Tabla de contenido

1. OBJETIVO

Determinar las medidas esenciales de seguridad de la información que Grupo MOK debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.), pérdida de imagen frente a los clientes/sponsors o interrupción total o parcial de los procesos que soportan el negocio. Así mismo, proporcionar a todo el personal de Grupo MOK una herramienta que facilite la toma de decisiones apropiada, en situaciones relacionadas a la preservación de seguridad de la información.

2. ALCANCE

Estas normas son de obligatorio cumplimiento por parte de todos los empleados directos, temporales, aprendices, contratistas, consultores de GRUPO MOK y de las sedes a las cuales se les presta soporte de Tecnología. También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger estos activos de información.

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.

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.

4. INTRODUCCIÓN

La dirección de **GRUPO MOK**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la adopción de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes, basado en el estándar de la norma ISO/IEC 27001 y enmarcado en el estricto cumplimiento y en concordancia con la misión y visión de la compañía, así como el cumplimiento de demás requisitos aplicables a seguridad de la información.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. Política General de Seguridad de la Información GRUPO MOK

Para **GRUPO MOK**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. Por tal motivo, Grupo MOK establece los siguientes objetivos estratégicos de seguridad de la información:

- Identificar y proteger, para todos los procesos de negocio, los activos de información involucrados, tanto información física, como información digital,

personas e infraestructura, clasificándolos de acuerdo con los lineamientos de la compañía.

- Entender y dar cobertura a las necesidades de todas las partes interesadas.
- Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización.
- Mitigar los riesgos detectados y asociados a la seguridad de la información y a los activos de información.
- Establecer las políticas, procedimientos y demás lineamientos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Grupo MOK.
- Velar por la continuidad del negocio frente a incidentes de seguridad de la información u operativos.
- Implementar un Sistema de Gestión de Seguridad de la Información en Grupo MOK para proteger la información y los activos de información.

Grupo MOK ha decidido definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información SGSI establecido, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios

El incumplimiento a la política de Seguridad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa interna y externa de la GRUPO MOK, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.2. Principios de Seguridad

A continuación, se establecen 11 principios de seguridad que soportan el SGSI de **GRUPO MOK**:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2. **GRUPO MOK** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej : proveedores o clientes), o como resultado de un servicio interno en outsourcing, bien sea en cumplimiento de los requisitos legales, reglamentarios y contractuales.
3. **GRUPO MOK** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. **GRUPO MOK** protegerá su información de las amenazas originadas por parte del personal.
5. **GRUPO MOK** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. **GRUPO MOK** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. **GRUPO MOK** implementará control de acceso a la información, sistemas y recursos de red.
8. **GRUPO MOK** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. **GRUPO MOK** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

10. **GRUPO MOK** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
11. **GRUPO MOK** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5.3. Política Organizacional de Seguridad de la Información

GRUPO MOK, como parte del proceso de mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, establece la creación del Comité de Seguridad de la Información que se reunirá de forma periódica, como mínimo semestralmente, y cuyo principal objetivo es garantizar el cumplimiento de las Políticas de Seguridad de la Información de la Compañía; el establecimiento de roles y responsabilidades que involucran las actividades de gestión, administración y operación de los sistemas de información de GRUPO MOK; crear, aprobar y revisar la presente política de seguridad de la información; promover las políticas y procesos de seguridad y velar por su cumplimiento; velar por los resultados del SGSI; promover la mejora continua; entre otros.

El equipo de seguridad de la información de Grupo MOK mantiene el contacto o se mantiene informado con los grupos de interés del ámbito de la seguridad de la información, para aplicar buenas prácticas en la materia.

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, GRUPO MOK debe implementar controles de acceso, si es factible técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen, protección de funcionalidades y opciones de configuración reservadas para personal autorizado, identificación de los dispositivos y la computación móvil de la compañía, y/ o los demás controles que se consideren necesarios y pertinentes para garantizar la

seguridad de la información. Esto se encuentra en la Política de Dispositivos y Computación Móvil vigente de la compañía.

Grupo MOK implementa el trabajo en casa, teletrabajo o trabajo híbrido, implementando y tomando en cuenta aspectos de seguridad de la información para proteger la confidencialidad, la integridad y la disponibilidad de la información, tales como otorgar equipos corporativos según se requiera dadas las funciones de los empleados o la clasificación de la información que se debe manejar, revisión y autorización de trabajo en casa por el área de Riesgos y Seguridad de la Información, otorgar acceso remoto según sea necesario, entre otros que se establezcan en la Política de Trabajo en Cas vigente de Grupo MOK.

5.4. Política de Seguridad para el Recurso Humano:

Para **GRUPO MOK** las personas hacen parte integra para el cumplimiento de sus objetivos, misión y visión, es por esto por lo que vela por contar con el personal idóneo para la prestación de los servicios internos y externos de la compañía.

5.4.1. Antes de asumir el empleo:

- **GRUPO MOK** define y documenta los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización. Para esto se pueden utilizar las descripciones del trabajo para documentar las funciones y responsabilidades para la seguridad.
- El área de Recursos Humanos de **GRUPO MOK** debe velar por la verificación de los antecedentes judiciales, penales y policiales de todos los candidatos a un empleo, siempre y cuando la legislación pertinente a la privacidad, la protección de datos personales y/o el empleo lo permita.

- El área de Recursos Humanos de **GRUPO MOK** debe confirmar la información de referencias personales, familiares y/o comerciales, según sea necesario o requerido.
- El área de Recursos Humanos de **GRUPO MOK** debe realizar de manera independiente una validación de la identidad del candidato.
- Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible o de alta confidencialidad de los clientes, empleados, o demás terceros, **GRUPO MOK** debe considerar verificaciones adicionales más detalladas, tales como verificación de información crediticia, polígrafo o estudio de seguridad, siempre y cuando la legislación pertinente a la privacidad, la protección de datos personales y/o el empleo lo permita.
- Las verificaciones adicionales más detalladas que se realicen, tales como verificación de información crediticia, polígrafo o estudio de seguridad deben ser revisadas por el área de Riesgos y Seguridad de la Información para determinar el personal o candidatos que pudiesen llegar a afectar la confidencialidad, integridad y/o disponibilidad de la información, donde esta área podrá dar sus percepciones sobre el nivel de riesgo y, de ser necesario, impedir o no dar visto bueno para la contratación/promoción del individuo.
- **GRUPO MOK** debe establecer acuerdos de confidencialidad con los empleados, contratistas, usuarios de terceras partes y/o demás terceros como manifestación de la voluntad de las partes encaminada a producir la obligación de guardar y no revelar a terceros información que la empresa desea proteger.

5.4.2. Durante la ejecución del empleo:

- La alta dirección debe velar por la aprobación de Políticas, normas y demás lineamientos que permitan el fortalecimiento de la Seguridad de la Información en **GRUPO MOK.**
- La alta dirección debe promover la importancia de la seguridad de la información entre todos los empleados de **GRUPO MOK,** así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las Políticas de Seguridad de la Información.
- La alta dirección debe establecer el proceso disciplinario adecuado para el tratamiento de las faltas de cumplimiento de las políticas de seguridad de **GRUPO MOK.**
- Los empleados de **GRUPO MOK** deben leer, entender y acatar las Políticas de Seguridad de la Información de la empresa.
- Los empleados de **GRUPO MOK** deben informar los eventos de seguridad, los eventos potenciales u otros riesgos de seguridad para la organización.
- **GRUPO MOK** debe dar a conocer o tener disponibles para consulta las responsabilidades de Seguridad de la Información a los empleados

5.4.3. Terminación y Cambio de empleo:

- El área de Recursos Humanos de **GRUPO MOK** debe asegurar que la desvinculación o reasignación de labores, sea de forma ordenada, controlada y segura.
- El área de Recursos Humanos de **GRUPO MOK** debe realizar el procedimiento de desvinculación, otorgamiento de licencias, incapacidades, vacaciones o cambio de labores de los empleados llevando a cabo los procedimientos establecidos y aprobados.
- Cada Jefe de Oficina debe reportar de manera inmediata a el área de Recursos Humanos de **GRUPO MOK**, la desvinculación o cambio de labores de los

empleados, con el fin que se tomen las medidas pertinentes y a su vez se informe a las áreas interesadas.

- Los contratos del empleado y/o acuerdos de confidencialidad del contratista o el usuario de terceras partes de **GRUPO MOK** debe incluir las responsabilidades y deberes válidos de confidencialidad aún después de la terminación del contrato laboral.
- **GRUPO MOK** debe retirar los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información una vez finalizada su contratación laboral o acuerdo, o se deben ajustar tales derechos de acceso después del cambio de funciones y/o cargo.

5.5. Política de Seguridad para la Gestión de Activos de TI

GRUPO MOK es propietario de los activos de información de la compañía y los administradores de estos activos son los empleados (usuarios) que estén autorizados y sean responsables por la información, sistemas de información, hardware, software o infraestructura tecnológica de los procesos a su cargo.

5.5.1. Responsabilidad de los Activos:

- Toda la información creada en función de labores es propiedad de **GRUPO MOK**, así como los activos donde esta se almacena deben ser inventariados, clasificados y asignados a un responsable.
- Cada jefe de área debe actuar como responsable de la información física y electrónica de la dependencia a cargo, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- **GRUPO MOK** establece que las labores rutinarias se pueden delegar, por ejemplo, a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del propietario.

- Cada Jefe de área como responsable de los activos de información debe estar al tanto del inventario de los activos para las áreas o procesos que lideran, acogiendo las indicaciones de la Política de Clasificación de la Información con el apoyo del Gerente de Tecnología y el personal de Seguridad de la Información de **GRUPO MOK**.
- Los empleados de **GRUPO MOK** deben utilizar los recursos tecnológicos de la compañía, con el único objetivo de llevar a cabo las labores asignadas al cargo; por consiguiente, no deben ser utilizados para fines personales.
- Los empleados que estén en proceso de desvinculación o cambio de labores deben realizar la entrega de su puesto de trabajo al Jefe de área o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación de **GRUPO MOK**.
- El área de TI y de Seguridad de la Información de **GRUPO MOK** debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo de la compañía para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.
- Los directores de área en conjunto con el personal de TI, Seguridad de la Información y Riesgos de **GRUPO MOK** deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información. Todos los empleados, contratistas y usuarios por tercera parte deben seguir estas reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo reglas para el correo electrónico, Internet, directrices para dispositivos móviles, entre otros que la empresa considere necesarios.

5.5.2. Política de Clasificación:

- La información de **GRUPO MOK** se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y/o la importancia para la organización.
- **GRUPO MOK** genera procedimientos para realizar la destrucción de la información cuando se ha cumplido su ciclo de almacenamiento, este se detalla en el documento Procedimiento de borrado seguro vigente de la compañía.
- Los usuarios deben acatar los lineamientos de clasificación de la información para el acceso, almacenamiento, copia, transición, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de **GRUPO MOK**.
- Los usuarios deben tener en cuenta las siguientes consideraciones cuando impriman, escaneen, saquen copias o envíen faxes:
    - Verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales.
    - Recoger de las impresoras, escáneres, fotocopiadoras y máquinas de Fax de manera inmediata los documentos confidenciales para evitar su divulgación no autorizada.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y lógico con las condiciones de almacenamiento y resguardo adecuadas.
- Los acuerdos con otras organizaciones que incluyen compartir información deben incluir lineamientos para identificar la clasificación de dicha información y para interpretar las etiquetas de clasificación de otras organizaciones.
- **GRUPO MOK** define los métodos de clasificación de información de acuerdo con lo indicado en la Política de Clasificación de la Información vigente de la compañía.

5.5.3. Manejo de Medios:

- El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de **GRUPO MOK** será reglamentado por el área de TI y Riesgos, considerando las labores realizadas por cada uno de los empleados.
- El área de TI debe implantar controles que regulen el uso de los periféricos y medios de almacenamiento en la plataforma tecnológica de **GRUPO MOK**, de acuerdo con los lineamientos y condiciones establecidos.
- **GRUPO MOK** establece lineamientos de seguridad y manejo de medios a través de la Política de Uso Aceptable de los Activos vigente de la compañía.
- La documentación de los sistemas de **GRUPO MOK** debe estar protegida contra el acceso no autorizado y almacenada con seguridad.

5.6. Política de Control de Acceso:

GRUPO MOK vela por la protección de las redes de datos y los recursos de red, mediante controles de acceso lógicos que evita el acceso no autorizado

- Los administradores de los activos de la información de TI deben establecer medidas de control de acceso a los servicios tecnológicos con el fin de mitigar riesgos asociados al acceso no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de **GRUPO MOK**.
- Los administradores de los activos de la información en conjunto con el área de Riesgos y Seguridad de la Información deben revisar periódicamente los accesos permitidos en los servicios tecnológicos con el fin de evitar riesgos de seguridad de la información.
- **GRUPO MOK** debe establecer matrices para el control de usuarios y sus accesos a los diferentes sistemas de la empresa, teniendo en cuenta perfiles únicos y estándar de acceso de usuario para funciones laborales comunes en la organización.

5.6.1. Acceso a Redes y servicios de Red:

- **GRUPO MOK** en cabeza del área de TI, es responsable de las redes de datos y los servicios de red de la compañía, por lo tanto, debe velar por que estas se encuentren debidamente protegidas contra accesos no autorizados implementando controles de acceso lógico.
- Los usuarios de las redes de **GRUPO MOK** sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.
- Toda solicitud de creación, modificación, bloqueo o eliminación de usuarios de acceso a los servicios de red a través de VPN debe realizarse mediante un ticket de servicio, debidamente autorizado por el jefe de área.
- Es responsabilidad de los usuarios que cuenten con acceso a VPN contar con contraseñas que cumplan los lineamientos de contraseña segura de **GRUPO MOK**.
- La conexión remota a la red de área local de **GRUPO MOK** debe ser establecida a través de una conexión VPN segura, aprovisionada por el área de TI y debidamente autorizada.
- El área de TI debe asegurar que las redes inalámbricas de **GRUPO MOK** cuenten con métodos de autenticación que evite accesos no autorizados, tales como MAC por equipo para las redes corporativas, y para redes de invitados seguridad mínimo a través de WPA2, token dinámico.
- El área de TI debe garantizar que los equipos ajenos a **GRUPO MOK** no accedan a la red local de la empresa.

5.6.2. Gestión de Control de Acceso:

- **GRUPO MOK** en cabeza del área de TI establece el procedimiento formal para la administración de los usuarios en las redes de datos, servicios tecnológicos y sistemas de información mediante los Procedimiento de creación de usuarios, Procedimiento desactivación de usuarios y Procedimiento modificación de usuarios vigentes de la compañía.

- Toda solicitud de creación, modificación o novedad de usuarios debe realizarse mediante el procedimiento establecido para tal fin. Es importante que los usuarios tengan en cuenta que los permisos de acceso que se van a asignar van ligados al área y perfil del usuario que ingresa a **GRUPO MOK**.
- **GRUPO MOK** con el apoyo del área de TI, hace entrega de los usuarios y contraseñas para el uso de los servicios tecnológicos a los cuales el usuario esté autorizado a ingresar teniendo en cuenta su perfil para el desempeño de las funciones y actividades a su cargo.
- Es indispensable que la solicitud de creación, modificación o eliminación de usuarios o accesos sea diligenciada con la información correcta y pertinente.
- El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario será responsabilidad de la persona a la cual le fue asignado.
- Todo usuario no genérico de los sistemas debe tener una persona responsable y de uso individual, deben generar registros de actividad, de tal forma que su actividad sea rastreable.
- Todo usuario genérico de los sistemas debe tener un responsable asignado que vele por la confidencialidad, integridad y disponibilidad de la información. Esto no implica un uso único individual, sino que, la cuenta genérica tiene un responsable, aunque sea de uso de más de un usuario.
- **GRUPO MOK** con el apoyo del área de TI y de Seguridad de la Información debe realizar las revisiones periódicas de las estaciones de trabajo, con el fin de bloquear o eliminar cualquier usuario local que esté activo en los equipos propiedad de la compañía.
- El personal provisto por terceras partes que posean acceso a la plataforma tecnológica y/o servicios tecnológicos de **GRUPO MOK** debe acogerse a las políticas de seguridad de la información corporativas.

- El área de TI debe garantizar que los usuarios que ingresen por primera vez realicen el cambio de contraseña de acceso a los servicios de **GRUPO MOK** tan pronto como estos ingresen a su sesión corporativa.
- Toda solicitud de cambio de contraseñas de personal que se encuentre ausente debe ser autorizado por el jefe inmediato o el encargado de Tecnología de **GRUPO MOK**.
- El área de Infraestructura de **GRUPO MOK** debe retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.
- Los derechos de acceso de los usuarios se deberían revisar de forma general a intervalos regulares de tiempo, con una periodicidad mínima de 6 meses.

5.6.3. Gestión de derechos de acceso privilegiado:

- El área de TI debe velar por que los recursos de la plataforma y los servicios tecnológicos de **GRUPO MOK**, sean operados y administrados en condiciones controladas y seguras, permitiendo el monitoreo y posterior auditoria de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre los servicios tecnológicos.
- **GRUPO MOK** debe asignar los privilegios a los usuarios sobre los principios de necesidad-de-uso y evento-por-evento, teniendo en cuenta el requisito mínimo para su función, sólo cuando sea necesario.
- El área de TI de **GRUPO MOK** debe otorgar los privilegios para la administración de los servicios tecnológicos, solo a aquellos empleados autorizados para dicho fin.
- Todos los administradores de los servicios tecnológicos de **GRUPO MOK** deben asegurarse de que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware, las bases de datos y demás elementos tecnológicos sean cambiados o suspendidos de acuerdo con las mejores prácticas de seguridad, según la necesidad del negocio.

- El área de TI debe establecer controles lógicos para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan obtención de privilegios sin ser autorizados.

5.6.4. Gestión de Contraseñas:

- El área de TI y de Riesgos y Seguridad de la Información con el fin de garantizar una buena gestión de las contraseñas en los servicios tecnológicos de **GRUPO MOK** ha dispuesto la Política general de contraseñas vigente de la compañía.
- La asignación de contraseñas de **GRUPO MOK** se debe controlar a través de un proceso formal y documentado de gestión.
- Es responsabilidad de los usuarios, acatar los lineamientos de generación y control de contraseñas de **GRUPO MOK**.
- **GRUPO MOK** exige a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales, en la descripción de perfil del empleado o en declaraciones independientes.
- Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.
- El área de TI y de Seguridad de la Información de **GRUPO MOK** debe garantizar que las contraseñas de la empresa tengan un período definido de vigencia.
- A los usuarios inicialmente se les debería suministrar una contraseña temporal que estén forzados a cambiar en el primer acceso.
- Las contraseñas temporales que asigne **GRUPO MOK** deben ser únicas para un individuo y no ser descifrables.

5.6.5. Responsabilidad de los usuarios:

- Es responsabilidad de los usuarios mantener la confidencialidad de la información de autenticación a los servicios tecnológicos de **GRUPO MOK**.
- Los usuarios deben evitar el registro físico o lógico de la información de la autenticación para el acceso a los servicios tecnológicos de **GRUPO MOK**.
- Es responsabilidad de cada usuario realizar el cambio de contraseña con los lineamientos indicados en la Política general de contraseñas vigente de la compañía.
- Es responsabilidad del usuario realizar el cambio de contraseña cuando solicite su renovación por olvido para los servicios tecnológicos de la compañía.
- El usuario debe realizar el cambio de contraseña de acceso a los servicios de red, por lo menos 1 vez cada sesenta días (60) días, de lo contrario la contraseña caducará y obligará su cambio.
- En caso de que el usuario crea que su contraseña ha sido comprometida por terceros, debe realizar el cambio inmediatamente e informar al área de TI y de Riesgos y Seguridad de la Información la situación que se presenta.
- Los usuarios deben asegurarse de que los equipos desatendidos tengan protección apropiada y cumplir con los lineamientos de escritorio y pantalla despejada.
- Todos los empleados de **GRUPO MOK** deben seguir y aplicar la Política de Cero Papel definida por la empresa en consecuencia de su compromiso por el cuidado del medio ambiente, teniendo en cuenta la clasificación de la información que se maneje den dichos.

5.6.6. Control de acceso a sistemas y aplicaciones:

5.6.6.1. Restricciones de acceso:

- El área de TI debe velar por que los servicios tecnológicos incluidas las aplicaciones, sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, así mismo debe ejecutar mecanismos para que los desarrolladores, tanto internos como externos, acojan las buenas

prácticas de desarrollo seguro en los productos generados, con el fin de controlar el acceso lógico y evitar accesos no autorizados cuando estos estén en producción.

- El área de TI y de Riesgos y Seguridad de la Información debe establecer un instructivo para la asignación de accesos a los sistemas de información y aplicativos de **GRUPO MOK**.
- Los administradores y custodios de los servicios de información y aplicaciones deben autorizar el acceso a sus sistemas de información o aplicativos de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- **GRUPO MOK** debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, siempre y cuando esto sea posible y necesario.
- El área de Seguridad de la Información, con el apoyo de los administradores y custodios de los sistemas de información y aplicativos, debe monitorear periódicamente (cada seis meses como mínimo) los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

5.6.6.2. Control de acceso a códigos fuente:

- El área de TI debe establecer ambientes separados a nivel físico y/o lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción. Cuando esto no sea posible, se debe garantizar, como mínimo la separación del ambiente productivo de los no productivos.
- El área de TI debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios.

- Los accesos a los repositorios de código fuente deben ser otorgados únicamente por personal autorizado y definido para ello, estos accesos deben asignarse únicamente a personal que pertenezca al proyecto de desarrollo o personal autorizado por ocasiones de fuerza mayor debidamente autorizado.
- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones que permitan implementar medidas de autenticación acordes a las políticas de la compañía.
- Los desarrolladores deben certificar que no se almacenan contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben asegurar que no se desplieguen en pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores y/o los administradores de sistemas deben certificar, siempre y cuando sea posible, que se inhabilitan las cuentas luego de un número establecido en intentos fallidos de ingreso a los sistemas desarrollados, de acuerdo con las necesidades del cliente o sistema.
- Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
- La actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debe efectuar después de recibir la autorización apropiada.

5.7. Política de Criptografía:

- **GRUPO MOK** con el apoyo del área de TI y de Seguridad de la Información establece los lineamientos necesarios para el control y el uso de los controles criptográficos de la compañía.
- **GRUPO MOK** debe emplear el nivel de protección requerido basado en la evaluación de riesgos, teniendo en cuenta tipo, fortaleza y/o calidad del algoritmo de encriptación requerido.
- **GRUPO MOK** debe utilizar algoritmos de cifrado estandarizados y/o aprobados por normas internacionales.
- **GRUPO MOK** debe establecer protección contra modificación, pérdida y destrucción de todas las claves criptográficas.
- El área de TI de **GRUPO MOK** debe revocar las claves, incluyendo la forma de retirarlas o desactivarlas, cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización (en cuyo caso las claves también se deben archivar).
- **GRUPO MOK** dispone de lineamiento de criptografía y sus claves en la Política de Criptografía vigente de la compañía.

5.8. Política de Seguridad física y del entorno:

GRUPO MOK, proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso a las instalaciones de la compañía y a las áreas de procesamiento de información, que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

5.8.1. Áreas seguras

- **GRUPO MOK** debe contar con perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información.
- **GRUPO MOK** establece los lineamientos para asegurar la seguridad física de las instalaciones mediante la Política de Acceso Físico vigente de la compañía.
- **GRUPO MOK** debe establecer o contar un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación, donde no se realice atención al cliente de directa presencial. El acceso a los sitios y edificaciones está restringido únicamente al personal autorizado y su ingreso se debe hacer siguiendo el Procedimiento de ingreso y salida de visitantes vigente de la compañía.
- La infraestructura tecnológica de la compañía debe estar protegida frente a posibles fallas en el suministro de energía eléctrica, para asegurar la continuidad del servicio.
- Queda totalmente prohibido el ingreso de elementos cortopunzantes, armas de fuego, explosivos y/u otro elemento que pueda afectar la integridad física de los empleados y las instalaciones de la empresa.
- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información de la compañía debe estar protegido contra intercepción o daños.
- Las solicitudes de acceso por parte de los empleados o personas ajenas a las áreas seguras deben ser aprobadas por el encargado de dicha área. Igualmente deberán estar acompañadas por el personal autorizado de **GRUPO MOK**.
- **GRUPO MOK** debe exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible otorgada por la compañía y se debería notificar inmediatamente al personal de seguridad si se

encuentran visitantes sin acompañante y cualquiera que no use identificación visible.

- El área de TI debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas deben monitorearse.
- GRUPO MOK debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
- El área de TI debe realizar mantenimientos preventivos al centro de cómputo y centros de cableado que estén bajo su custodia.
- No se permite equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, dentro las áreas de procesamiento de datos sensibles de GRUPO MOK a menos que esté autorizado por el área de Riesgos y el Jefe de área. Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.
- Las actividades de soporte y mantenimiento dentro del centro de cómputo deben ser supervisados personal del área de infraestructura.
- Las puertas del centro de cómputo deben permanecer cerradas.
- En el centro de cómputo, centro de cableado, cuarto de tratamiento de bases de datos y demás áreas seguras está prohibido:
    - Fumar.
    - El porte de armas de fuego, corto punzantes o similares.
    - Mover, desconectar y/o conectar equipos sin autorización.
    - Modificar la configuración del equipo o interconectarlo sin autorización

- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos sin previa autorización.
- Abuso y/o mal uso de los sistemas de información.
- Ingreso de equipos fotográficos, de video, audio u otro tipo de grabación tales como cámaras de dispositivos móviles, a menos que se encuentre autorizado.

- El centro de cómputo debe estar provisto de:
  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión Este equipo debe contar con un sistema de refrigeración de respaldo para que en caso de falla se cuente con continuidad.
  - Unidades de potencia ininterrumpida UPS, que proporcione respaldo al mismo, con el fin de garantizar el servicio de emergencia eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - Alarmas de detección de humo y sistemas automáticos de extinción de fuego.
  - Extintores de incendios.
- El área de TI debe velar por que los cables de potencia estén separados de los de comunicaciones siguiendo las normas técnicas pertinentes.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencia.

5.8.2. Equipos:

- Todas las entregas de equipo o dispositivos que sean realizadas por **GRUPO MOK** se deben documentar y firmar por parte de quien hace la entrega y de quien la recibe.
- **GRUPO MOK** con apoyo del área de TI define las pautas generales para asegurar una adecuada protección de la información que los usuarios manejan en los equipos de trabajo asignados para dicho fin.
- Los servicios de procesamiento de información que manejan datos sensibles deben estar ubicados de forma tal que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento deben estar asegurados para evitar el acceso no autorizado.
- El área de TI debe proveer los mecanismos y estrategias necesarias para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos dentro y fuera de las instalaciones de **GRUPO MOK**.
- Sólo el personal autorizado por el área de Infraestructura puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de **GRUPO MOK**; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la organización.
- Los usuarios que requieran acceder de forma remota a sus estaciones de trabajo deberán generar la solicitud al área de Infraestructura con la respectiva autorización del jefe inmediato y de la Dirección de Infraestructura de **GRUPO MOK**.
- El área de Infraestructura debe generar estándares de configuración segura para los equipos de cómputo de los empleados de **GRUPO MOK** con los estándares autorizados.
- El área de Infraestructura debe asegurar el bloqueo de los puertos USB, SD, entre otros, que permitan la conexión de dispositivos de almacenamientos externos a los equipos propiedad **GRUPO MOK**.

- Las áreas de Infraestructura y de Riesgos y Seguridad son responsables de definir la lista actualizada de software y aplicaciones autorizadas para su instalación en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- El área de Infraestructura debe de manera periódica, realizar las actualizaciones emitidas por los fabricantes de Software y Hardware a todas las estaciones de trabajo pertenecientes a **GRUPO MOK**.
- El área de Infraestructura debe establecer condiciones que deben cumplir los equipos de cómputo de personal provistos por terceros, que requieran conectarse a la red de datos de la compañía y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- El área de Infraestructura en conjunto con el área de Riegos y Seguridad de la Información debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los empleados de **GRUPO MOK**.
- El área de Infraestructura debe implementar controles de bloqueo automático de sesiones de inicio a equipos propiedad de **GRUPO MOK**.
- El área Administrativa debe velar por que los equipos de cómputo que se encuentren sujetos a traslados físicos fuera de las oficinas de **GRUPO MOK**, posean pólizas de seguro.
- El área de Infraestructura es la única autorizada para realizar movimientos y asignaciones de equipos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier empleado de los equipos tecnológicos de **GRUPO MOK**.
- Cuando se presente un incidente de hardware o software en el equipo o en una estación de trabajo o servicio tecnológico propiedad de **GRUPO MOK**, es obligación del usuario informar al área de Infraestructura por los medios dispuestos, con el fin de realizar la asistencia adecuada.

- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás servicios tecnológicos de **GRUPO MOK**, solo puede ser realizado por los responsables de Infraestructura.
- Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por el área de Infraestructura.
- Los equipos de cómputo, en ninguna circunstancia, deben estar desatendidos en lugares públicos o a la vista, en caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas que garanticen su integridad física.
- En caso de pérdida o robo de un equipo tecnológico, propiedad de **GRUPO MOK**, se debe reportar de forma inmediata a las áreas de Administración y de Infraestructura, con el fin de realizar la investigación correspondiente.
- Todo visitante debe registrar su equipo portátil en las planillas creadas para dicho fin.
- Los dispositivos que contienen información sensible se deben destruir físicamente o su información se debería borrar o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar.

5.8.2.1. Política de Pantalla y Escritorio limpio:

- Todos los empleados de **GRUPO MOK** deben conservar el escritorio libre de información confidencial que pueda ser copiada o usada por terceros sin autorización.
- Mantener el escritorio limpio, sin archivos reservados o confidenciales cuando no esté presente y estos no sean necesarios.

- El área de Seguridad de la Información de **GRUPO MOK** debe implementar controles que garantice que los escritorios de los equipos de la Compañía estén libres de información confidencial.
- El área de Infraestructura debe aplicar el bloqueo de pantalla al pasar 5 minutos de inactividad en el equipo.
- Es responsabilidad de cada usuario de **GRUPO MOK** velar por que los documentos y elementos que contengan información de la compañía y que requieran protección especial, de acuerdo con la política de clasificación de la información que se maneje, se deben salvaguardar de manera que solo puedan ser accedidos por el personal pertinente en los tiempos necesarios.
- Todos los empleados de **GRUPO MOK** deben bloquear sus estaciones de trabajo en el momento de abandonar su equipo de trabajo.
- Elementos como llaves, tarjetas de acceso, carnés o demás elementos que permitan acceso físico o lógico a sistemas o instalaciones deben permanecer siempre bajo custodia de la persona autorizada a la que se le haya asignado su custodia o bajo una protección adecuado que no permita su acceso o alcance no autorizado.
- En las zonas o áreas que se considere necesario se puede implementar medidas de seguridad adicionales, tales como el no uso de papeles, post it, esferos o demás en los escritorios o áreas, de acuerdo con términos contractuales o definiciones del área de Seguridad de la Información.

5.9. Política de Seguridad de las Operaciones TIC

El departamento de Tecnología será la encargada de la operación y administración de los servicios tecnológicos que soportan la operación de **GRUPO MOK**, así mismo, velará por la eficiencia de los controles asociados a estos, protegiendo la confidencialidad, integridad y disponibilidad de la información.

5.9.1. Procedimientos de Operación y Responsabilidades:

- **GRUPO MOK** debe documentar, mantener y tener disponibles los procedimientos de operación disponibles para todos los usuarios que los necesiten, siempre y cuando su nivel de clasificación y confidencialidad lo permitan.
- El departamento de Tecnología debe efectuar, a través de sus empleados, la documentación y actualización de los procedimientos, instructivos y guías relacionados con la operación y administración de la plataforma tecnológica de **GRUPO MOK**.

5.9.2. Gestión de Cambios:

- **GRUPO MOK** debe establecer un procedimiento formal y documentado para controlar la gestión de cambios.
- **GRUPO MOK** establece un comité de control de cambios, donde debe haber representación de cada área y los cuáles realizarán la valoración y aprobación o rechazo del cambio.
- La infraestructura y el software de aplicación de **GRUPO MOK** deben estar sujetos a un control estricto de la gestión del cambio, estableciendo las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos.
- El departamento de Tecnología debe velar por el control de los cambios en los servicios tecnológicos y sistemas de información que puedan afectar la Seguridad Digital de **GRUPO MOK**.
- El departamento de Tecnología, con el apoyo del Gestor de Cambios, debe velar por la correcta identificación y registro de los cambios en los servicios tecnológicos y sistemas de información de la compañía.
- El departamento de Tecnología, con el responsable del cambio, debe velar por que se realice una adecuada planeación, pruebas, ejecución y documentación de los cambios a los servicios tecnológicos y/o sistemas de información de la Compañía.

- Toda Gestión de Cambio debe ser sometida a una evaluación de riesgo realizada por quien propone el cambio, los Funcionales o el Responsable del cambio, dicha evaluación debe ser documentada y presentada para aprobación del cambio.
- El departamento de Tecnología, con el apoyo de la mesa de ayuda, debe informar con anticipación a la compañía, la fecha y servicios que no estarán disponibles.
- El responsable del cambio debe cumplir el procedimiento establecido para la gestión de cambios.
- El área de TI, en cabeza del personal de apoyo para la Gestión de Cambios de Emergencia, debe verificarlos en caso de presentarse un incidente que lo requiera.

5.9.3. Protección contra códigos maliciosos:

- **GRUPO MOK** proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre los empleados frente a los ataques de software malicioso.
- El área de TI debe contar con herramientas tales como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo de contagio de software malicioso y respalden la Seguridad Digital contenida y administrada en la plataforma tecnológica de la compañía y los servicios que se ejecutan en la misma.
- El área de Infraestructura debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.
- El área de Infraestructura a través de sus empleados debe asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware.

- Los usuarios tienen prohibido la instalación de software en los equipos de la compañía, en caso de requerirlo, deben escalar la solicitud a la mesa de ayuda de la compañía, quien validará si el software requerido está o no autorizado para su uso sin que represente un riesgo de Seguridad Digital.
- Los usuarios de los servicios tecnológicos de la compañía no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware y antispam definida por el área de Infraestructura; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de los servicios tecnológicos deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al área de Infraestructura y de Riesgos y Seguridad de la información a través de los mecanismos oficiales dispuestos para ello, con el fin de ejercer los controles correspondientes.
- El área de Riesgos y Seguridad de la Información debe brindar consciencia a los empleados y proveedores de **GRUPO MOK** sobre seguridad y sobre las principales amenazas de seguridad.
- **GRUPO MOK** debe velar por la implementación de procedimientos para recolectar información con regularidad, como la suscripción a sitios web de verificación y / o listados de correo que suministren información sobre los códigos maliciosos nuevos, dicha información debe prevenir de fuentes calificadas, sitios confiables de internet o proveedores de software de protección contra códigos maliciosos para diferenciar entre falsas alarmas y códigos maliciosos.

5.9.4. Copias de Respaldo:

- **GRUPO MOK**, con el apoyo del departamento de Tecnología certificará la generación de las copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procesos y mecanismos para la realización de estas actividades.
- **GRUPO MOK** a través de sus empleados, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- **GRUPO MOK** debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- **GRUPO MOK** debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- **GRUPO MOK** dispone de una Política de Backups para la realización y establecimientos de respaldo aplicables a los sistemas de información.
- El departamento de Tecnología debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la compañía.
- Es responsabilidad de los usuarios, guardar la información crítica de sus funciones en las Carpetas de Red asociada a su nombre o a su área de trabajo, con el fin de garantizar su respaldo.
- Por ningún motivo se permite alojar en servidores información catalogada como personal propia, música, videos, etc. Solo se permite este tipo de información digital de trabajo.
- La Presidencia, Vicepresidencias, la Gerencia de Cumplimiento y Seguridad, Gerencia de Desarrollo y Dirección de Infraestructura y Datos son los únicos

autorizados para solicitar la recuperación de la información ante una pérdida total o parcial.

5.9.5. Registro y seguimiento:

- En los sistemas de Grupo MOK se deben registrar las actividades tanto del operador como del administrador del sistema, esto tanto de eventos exitosos como fallidos.
- **GRUPO MOK** podrá realizar monitoreo del uso que dan los empleados, a los recursos de la plataforma tecnológica y los sistemas de información de la compañía, esto es revisión de logs cuando la compañía lo considere necesario. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos por dichos registros.
- El área de TI debe certificar la confidencialidad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de **GRUPO MOK**, estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
- Los desarrolladores (internos y externos) deben habilitar en los logs de auditoria eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por el Personal de Seguridad de la Información.
- El departamento de Tecnología debe garantizar que todos los sistemas de procesamiento de información, los equipos y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo.
- Los logs o registros deben tener un responsable encargado y autorizado para su generación, custodia, protección y disposición.

- La información de los logs generados debe permanecer inmodificable y no se pude eliminar mientras esté en almacenamiento. A esta información solo tienen acceso personas autorizadas.

5.9.6. Control de Software Operacional

- **GRUPO MOK**, a través del área de infraestructura, designará responsables y establecerá instructivos y guías para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- El departamento de Tecnología debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúa con el procedimiento de cambios existente en la compañía.
- El área de Infraestructura debe asegurarse que el software operativo instalado en la plataforma tecnológica de la compañía cuente con soporte de los proveedores y fabricantes.
- El departamento de Tecnología debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe 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.
- Las áreas de TI, Riesgos y Seguridad de la Información deben establecer las restricciones y limitaciones para la instalación del software operativo en los equipos de cómputo de la compañía.
- El departamento de Tecnología debe implementar actualizaciones para el software, aplicaciones y librerías de programas, así como parches de seguridad, que deberán llevar a cabo el personal autorizado.

- Cuando alguna actualización presente fallo se debe notificar o informar de forma automática a través de correo electrónico a los responsables del parche o actualización, para la revisión y realización de la actividad.
- El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedor se deberían monitorea.
- Los sistemas operativos únicamente se deberían mejorar cuando existe un requisito para hacerlo, por ejemplo, si la versión actual del sistema operativo ya no da soporte a los requisitos del negocio. Las mejoras no deberían tener lugar sólo porque esté disponible una nueva versión del sistema operativo.
- Las áreas de TI, Riesgos y Seguridad de la Información deben restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

5.9.7. Gestión de Vulnerabilidad Técnica

- El departamento de Tecnología, con el apoyo del personal de Seguridad de la Información revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica, por medio de la realización de pruebas de vulnerabilidades, pentest o hacking ético-internos, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.
- GRUPO MOK debe realizar análisis de vulnerabilidades o hacking ético al menos una vez al año con un tercero.
- La clasificación de las vulnerabilidades debe estar alineada a un estándar internacional.
- Los responsables de la gestión de parches, actualizaciones de software y remediación de vulnerabilidades deber realizar reportes periódicos, dependiendo

de la criticidad de la vulnerabilidad, al área de Riesgos y Seguridad de la Información para llevar una traza y monitoreo de la gestión de la vulnerabilidad.

- **GRUPO MOK** deber definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes, dando prioridad a las vulnerabilidades de mayor criticidad.
- Antes de la salida a producción de un servicio, activo o producto se debe realizar un escaneo de vulnerabilidades para evitar fallas de seguridad. El servicio, activo o producto no podrá ser liberado para producción con vulnerabilidades abiertas, a menos que se establezca salida a producción en acuerdo con cliente o a directriz interna de la compañía.

5.9.8. Auditorias de Sistemas de Información:

- El personal de Seguridad de la Información de **GRUPO MOK** debe generar, ejecutar y monitorear planes de verificación de puntos de control de los sistemas de información de la compañía y/o las políticas y lineamientos de seguridad definidos.
- **GRUPO MOK** debe realizar auditoría independiente del Sistema de Gestión de Seguridad de la Información para medir de forma imparcial el cumplimiento de los lineamientos de seguridad y el cumplimiento con el estándar definido.
- **GRUPO MOK** debe velar por que las actividades de auditoría que implican verificaciones de los sistemas operativos sean aplicadas cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.
- La persona que realiza la auditoría debe ser independiente de las actividades auditadas, esto con el fin de evitar conflictos de intereses.

5.10. Política de Seguridad de las Comunicaciones:

GRUPO MOK establecerá, a través del área de TI, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos

5.10.1. Gestión de la seguridad de las Redes:

- **GRUPO MOK** debe contar con los perfiles profesionales adecuados para el personal encargado de la administración de los equipos de red de la compañía.
- El área de Infraestructura debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- El área de Infraestructura debe velar por la confidencialidad de la información, del direccionamiento y el enrutamiento de las redes de datos de la compañía.
- El área de Infraestructura debe garantizar que el acceso a los recursos de red siempre sea mediante un usuario y contraseña.

i. Seguridad de los servicios de red:

- El área de Infraestructura debe acoger las buenas prácticas de configuración establecidos por los fabricantes para los dispositivos de seguridad y de la red de la plataforma tecnológica de la compañía, según lo considere necesario.
- El área de Infraestructura debe diseñar y aplicar instructivos para el uso de servicios de red, para restringir su acceso a servicios y aplicaciones, cuando sea necesario.
- La capacidad del proveedor del servicio de red para gestionar los servicios acordados de forma segura se debe determinar y monitorear regularmente, y se debe acordar el derecho a auditoría.

ii. Seguridad para uso de servicio de Internet:

- El área de Infraestructura debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
- El área de Infraestructura debe generar registros de navegación y los accesos de los usuarios a Internet.
- El área de Infraestructura y de Riesgos y Seguridad de la Información debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.
- El área de Infraestructura y el área de Seguridad de la Información deben establecer y aplicar controles para evitar el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking o cualquier otra página que vaya en contra de la ética moral o que no vaya acorde al desarrollo de las funciones de los empleados.
- Los usuarios autorizados para hacer uso del servicio de internet son responsables de evitar prácticas o usos que puedan comprometer los servicios tecnológicos de la compañía o que afecten la seguridad de la información de la compañía.
- Los usuarios del servicio de Internet de la compañía deben hacer uso de este en relación con las actividades laborales que así lo requieren, según el horario, perfil y roles autorizados por su jefe directo.
- Los usuarios de la compañía tienen prohibido la transferencia de información catalogada como confidencial a entidades externas sin previa autorización. Igualmente, deben realizar transferencia de información únicamente por medios permitidos dispuestos por el área de Infraestructura y el área de Seguridad de la Información.
- No está permitido la generación y/o almacenamiento de información relacionada con la compañía en plataformas de Internet no autorizadas

por GRUPO MOK, tales como Dropbox, Google Drive, BOX, Mega, Amazon Cloud, iCloud, WeTransfer, TransferXL o alguna otra plataforma de almacenamiento distinta a la suite de Office Corporativo.

iii. Separación de redes:

- El área de Infraestructura debe mantener las redes de datos segmentadas por grupos de equipos de escritorio, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la compañía.
- El área de Infraestructura debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la compañía, tales protecciones pueden ser firewalls o demás herramientas que permitan la seguridad de las redes de **GRUPO MOK**.
- El área de TI debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la compañía.

5.10.2. Transferencia de Información:

- **GRUPO MOK** asegurará la protección de la información en el momento de ser transferida o intercambiada con las otras entidades y establecerá los lineamientos y controles necesarios para el intercambio de información.
- La transferencia de información deberá tener en cuenta el esquema de clasificación de la información establecido por **GRUPO MOK** para evitar la fuga de información confidencial, reservada o de uso interno.
- Los administradores de los activos de la información deben asegurarse que el intercambio de información digital solamente se realice mediante la herramienta autorizada por las áreas de Infraestructura y Riesgos, y que estén alineadas con las Políticas de Seguridad de la Información.

- El área de recepción de cualquier documento físico (Recepción de documentos) debe acoger el procedimiento para el intercambio de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- El área Administrativa y demás áreas que realicen transferencia de información física o activos de información de **GRUPO MOK** deben certificar que todo envío de información física a terceros (documentos o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por **GRUPO MOK**.
- El área de Infraestructura debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

i. **Mensajería electrónica:**

- El área de Infraestructura debe implementar controles que eviten el acceso no autorizado a los servicios de mensajería autorizados por **GRUPO MOK** (Correo institucional, SFTP, entre otros autorizados) con el fin de evitar cualquier modificación o denegación del servicio.
- El área de Infraestructura debe velar por que los controles de autenticación desde redes públicas hacia los servicios de la compañía sean fuertes y en lo posible, contar con doble factor de autenticación.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la compañía y cada usuario, como responsable de su buzón, debe mantener únicamente los mensajes relacionados con el desarrollo de sus funciones.
- El personal de seguridad de la información debe velar por la implementación de mecanismos que permitan garantizar la integridad y

no repudio de la información, mediante el uso de firmas digitales dependiendo de las funciones o roles del colaborador.

- El único servicio de correo electrónico autorizado es el asignado directamente por el área de Infraestructura, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
- El área se Seguridad de la Información e Infraestructura debe definir y aplicar controles de recepción y envío de correo electrónico a los empleados de **GRUPO MOK**, de acuerdo con la realización y cumplimiento de sus funciones.
- La cuenta de usuario de correo electrónico corporativa asignada es de carácter individual, por lo tanto, ningún empleado que realice actividades para **GRUPO MOK**, debe compartirla o usar una cuenta que no sea la suya en ninguna circunstancia.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por **GRUPO MOK** y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.
- **GRUPO MOK** debe hacer uso de sistemas acordados de etiquetado, automatizados o no, de la información sensible o crítica, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente.
- Es responsabilidad del usuario reportar al área de Riesgos e Infraestructura, los correos electrónicos cuando crea que son de dudosa

procedencia, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la compañía.

- El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de **GRUPO MOK**.
- Los empleados de **GRUPO MOK** no deben usar otros servicios de correo electrónico, además del administrado por el área de Infraestructura para el envío de información corporativa.
- Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.
- Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo de **GRUPO MOK**, cuando su ausencia sea mayor a tres (3) días.

ii. Acuerdos de confidencialidad y de no divulgación

- **GRUPO MOK**, con el apoyo del personal de Seguridad de la Información, Protección de Datos y área Legal, establecerán los modelos de Acuerdos de Confidencialidad y/o Intercambio de Información entre **GRUPO MOK** y sus empleados o terceras partes con quienes se realice dicho intercambio.
- Los acuerdos pueden ser electrónicos o manuales y pueden tomar la forma de contratos formales o condiciones de empleo. Para la información sensible, los mecanismos específicos utilizados para el intercambio de dicha información deberían ser consistentes para todas las organizaciones y todos los tipos de acuerdos.
- Todos los empleados y terceros de **GRUPO MOK** deben leer y firmar un Acuerdo de confidencialidad que garantice la confidencialidad de la información a la que el empleado o tercero tenga acceso.

5.11. Política de Adquisición, desarrollo y mantenimiento de sistemas:

- El área de Desarrollo velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos y lineamientos de desarrollo seguro adecuados para la protección de la información de **GRUPO MOK**.
- El departamento Tecnología de **GRUPO MOK** cuenta con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes áreas, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la compañía. Sin embargo, este debe cumplir con las medidas y visto bueno por parte del área de Riesgos y Seguridad de la Información y demás áreas directamente involucradas, y cumplir con las evaluaciones de riesgo y verificaciones de seguridad respectivas.
- Toda adquisición de desarrollo debe cumplir con lineamientos de desarrollo seguro, donde el tercero deberá garantizar el seguimiento de una metodología de desarrollo que garantice niveles de seguridad adecuados.

5.11.1. Requisitos de seguridad de sistemas de información:

- El área de Desarrollo, con el apoyo del área de Riesgos y Seguridad de la información incluirán requisitos de desarrollo seguro en la definición de requerimientos de seguridad.
- El área de Desarrollo debe establecer metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

- Los responsables de la administración de los sistemas de información deben definir qué perfiles deben contener los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
- El departamento de Tecnología debe velar por que la entrega de los ambientes de desarrollo, pruebas y producción estén libres de vulnerabilidades en sus sistemas operativos.
- El departamento de Tecnología debe asegurar que cada vez que se vaya a implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades, las cuales deberán ser remediadas antes del despliegue en producción por las áreas encargadas, o bajo las condiciones que se acuerden con Grupo MOK.
- El departamento de Tecnología debe certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas, soportadas, actualizadas y reconocidas en el mercado.
- El área de Desarrollo debe establecer mecanismos que permitan deshabilitar las funcionalidades de autocompletar en formularios de solicitud que requieran información sensible.
- El equipo de Desarrollo debe integrar en las fases iniciales de los proyectos los requisitos del sistema para la seguridad de la información y los procesos para implementarla.
- El departamento de Tecnología con el apoyo del personal de Seguridad de Información debe establecer el tiempo de duración de cada sesión inactiva de las aplicaciones web de uso propio de la compañía. Para sistemas de uso externo se establece de acuerdo con necesidades del sponsor/cliente. No es de obligatoriedad para aplicaciones de escritorio o demás que salen del dominio o de la administración de Grupo MOK, dada la naturaleza de estos sistemas.
- El área de TI, con el apoyo del personal de Desarrollo y Bases de Datos debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos.

- Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o realizar evaluación de riesgo para determinar el impacto de esta y viabilidad de su uso.

5.11.2. Seguridad en los procesos de desarrollo y soporte:

- **GRUPO MOK** debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción, dentro de la infraestructura de Desarrollo de la compañía.
- Ante la no posibilidad de implementación de los tres ambientes separados, se debe implementar la separación del ambiente productivos de los no productivos.
- El ambiente de desarrollo/pruebas se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código fuente; además se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo.
- El ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la compañía.
- El departamento de Tecnología debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.
- El equipo de Desarrollo debe realizar las debidas pruebas de funcionalidad y validar que el desarrollo esté acorde para lo que fue diseñado y desarrollado.
- El departamento de Tecnología debe contar con un sistema de control de cambios para administrar los cambios en los sistemas de información de la compañía.
- El departamento de Tecnología, con el apoyo del área legal cuando sea necesario, debe asegurarse 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.

- El departamento de Tecnología debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los parches generados y estables para las versiones en uso.
- Los desarrolladores internos y externos de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores internos y externos deben proporcionar un nivel adecuado de soporte para solucionar los problemas en los sistemas de información de la compañía; de acuerdo con los niveles de servicio acordados entre las partes.
- Los desarrolladores internos y externos deben construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de datos de salida de manera confiable, utilizando rutinas de validación centralizada y estandarizadas.
- Los desarrolladores internos y externos deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
- Los desarrolladores internos y externos deben asegurar el manejo de operaciones sensibles o críticas de los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores internos y externos deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores internos y externos deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Los desarrolladores internos y externos deben prevenir la revelación estricta de directorios de los sistemas de información construidos.
- Los desarrolladores internos y externos deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.
- Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Ni los desarrolladores ni terceros deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- El área de TI, en conjunto con los desarrolladores, debe crear e implementar una guía de desarrollo seguro usando metodologías de desarrollo seguro.
- El departamento de Tecnología debe asegurar que no se liberen versiones beta a ambientes productivos.

5.11.3. Datos de Prueba:

- El departamento de Tecnología protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información privada o sensible personal de los ambientes de producción.

- No se debe emplear bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba.
- Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deben retirar o modificar antes del uso para evitar el reconocimiento.
- Cuando sea estrictamente necesario el uso de data personal real en ambientes no productivos, esto debe ser autorizado por el personal de Riesgos y Seguridad de la Información.

5.12. 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.

5.12.1. Seguridad de la Información en las relaciones con los proveedores:

- Las áreas de Tecnología, Riesgos y Seguridad de la Información, Administrativa y Jurídica deben generar un modelo de base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- Las áreas de Tecnología, Riesgos y Seguridad de la Información, Administrativa y Jurídica deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de información con terceras partes. De dichos acuerdos podrá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

- El departamento de Tecnología debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- El departamento de Tecnología y Riesgos debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la compañía.
- El departamento de Tecnología y Riesgos debe identificar, evaluar y monitorear 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 por parte de los proveedores.
- Con las personas responsables de contratos con terceros se deben divulgar las políticas, normas y procedimientos de seguridad de la información de la compañía, 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 se debe incluir una cláusula de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las Políticas de Seguridad de la Información.
- El área de Seguridad de la Información de **GRUPO MOK** debe realizar capacitaciones o informar a los proveedores de la empresa en temas de seguridad de la información.

5.12.2. 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 Infraestructura debe verificar 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 departamento de Tecnología debe garantizar las condiciones de comunicación segura, cifrado y/o transmisión de información desde y hacia terceros.
- Los responsables de contratos con terceros deben administrar 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 deberá verificar la aparición de nuevos riesgos.
- Los acuerdos de prestación de servicios deben contener, de ser necesario, el derecho de auditoría y/o verificación de puntos de control a los servicios prestados, así como revisiones periódicas de riesgos.
- Para la gestión de seguridad en relaciones con los proveedores, **GRUPO MOK** sigue los lineamientos establecidos en la Política de Gestión de Seguridad con Proveedores vigente de la compañía.

5.13. Gestión de Incidentes de Seguridad de la Información:

- **GRUPO MOK** asegura que los eventos e incidentes de seguridad de la información que se presentan en los activos de información de la compañía sean comunicados y atendidos oportunamente, aplicando los procesos definidos con el fin de tomar las acciones correctivas.
- **GRUPO MOK** establece como responsable de esta política al personal de Seguridad de la información, así mismo, la Gestión de Incidentes de seguridad de la información al área de Gestión de Riesgos y Seguridad de la información, con apoyo de las áreas que se encuentren involucradas en los respectivos incidentes.
- Las áreas de Riesgos y Seguridad de la Información, en compañía de las áreas involucradas en los procesos, deben documentar los instructivos y guías para la planificación y preparación de respuestas a incidentes.

- **GRUPO MOK** debe contar con un canal de comunicación establecido y conocido por todos los empleados, contratistas y usuarios de la empresa para el reporte de incidentes de seguridad de la información.
- El área de Riesgos de GRUPO MOK debe levantar las matrices de riesgo de los debidos procesos y en compañía de las demás áreas de la organización, generar planes de tratamiento de riesgos para mitigar los riesgos identificados.
- Las matrices de riesgo y planes de tratamiento de riesgo deben ser aprobadas por los responsables del riesgo o responsables del proceso, así como la aceptación de los riesgos residuales.
- El área de Riesgos y Seguridad de la Información debe documentar el instructivo de respuesta, escalamiento, recuperación controlada de un incidente y la comunicación a personas o entidades externas, teniendo en cuenta que son los únicos autorizados para reportar incidentes de seguridad ante las autoridades.
- Los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante las entidades externas son el Comité de Seguridad de la Información o la Junta Directiva de **GRUPO MOK.**
- El departamento de Tecnología y el área de Riesgos deben contar con un directorio que contenga la información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.
- El área de Riesgos debe garantizar que cuenta con los formatos necesarios para el reporte de un evento y la lista de chequeo de acciones que debe verificar ante un incidente de seguridad.
- Todos los empleados, contratistas y usuarios de tercera parte deben tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Así mismo deben conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto.
- El área de Riesgos debe evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares.

- **GRUPO MOK** debe tener procedimientos o lineamientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.
- El personal de Riesgos y Seguridad de la Información debe realizar charlas o capacitaciones a los empleados de la compañía, de acuerdo con las políticas e instructivos existentes relacionados con los estándares y recomendaciones de seguridad de **GRUPO MOK**.
- **GRUPO MOK** debe establecer procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información participen en los controles correctivos, preventivos y/o planes de mejora.
- El área de Riesgos debe establecer un procedimiento formal para la recolección, protección y disposición de evidencias de incidentes de seguridad.
- **GRUPO MOK** debe tener en cuenta la evaluación de los incidentes de seguridad de la información para mejorar o agregar controles para limitar la frecuencia, el daño y el costo de futuras recurrencias, o de considerarlos en el proceso de revisión de la política de seguridad y promover la mejora continua.

5.14. Aspectos para Continuidad del Negocio:

GRUPO MOK proporcionará los recursos suficientes para proporcionar una respuesta efectiva de sus empleados y servicios ante eventos de catastróficos que se presenten en el instituto y que afecten la continuidad de la operación.

5.14.1. Continuidad de la Seguridad de la Información:

- El área de Continuidad de Negocio en conjunto con las áreas operativas y tecnológicas deben generar documentación de procedimientos de continuidad que puedan ser utilizados en caso de un evento adverso, teniendo en cuenta la

seguridad de la información. Estos deberán ser aprobados para verificar su efectividad.

- El comité de Seguridad de la Información, junto a la oficina de Riesgos, deben reconocer las situaciones que serán identificadas como emergencia o desastre para la compañía, los procesos o las áreas y determinar cómo se debe actuar sobre estas.
- El comité de Seguridad de la Información y el personal de Continuidad de Negocio deben definir y liderar el/los Planes de Continuidad de Negocio y Plane de Recuperación ante Desastres.
- El equipo de TI y el personal de Continuidad de Negocio deben realizar la actualización del BIA (Análisis de impacto de negocio), en donde se propongan estrategias de recuperación en caso de activarse el plan de continuidad.
- La Gestión de Riesgos y de Continuidad de Negocio, debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El personal de Continuidad de Negocio debe asegurar la realización de pruebas periódicas de continuidad de negocio.
- La Gestión de Riesgos en conjunto con el área de Infraestructura y el personal de Continuidad de Negocio, deben elaborar y actualizar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad de cada uno de los servicios y sistemas prestados
- El departamento de Tecnología, el personal de Continuidad de Negocio el personal de las áreas operativas debe participar activamente en las pruebas de continuidad de negocio.
- Las evaluaciones de riesgos para la continuidad del negocio se deben efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deben considerar todos los procesos del negocio sin limitarse a

los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información.

- **GRUPO MOK** debe definir un RTO y RPO para la continuidad de negocio de los diferentes servicios que permitan determinar las metas de indisponibilidad de dichos servicios o procesos.

5.14.2. Redundancias:

- El departamento de Tecnología y el área de Continuidad de Negocio deben analizar y establecer los requerimientos de redundancia para los sistemas de información crítica para la compañía y la plataforma tecnológica que los soporta.
- El departamento de Tecnología y el área de Continuidad de Negocio deben evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de **GRUPO MOK**.
- El departamento de Tecnología, a través de sus empleados, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas, en conjunto con el personal de Continuidad de Negocio, sobre dichas soluciones para asegurar el cumplimiento de los requerimientos de disponibilidad de **GRUPO MOK**.

5.15. Cumplimiento:

GRUPO MOK velará por la identificación, documentación y cumplimiento de los requisitos legales 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.

5.15.1. Cumplimiento de requisitos legales y contractuales:

- El personal de Seguridad de la Información debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a **GRUPO MOK**.
- El departamento de Tecnología debe asegurar que todo el software que se ejecuta en la compañía este protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software libre de distribución y uso.
- Los empleados de **GRUPO MOK** deben cumplir 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.

i. **Principios que constituyen las reglas a seguir en la recolección, manejo, tratamiento, almacenamiento e intercambio de datos personales:**

- **Legalidad:** El Tratamiento de datos personales se realizará conforme a las disposiciones legales aplicables (Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios).
- **Finalidad:** Los datos personales recolectados serán exclusivos para un propósito específico y explícito el cual debe ser informado al Titular o permitido por la Ley El Titular será informado de manera clara, suficiente y previa acerca de la finalidad de la información suministrada.
- **Libertad:** La recolección de los datos personales solo podrá ejercerse con la autorización, previa, expresa e informada del Titular
- **Veracidad o Calidad:** La información sujeta al tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Transparencia:** En el tratamiento de datos personales se garantiza el derecho del Titular a obtener en cualquier momento y sin

restricciones, información acerca de la existencia de datos que le conciernen.

- **Acceso y circulación restringida:** El tratamiento de datos personales solo podrá realizarse por las personas autorizadas por el Titular y/o por las personas previstas en la Ley.
- **Seguridad:** Los datos personales sujetos a tratamiento se manejarán adoptando todas las medidas de seguridad que sean necesarias para evitar su pérdida, adulteración, consulta, uso o acceso no autorizado o fraudulento.
- **Confidencialidad:** Los empleados de la compañía, están obligados a guardar reserva sobre la información personal a la que tengan acceso con ocasión de su vínculo contractual con **GRUPO MOK**.
- En las relaciones contractuales, **GRUPO MOK** debe incluir en los procesos de contratación cláusulas con el fin de autorizar de manera previa y general el tratamiento de datos personales relacionados con la ejecución del contrato, lo que incluye la autorización para recolectar, modificar o corregir estos datos en momentos futuros. También incluirá la autorización de que algunos de los datos personales, en caso dado, puedan ser entregados a terceros con los cuales la compañía tenga contratos de prestación de servicios, para la realización de tareas tercerizadas.
- Cuando **GRUPO MOK** lleve a cabo contrataciones a terceros para la realización de tareas complementarias, y el contratado requiera de datos personales, la compañía le suministrará estos datos siempre y cuando exista una autorización previa y expresa del titular de los datos para esta transmisión. Dado que en estos casos los terceros son encargados del tratamiento de datos, sus contratos incluirán cláusulas que precisan los fines y los tratamientos autorizados por la compañía y delimitan de manera precisa el uso que estos terceros le

pueden dar a estos datos. En todo caso, se incluirá una cláusula que prohíba una entrega posterior a otros terceros, así como el uso comercial de los datos personales entregados.

- La transferencia de datos personales a otros países sólo se debe realizar cuando exista la autorización o solicitud correspondiente del cliente y/o del titular y, en caso dado, cuando responda a solicitudes de entidades públicas o administrativas en ejercicio de sus funciones legales.
- **GRUPO MOK** debe informar y capacitar a los empleados, sobre el uso adecuado de datos personales por parte de estos. Adicionalmente, se deben desarrollar campañas y programas de información y reflexión con los empleados para instruirlos sobre sus derechos en relación con sus datos personales y su uso adecuado, especialmente en relación con las tecnologías de información.
- De acuerdo con el Artículo 25 de la Ley 1581 de 2012, la compañía en calidad de responsable del tratamiento de datos personales debe registrar sus bases de datos en el Registro Nacional de Bases de Datos, administrado por la Superintendencia de Industria y Comercio.
- **GRUPO MOK** debe asegurar y dar a conocer a los usuarios los principios, deberes, políticas, finalidad del tratamiento de los datos personales, derechos de los titulares para instaurar una queja, consulta o reclamo en ejercicio del derecho de habeas data, tiempos de respuesta.

5.15.2. Revisiones de Seguridad de la Información

i. Cumplimiento con las políticas de seguridad de la Información:

El personal de Seguridad de la Información y el Comité de Seguridad de la Información, tienen como una de sus funciones proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de la base de datos de información automatizada en general. Esta política de Seguridad de la Información se debe revisar y/o actualizar de manera anual, o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Así mismo, el Sistema de Gestión de Seguridad de la Información debe ser evaluado por personal independiente, con el fin de revisar y garantizar el nivel de cumplimiento del presente SGSI con los requisitos normativos. El área de Seguridad de la Información también debe realizar verificaciones de puntos de control sobre sus lineamientos o políticas definidas dentro del Sistema de Gestión de Seguridad de la información, esto para garantizar y velar por el cumplimiento con la normatividad interna en temas de seguridad.

ii. Cláusulas de cumplimiento:

- El personal de Seguridad de la Información debe gestionar la verificación del cumplimiento del presente documento de Políticas Corporativas de Seguridad de la Información.
- El personal de Seguridad de la Información puede implementar mecanismos de control que permita identificar tendencias de uso de recursos informáticos del personal interno y externo. El mal uso de los recursos informáticos que sea detectado será reportado.
- Los jefes de área como dueños de los procesos establecidos en **GRUPO MOK** deben apoyar las revisiones del cumplimiento de las Políticas de

Seguridad de la Información que les competa y cualquier otro requerimiento de seguridad.

iii. Violaciones de Seguridad de la Información:

- Ningún empleado debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de TI o por el personal de Seguridad de la Información.
- Ningún empleado debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a los equipos de cómputo, redes o información de la **GRUPO MOK**.
- Ningún empleado debe hacer uso de los recursos asignados para actividades no relacionadas con el propósito de la compañía, o bien con la extralimitación en su uso.
- Ningún empleado debe realizar actividades como: traer equipos o ejecutar aplicaciones que no estén directamente especificados como parte del software, hardware o de los estándares de los recursos informáticos propios de **GRUPO MOK**.
- Ningún empleado debe introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Ningún empleado debe introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o

secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño a la información o los recursos informáticos de **GRUPO MOK**.

- Ningún empleado debe intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Ningún empleado debe albergar datos de carácter personal en carpetas diferentes a la asignada para este fin, en los computadores de trabajo.
- Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.
- Los empleados de GRUPO MOK, así como contratistas y terceros deben acatar las medidas de seguridad correspondientes, el no cumplimiento de las políticas y normas de seguridad implica violaciones de seguridad de la información que puede acarrear, mas no limitarse a llamados de atención, levantamientos de incidentes de seguridad de la información, sanciones, despido o aplicación del Código Disciplinario de la compañía.

6. CONTROL DE CAMBIOS

Versión No	Descripción del cambio	Responsable	Fecha
1	Elaboración de la primera versión del documento.	Director de Tecnología	24/07/2017
2	Se añade definiciones, se modifican las premisas y se establecen principios y seguridad.	Analista de Procesos	08/05/2018
3	Se cambia el título y se agregan diferentes políticas.	IDENTIAN	11/04/2019
4	Se realizan cambios generales faltantes al documento, se establecen pautas para el cumplimiento de las políticas y se hace revisión y validación de las obligaciones de la compañía.	Director Administrativo.	16/08/2019
5	Revisión y actualización de la Política de Seguridad de la Información	Analista de Riesgos y Seguridad de la Información.	22/02/2021
6	Se modifican políticas generales y lineamientos de seguridad de acuerdo con auditorías realizadas durante el año, así como implementaciones de acuerdo con la Norma ISO 27001.	Analista de Seguridad de la Información.	20/01/2022
7	Revisión y actualización general del documento de acuerdo con el SGSI.	Oficial de Seguridad de la Información	16/12/2022

7. REGISTRO DE COLABORADORES

Elaboró	Revisó:	Aprobó:
Nombre: Alejandro Erazo Bolaños.	**Nombre:** Miguel Omar Ríos Cabra.	**Nombre:** Comité de Seguridad de la Información
Cargo: Oficial de Seguridad de la Información.	**Cargo:** Gerente Cumplimiento Y Seguridad Global	**Cargo:** Comité de Seguridad de la Información