofrecen actualmente.

- Implementación de controles nuevos o modificados que permiten solucionar incidentes de la seguridad de la información a través de mejoras.

Cambios en los servicios de los proveedores que podrán ser implementados:

- Mejoras, actualizaciones y cambios en las redes.
- La inclusión y uso de nuevas tecnologías.
- La acogida de productos nuevos o versiones más recientes
- Ambientes de desarrollo y herramientas totalmente nuevos.
- Modificación en las ubicaciones físicas de las instalaciones de servicio de los proveedores.
- Un posterior cambio de proveedor.
- La contratación externa de proveedores diferentes.

4.3 Desarrollo Tercerizado.

Para la subcontratación de desarrollos de software, el Grupo MOK tendrá en cuenta los siguientes puntos:

- En el proceso de análisis y adquisición de paquetes de software a terceros, se considerarán aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente a eventuales cambios o modificaciones para su implantación en el Grupo MOK.
- Se incluirán acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual que tengan relación con el software contratado externamente.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas

- Si se adquieren productos de software a terceros, se seguirá un proceso formal de adquisición y prueba de calidad. Los contratos con el proveedor abordarán los requisitos de seguridad identificados.
- Establecer y supervisar el cumplimiento de los requisitos de seguridad.
- Controlar y gestionar todos los aspectos de licencias y propiedades de código fuente.
- Se establecerá una metodología y definición de las pruebas a realizar al software subcontratado, esto se hará por parte del área de TI del Grupo MOK.
- Las modificaciones a los paquetes de software o sistemas adquiridos a terceros, que aparezcan producto de su utilidad y estén relacionados con la seguridad de la información, serán aprobados por el área de TI y por el encargado de Seguridad de la Información del Grupo MOK.
- Queda prohibido el uso y/o copia de cualquier software, por parte de los colaboradores de Grupo MOK, del cual no se disponga de su respectiva licencia que lo autorice.
- Se solicitarán certificados de depósito en garantía, en caso de que el código fuente ya no esté disponible.
- Se solicitará documentación eficaz del ambiente de desarrollo usado para crear entregables.
- El desarrollador externo deberá suministrar evidencia de que se han practicado pruebas suficientes para proteger el software contra la presencia de vulnerabilidades conocidas.
- El desarrollador externo deberá entregar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- El desarrollador externo deberá entregar evidencia de que se han practicado pruebas suficientes para certificar que no existe contenido malicioso intencional y no intencional al momento de la entrega.

- El Grupo MOK seguirá siendo responsable del cumplimiento con las leyes aplicables y con la verificación de la eficiencia de los controles.

5. CONTROL DE CAMBIOS

VERSIÓN No.	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA
01	Elaboración de la primera versión del documento.	Analista de Cumplimiento	21/09/2022

6. REGISTRO DE COLABORADORES

Elaboró	Revisó:	Aprobó:
Nombres: Natali Diaz Pardo	**Nombre:** John Ochoa	**Nombre:** Miguel Omar Ríos Cabra
Cargo: Analista de Seguridad de la Información	**Cargo:** Director de Riesgos y Seguridad Global	**Cargo:** Gerente de Cumplimiento y Seguridad Global