

# **POLÍTICA ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES**

## **USO INTERNO**

Cualquier uso, copia o distribución total o parcial de este documento, no autorizado, está prohibida y sancionada por Ley. El contenido íntegro de este documento es de propiedad de CARRO SEGURO CARSEG S.A., bajo el nombre comercial de HUNTER.

Asimismo, es de uso exclusivo y confidencial de los colaboradores de la empresa, en caso haya llegado a usted por error agradecemos eliminarlo. La versión vigente se encuentra bajo custodia del área de Organización y Métodos.

## 1. OBJETIVO

El objetivo del presente documento es establecer la Política Específica de Protección de Datos Personales de acuerdo a las normas vigentes ISO/IEC 27001:2013 y ISO/IEC 27002:2013, con la finalidad de proporcionar los lineamientos y principios básicos para gestionar de forma segura la información de CARRO SEGURO CARSEG S.A., bajo la razón comercial de HUNTER (en adelante "la empresa"), en lo que respecta al aseguramiento de la privacidad y la protección de datos personales en concordancia con la legislación aplicable.

## 2. ALCANCE

El presente documento está dirigido a:

- Todo el personal involucrado en el procesamiento de datos personales.

## 3. CONSIDERACIONES GENERALES

La Política Específica de Protección de Datos Personales debe ajustarse a lo establecido en el presente documento, debiendo tener en cuenta lo siguiente:

- Organización y métodos dispondrá de la difusión y control del presente documento de acuerdo a los lineamientos de la clasificación de la información que corresponda.
- Las infracciones y faltas a lo establecido en el presente documento serán sancionadas de conformidad a lo previsto en el Reglamento Interno de Trabajo.
- La Unidad de Auditoría Interna, dentro de su plan de trabajo, evaluará el cumplimiento de lo dispuesto en el presente documento.

## 4. CONCEPTOS

- Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la Ley orgánica de protección de datos personales, reglamento y resoluciones que se dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
- Base de datos o fichero:** Conjunto estructurado de datos personales, cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
- Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el Titular de los datos personales autoriza al Responsable del tratamiento de datos personales a tratar los mismos.
- Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- Responsable de tratamiento de datos Personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

- ☑ **Titular de datos personales:** Persona natural cuyos datos son objetos de tratamiento.
- ☑ **Transferencia o comunicación de datos personales:** Manifestación, declaración entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado de del tratamiento de datos personales. los datos personales que comuniquen deben ser exactos, completos y actualizados.
- ☑ **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.
- ☑ **Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

## 5. REFERENCIAS DOCUMENTARIAS

Código	Nombre del Documento
<b>SGSI.POL.001.01</b>	Política General de Seguridad de la Información
	Ley Orgánica de Protección de Datos Personales

## 6. DISPOSICIONES

Las políticas descritas definen las funciones y responsabilidades que deben seguir todo el personal involucrado en el procesamiento de datos personales de acuerdo a la Política Específica de Protección de Datos Personales de la empresa.

### 6.1. COMPROMISO DE CUMPLIMIENTO

1. Garantizar el cumplimiento de las disposiciones establecidas en las legislaciones vigentes y sus regulaciones, en materia de protección de datos personales.
2. Garantizar la confidencialidad en el tratamiento de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
3. Adoptar los niveles de seguridad de protección de los datos personales contenidos en las bases de datos de responsabilidad de la empresa, instalando los medios y las medidas técnicas, organizativas y legales a su alcance.
4. Garantizar la atención del ejercicio de derechos formulados por los Titulares, así como, la atención de las solicitudes o requerimientos formulados por la Autoridad de Protección de Datos Personales.

### 6.2. GENERALIDADES

1. La información es un activo valioso para la empresa, y en consecuencia requiere una protección adecuada. La seguridad de la información protege a esta de un amplio rango de amenazas para asegurar la continuidad de las actividades de la empresa y minimizar daños. Dentro de la información de la empresa se encuentran incluidos datos personales de diferentes usuarios, por lo que, el Oficial de Seguridad de la Información en su calidad de responsable de la Seguridad de la Información de la empresa se encuentra comprometido con el cumplimiento de la legislación vigente.
2. Con el fin de dar cumplimiento de las disposiciones establecidas en la legislación vigente (en relación a la Protección de Datos Personales), el Responsable de Protección de Datos Personales será quien brinde el soporte, asesoría y ayuda necesaria para dimensionar cualquier proceso, producto o servicio que requiera algún tipo de tratamiento de datos personales en concordancia con la legislación aplicable, gestionar la identificación e implementar los controles técnicos de la información e infraestructura que favorezcan al cumplimiento de las regulaciones aplicables, y demás actividades que conlleven al estricto cumplimiento de la legislación aplicable, coordinando e informando a la Gerencia General. La legislación señalada contempla disposiciones en materia de seguridad de los datos personales, por lo que, es de responsabilidad del Oficial de Seguridad de la Información gestionar el cumplimiento respectivo, previa coordinación con el Responsable de Protección de Datos Personales.
3. Todo el personal de la empresa y terceros guardará confidencialidad respecto al tratamiento, así como de la información de los datos personales a los que podría tener acceso, como parte de la ejecución de sus actividades y/o responsabilidades ante la empresa.
4. Todo el personal de la empresa que tuviera acceso a la información de datos personales deberá realizar el debido tratamiento del mismo, conforme se dispone en el presente documento y en las legislaciones aplicables.

### **6.3. TEMPORALIDAD DEL TRATAMIENTO**

La temporalidad del tratamiento de los datos personales de los Titulares por parte de la empresa son diferentes y se encuentran definidos en función a la finalidad del tratamiento. Por ello, los datos personales serán conservados mientras se mantenga la relación contractual entre los Titulares y la empresa, mientras no se soliciten su cancelación y/o en cumplimiento de obligaciones legales que apliquen.

Cuando la finalidad para lo cual han sido recopilados los datos personales haya culminado, el tratamiento de los datos personales será cancelado; sin embargo, se conservará la información registrada durante el tiempo en que pueda exigirse algún tipo de responsabilidad a la empresa derivada de la relación que mantenga con los Titulares y/o cuando por mandato legal así lo requiera.

### **6.4. CONFIDENCIALIDAD DE LOS DATOS PERSONALES**

Los datos personales serán tratados con total confidencialidad, por lo que, la empresa tiene el compromiso de guardar secreto profesional indefinidamente respecto de los mismos y garantiza el deber de guardarlos adoptando todas las medidas de seguridad y

confidencialidad necesarios para asegurar la confiabilidad, integridad y disponibilidad de la información recopilada.

### **6.5. TRANSFERENCIA DE DATOS PERSONALES**

No se transmitirán datos personales a terceros para las finalidades distintas a las establecidas, con la salvedad de requerimientos y/o obligaciones legales que correspondan (previa coordinación con el Responsable de Protección de Datos Personales).

Si como parte de sus operaciones la empresa debe transferir información de datos personales a terceros (a nivel nacional y/o internacional) se dispondrán de los recursos necesarios, previa coordinación con el Responsable de Protección de Datos Personales, para su realización y conforme a las legislaciones aplicables.

### **6.6. DERECHOS DEL TITULAR**

Los Titulares tienen el derecho de recibir la información sobre el tratamiento de sus datos personales; acceder (obtener de la empresa) a la información relativa de sus datos personales, así como a todas las condiciones y generalidades del tratamiento de los mismos; rectificar (actualizar o incluir) aquellos datos que han sido modificados a la fecha del ejercicio del derecho o que resulte ser incompleto, inexacto, erróneo o falso; cancelar (suprimir) el tratamiento de sus datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad por la que han sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento o en los demás casos en los que no están siendo tratados conforme se dispone en el presente documento; oponer al tratamiento de sus datos personales si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que lo justifique en el ejercicio de este derecho; así como, el de revocar su consentimiento para el tratamiento de sus datos personales, en cualquier momento, sin justificación previa y sin que le atribuyan efectos retroactivos, conforme se dispone en la legislación aplicable.

Para el ejercicio de los derechos de los Titulares, la empresa ha dispuesto los recursos necesarios para la atención de las solicitudes del ejercicio de derechos, siendo de responsabilidad del Responsable de Protección de Datos Personales ejercer dicha gestión. En ese sentido, aquellas solicitudes que guarden relación con la seguridad de la información serán solicitadas por el Responsable de Protección de Datos Personales al Oficial de Seguridad de la Información para la atención respectiva, considerando los requisitos y plazos previstos por la legislación aplicable.

### **6.7. NOTIFICACIÓN DE VULNERACIÓN DE SEGURIDAD**

El Responsable de Protección de Datos Personales es el encargado de gestionar la notificación de la vulneración de la seguridad de los datos personales, que se haya sufrido la empresa, a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones dentro del periodo establecido. Para ello, deberá de coordinar con el Oficial de Seguridad de la Información para recabar toda la información relacionada con la vulneración y cumplir con la notificación respectiva. asimismo, ambos

responsables con el responsable de TI gestionaran la facilidad de acceso a las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad (nacionales e internacionales) para efectuar tratamientos sobre los datos personales cometidos en las notificaciones de vulneración de seguridad, durante el tiempo necesario, exclusivamente para la detección análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

#### **6.8. AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES**

Las solicitudes y/o requerimientos que provengan de la Autoridad de Protección de Datos Personales, en materia de seguridad de la información serán solicitados al Oficial de Seguridad de la Información, quien será responsable de proporcionar toda la información que le solicite y dentro del tiempo requerido. Asimismo, ante las fiscalizaciones que la Autoridad de Protección de Datos Personales ejecute de manera presencial, el Oficial de Seguridad de la Información podrá participar o designar al Administrador de TI para atender los requerimientos en materia de su competencia.

#### **6.9. SANCIONES**

Ante el incumplimiento parcial o total de lo estipulado en el presente documento será motivo de sanción, siendo el Responsable de Protección de Datos Personales (en coordinación con el área de Gestión Humana) quien disponga de su aplicación conforme al Reglamento Interno de Trabajo.