POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN GP KARS S.A.S.

1. INTRODUCCIÓN

En la actualidad, para la compañía **GP KARS S.A.S.** la información se reconoce como un activo valioso, y a medida que los sistemas de información apoyan cada vez más los procesos, se quiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Reconocemos que, en la compañía, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso, o ataques de denegación de servicio se hacen cada vez más comunes.

Con la promulgación de la presente Política de Seguridad de la Información la compañía **GP KARS S.A.S.** formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de lo dispuesto por en el documento de **GP KARS S.A.S.** denominado **POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN Y DATOS PERSONALES (PTIDP).**

2. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- **Confidencialidad:** Los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- **Autenticidad:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de Auditoría:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan, sí es del caso, registros de las copias generadas de aquellos catalogados como confidenciales.

• **No repudio:**	Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
• **Legalidad:**	Los activos de información cumplen los parámetros legales, normativos y estatutarios de **GP KARS S.A.S.**
• **Confiabilidad de la Información:**	Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

3. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

GP KARS S.A.S., garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN** cuya composición y funciones serán reglamentada por el Gerente de la compañía.

La comisión, deberá revisar y actualizar periódicamente esta política presentando, cuando así lo considere, un informe al Gerente de la compañía para su aprobación.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1. Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

GP KARS S.A.S. establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión, incluyendo nuestra **POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN Y DATOS PERSONALES (PTIDP),** y alinearlos de forma efectiva con los demás sistemas de gestión que se llegaren a establecer.

4.2. Alcance

Esta política es de aplicación obligatoria para todo el personal que trabaje y llegare a trabajar en la compañía.

4.3. Objetivos

a) Proteger, preservar y administrar objetivamente la información de **GP KARS S.A.S.** junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la compañía **GP KARS S.A.S.** para asegurar su permanencia y nivel de eficacia.

c) Definir las directrices de **GP KARS S.A.S.** para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

4.4. Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de **GP KARS S.A.S.**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe. Las directivas de la compañía aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de **GP KARS S.A.S.**

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

Los propietarios de activos de información, son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de Recursos Humanos, o quien haga sus veces, cumplirá la función de notificar a todo el personal que se vincula contractualmente con **GP KARS S.A.S.**, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos,

procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

El encargado de atender peticiones, consultas y reclamos, en nuestra **POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN Y DATOS PERSONALES (PTIDP)** será el encargado de supervisar y seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la compañía.

5. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN.

Cada persona vinculada por contrato a **GP KARS S.A.S.** bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Oficina Asesora de Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

6. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal vinculado a **GP KARS S.A.S.**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles.

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de "Responsabilidades Personales para la Seguridad de la Información en la compañía **GP KARS S.A.S.**

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, recae en la persona encargada de atender las peticiones, quejas y reclamos.

6.1. Responsabilidades del personal de GP KARS S.A.S.

Todo el personal de **GP KARS S.A.S.**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de los recursos de la información y las reglas que autorizan el uso de la información institucional, así como en cuanto a los dispositivos hardware y los elementos software.

7. SEGURIDAD FÍSICA Y DEL ENTORNO

7.1. Acceso

Se debe tener máximo cuidado con los bienes de la compañía, muy especialmente con los computadores de la compañía.

7.2. Seguridad en los equipos

Los equipos que contengan información deben ser mantenidos en un ambiente seguro y protegido por los menos con:

• Controles de acceso y seguridad física.

• Bajo riesgo de inundación.

• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

No se permite el alojamiento de información institucional en servidores externos, salvo en los teléfonos inteligentes personales.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

8. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

8.1. Reporte e investigación de incidentes de seguridad

Cada funcionario debe velar porque el antivirus y el corta fuegos de su computador esté funcionando de manera correcta y la protección actualizada, se debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad.

El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

8.2. Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la compañía elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo de **GP KARS S.A.S.** deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

8.3. Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional, como las bases de datos, o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Se deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

8.4. Intercambio de Información con Organizaciones Externas.

La entrega de información a entes externos, de control debe ser aprobada siempre de manera previa por el Gerente de la compañía y para su entrega debe ser cumplida de manera integral toda la legislación que haya al respecto, así como el cumplimiento total de las disposiciones internas a ese respecto.

8.5. Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento de los más altos estándares de calidad, así como cumplir con el manejo responsable de los recursos de las tecnologías de la información.

8.6. Instalación de Software

Todas las instalaciones de software que se realicen sobre los equipos de **GP KARS S.A.S.** debe ser aprobada por la Oficina de Asesores externos de Sistemas y seguir todos los procedimientos establecidos para el efecto.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas.

8.7. Computación Móvil

GP KARS S.A.S. reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc), se obliga a elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

8.8. Aviso de privacidad

El siguiente aviso de privacidad deberá ser inserto en las comunicaciones de **GP KARS S.A.S.**

AVISO DE PRIVACIDAD

En cumplimiento a la Ley de Protección de Datos Personales en Posesión de los Particulares (la "Ley") le informamos los términos y condiciones del Aviso de Privacidad de **GP KARS S.A.S con** domicilio en la Calle 86 No 11 – 08 ESQ, Bogotá.

Los Datos Personales, como dicho término se define en la Ley, que usted libre y voluntariamente proporcione a **GP KARS S.A.S.** están destinados para fines de identificación, activación, venta, publicidad, estadística, análisis interno, información a clientes y consumidores, reclutamiento y selección de personal o cualquier otra actividad análoga de conformidad con el objeto social de **GP KARS S.A.S.** Nosotros registraremos, utilizaremos y protegeremos toda la información personal que reunamos sobre usted, de conformidad con lo dispuesto por la Ley sobre protección de datos y la política de privacidad de Nosotros. Utilizaremos su información personal principalmente para brindarle nuestro servicio de asesoría legal, productos y servicios, para poder comprender mejor sus intereses y necesidades con el objeto de mejorar los productos y servicios que más le interesan, así como enviarle información por mensajes de correo electrónico o SMS u otros mensajes a través de redes sociales sobre productos, ofertas y noticias que podamos considerar de su interés.

Esta información puede guardar relación con productos, ofertas y noticias de **GP KARS S.A.S.** o socios comerciales cuidadosamente seleccionados. Solamente se lo enviaremos si ha optado por la afirmativa para recibir mensajes de correo electrónico o SMS o redes sociales de **GP KARS S.A.S. GP KARS S.A.S.** podrá contratar a uno o varios terceros como proveedores de servicios para administrar los Datos Personales que se recaban a través de cualquier medio por **GP KARS S.A.S.,** por lo que podrá incluso transferir esa información a dicho (s) tercero (s) sin fines comerciales sino únicamente en cumplimiento de la prestación de servicios contratados. Asimismo, **GP KARS S.A.S**. podrá transmitir sus datos personales con y entre sus empresas subsidiarias y unidades de negocio para los fines mencionados en el párrafo inmediato anterior.

Usted podrá cancelar su registro en cualquier momento y también podrá optar por la negativa a recibir mensajes de correo electrónico y/o SMS o a través de redes sociales de **GP KARS S.A.S.** Además, usted podrá optar por que se elimine toda su información personal de nuestra base de datos. Si no desea recibir más ningún mensaje de correo electrónico y/o SMS de nosotros o a través de redes sociales, o si desea modificar sus datos personales o que sus datos personales sean eliminados de nuestra base de datos, le solicitamos comunicarse al teléfono 3902920 o enviando un correo electrónico a: info@maseraticolombia.com.

GP KARS S.A.S. tiene implementadas medidas de seguridad físicas, electrónicas y técnicas para proteger sus Datos Personales, por lo que su información personal se encuentra protegidas y sólo puede acceder a ella una cantidad limitada de personas con derechos especiales de acceso que también están obligadas a mantener dicha información confidencial. No obstante, recuerde que siempre que proporcione información personal en línea existe el riesgo de que otras personas puedan interceptar y utilizar dicha información. Si bien **GP KARS S.A.S.** se esfuerza por proteger la información personal y la privacidad de sus usuarios, no podemos garantizar la seguridad de la información que nos divulgue en línea, y usted lo hace corriendo con el riesgo que ello conlleva.