Ley 29733

CÓDIGO DE CONDUCTA PARA LA PROTECCIÓN DE DATOS PERSONALES DEL GRUPO EUROMOTORS

CODIGO DE CONDUCTA PARA LA PROTECCION DE DATOS PERSONALES

DEL GRUPO EUROMOTORS

TITULO I

DISPOSICIONES GENERALES

Artículo 1°: Objeto

El presente Código de Conducta tiene por finalidad regular y unificar todas las acciones, disposiciones, criterios y políticas, así como todo aquello que sea concerniente al tratamiento de datos personales y su debida protección, aplicable de manera uniforme, vertical y horizontalmente, a todas las empresas que conforman el Grupo Euromotors, en cumplimiento del derecho fundamental a la protección de datos personales.

En tal sentido, su objetivo es lograr la protección y seguridad técnica, administrativa y legal para el tratamiento de los datos personales recabados por las empresas que conforma el Grupo Euromotors, en cumplimiento de la Ley de Protección de Datos Personales, su Reglamento, así como todas las normas concordantes, creadas o por crearse.

El Grupo Euromotors es un conglomerado de empresas vinculadas entre sí cuyo objetivo común es el desarrollo de la empresa automotriz en todas sus variantes, sin perjuicio de dedicarse a otras actividades, cuyo listado se aprecia en el **Anexo 1**, sin perjuicio de las nuevas empresas que conformen en un futuro el Grupo. Este Código de Conducta será de aplicación para todas las empresas del Grupo de Euromotors cuyo Directorio, o Gerencia General (en aquellas donde no haya Directorio), aprueben su contenido y dispongan su cumpliendo, incluyendo las modificaciones que se efectúen.

Artículo 2°: Ámbito de Aplicación

El presente Código de Conducta es de aplicación para la protección y tratamiento de la totalidad de datos personales recaudados de manera automatizada o no automatizada por parte de las empresas que conforman el Grupo Euromotors, ya sea través del consentimiento por parte de sus titulares, o que se encuentren exceptuados de ello con arreglo a Ley, estando todas las empresas, sus accionistas, directores, gerentes, apoderados, representantes, jefes, trabajadores, colaboradores, proveedores, responsables y/o encargados de tratamiento, y todos aquellos que pudieran tener acceso a información privilegiada, obligadas a su cumplimiento irrestricto.

El presente Código de Conducta abarca todos los procesos y/o actividades que se generen como consecuencia del tratamiento de datos personales, desde la recolección del consentimiento informado, el tratamiento en sí mismo, las acciones de tutela, las transferencias, los encargos, los procedimientos de seguridad técnica, administrativa, legal, y demás que se ejerciten en cumplimiento de la Ley.

Artículo 3°: Definiciones

3.1.- Banco de datos personales: Es la agrupación debidamente organizada de datos personales, automatizada o no, incorporada en cualquier tipo de soporte, que se haya creado, generado, se mantenga, organice, y a la que tengan acceso cualquiera de las empresas del Grupo Euromotors. Cada empresa es titular y responsable de su propio banco de datos.

3.2.- Bloqueo: Es la medida mediante la cual, el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación, supresión o cancelación.

3.3.- Cancelación o Supresión: Es la medida que consiste en eliminar o suprimir los datos personales de un banco de datos.

3.4.- Datos personales: Es cualquier tipo de información que identifique o esté referida a cualquier persona natural. Esta incluye, cualquier tipo de información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables, incluyendo sus perfiles digitales.

3.5.- Datos sensibles: Es cualquier dato personal referido a los datos biométricos de una persona natural, a su origen racial y/o étnico, ingresos económicos, ideologías, opiniones políticas, religiosas, o morales, afiliación sindical, información vinculada con su salud o vida sexual, u otra análoga.

3.6.- Encargado de tratamiento de datos personales: Es quien realiza el tratamiento directo de los datos personales por encargo de las empresas del Grupo Euromotors, en sus calidades de titulares de sus respectivos bancos de datos, en virtud de una relación jurídica que las vincula con el mismo, ya sean colaboradores de las mismas empresas, o ya sea empresas terceras que reciben el encargo de tratamiento debidamente definido, guardando la protección y confidencialidad física, legal y administrativa.

3.7.- Flujo transfronterizo de datos personales: Consiste en la transferencia de datos personales a destinatarios en el extranjero.

3.8.- Rectificación: Es la medida dirigida a modificar un banco de datos personales ya sea para actualizarlo, incluir información o rectificar su contenido.

3.9.- Titular de datos personales: Es la persona natural a quien corresponde los datos personales.

3.10.- Titular del banco de datos personales: Son cada una de las empresas del Grupo Euromotors, respecto de sus correspondientes bancos de datos, de los cuales son titulares

3.11.- Transferencia de datos personales: Es toda transmisión y/o comunicación y/o cesión de datos personales de los bancos de datos de las empresas del Grupo Euromotors, entre sí, o a terceros, a nivel nacional o internacional.

3.12.- Tratamiento de datos personales: Es toda operación o procedimiento, sin importar su naturaleza, que permita la recolección, registro, organización, almacenamiento, conservación,

elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales, incluyendo la elaboración y manejo de perfiles automatizados o no de cualquier tipo de dato personal.

3.13.- Oficial de Datos Personales: Es la persona designada por cada empresa titular de bancos de datos del Grupo Euromotors, siendo posible la designación de un nombramiento conjunto del Oficial para todas ellas, responsable de tratamiento o encargado del tratamiento de datos personales para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.

Artículo 4°: Cómputo de Plazos

Todos los plazos establecidos en este Código de computan en días hábiles, de lunes a viernes excluyendo los sábados, domingos, feriados nacionales, y feriados no laborables dispuestos mediante norma legal.

TITULO II

PRINCIPIOS DE PROTECCION

Artículo 5°: Legalidad, Consentimiento y Finalidad

Los datos personales únicamente podrán ser tratados de manera lícita, leal y transparente, en cumplimiento de la Ley de Tratamiento de Datos Personales, su Reglamento, y demás normas modificatorias, ampliatorias, y otras que pudieran promulgarse sobre la materia, adecuados, pertinentes y limitados a los fines para los que se hayan obtenido, que en todos los casos deberán ser determinados, explícitos y legalmente permitidos, contando para ello con el consentimiento previo de su titular, salvo las excepciones establecidas por ley.

Artículo 6°: Proporcionalidad, Calidad y Exactitud

El tratamiento de los datos deberá ser exacto, preciso, pertinente, necesario y relevante, para cumplir con la finalidad para la cual fue recabado, o conforme a la finalidad requerida para los casos de tratamiento de datos que no requieran consentimiento, y estarán actualizados para ello.

Si los datos resultaran inexactos o estuvieran desactualizados o incompletos, en la medida de lo posible se deberá tratar de rectificar, actualizar y completar con los datos correctos, en un plazo máximo de cinco días desde que tomó conocimiento de ello; de no ser posible ello, los datos serán cancelados y suprimidos.

Artículo 7°: Seguridad y Confidencialidad

Toda persona que tenga cualquier tipo de contacto con los datos personales de los bancos de datos de titularidad de las empresas del Grupo Euromotors, sean colaboradores, proveedores, directivos, apoderados, representantes, trabajadores, o cualquier tercero por encargo, está obligado a guardar plena confidencialidad de éstos, siendo información estrictamente reservada. Para el tratamiento de los datos, ello será única y exclusivamente de carácter temporal y para el cumplimiento de sus labores y/o encargo, y para la finalidad específica autorizada por el consentimiento o por ley, por lo que está prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en el cualquier tipo de soporte, sea cual fuere su naturaleza; asimismo, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que la empresa le haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno; asumiendo plena responsabilidad por las consecuencias y sanciones que se deriven del uso indebido por parte de él o terceras personas relacionadas.

El incumplimiento de las normas de confidencialidad respecto de los datos personales por parte de cualquier trabajador o colaborados de las empresas que conforma el Grupo Euromotors, deberá ser objeto de sanción con arreglo a la legislación aplicable, por comisión e infracción muy grave, sancionable con despido.

Las empresas del Grupo Euromotors, tienen la obligación de implementar medidas técnicas y organizativas idóneas para la protección de los datos personales objeto de tratamiento, con arreglo a la Ley de Protección de Datos Personales, su Reglamento, las normas modificatorias o ampliatorias que se promulguen, y conforme al presente Código.

Artículo 8°: Disposición de Procedimientos

Todas las empresas del Grupo Euromotors deberán habilitados canales de atención y procedimientos para el ejercicio de los derechos de acceso a la información de los datos personales proporcionados por el titular de los datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos.

TITULO III

EL CONSENTIMIENTO

Artículo 9°: Obtención del consentimiento

Para la obtención del consentimiento de los titulares de datos personales, las empresas del Grupo Euromotors deberán guiarse preferentemente del modelo de Consentimiento Para el Tratamiento de Datos Personales – Clientes y Prospectos que como **Anexo 2.1** forma parte de este Código, y para el caso

de recopilación de consentimiento de datos que formen parte de otros documentos como por ejemplo cotizaciones, pedidos, u otros análogos, deberán guiarse de la versión resumida de modelo de Consentimiento Para el Tratamiento de Datos Personales – Clientes y Prospectos que como **Anexo 2.2** forma parte de este Código; estos formatos aplicarán para el caso de la obtención del consentimiento de clientes y prospectos. Para el caso de la obtención del consentimiento de colaboradores, proveedores, trabajadores, operadores y terceros en general que no califiquen como clientes o prospectos, podrán guiarse del formato de Consentimiento Para el Tratamiento de Datos Personales – Colaboradores y Terceros en General que como **Anexo 2.3** forma parte de este Código.

De igual forma, para la recopilación del consentimiento de datos en línea, podrán guiarse del formato de Política de Privacidad – Protección de Datos Personales que como **Anexo 3** forma parte de este Código. La obtención de los datos y del consentimiento podrá realizarse bajo cualquier modalidad, escrita y/o digital y/o informática y/o móvil, que permita documentar y obtener prueba material o evidencia de haber logrado el consentimiento expreso por parte del titular de los datos.

La recopilación de los datos personales deberá asegurar y garantizar que el consentimiento que se obtiene del titular de datos personales haya sido totalmente libre y voluntario. Estará permitido la entrega de obsequios o premios con ocasión de la obtención del consentimiento para el tratamiento de los datos, lo cual no afectará la condición de libertad de su titular para otorgarlos, a excepción del caso de los menores de edad, a los que no se está permitido entregar ningún tipo de regalo.

Asimismo, el consentimiento deberá obtenerse de manera previa a cualquier acción de tratamiento.

Artículo 10°: Consentimiento Informado

El consentimiento informado y explícito, voluntario, previo, expreso e inequívoco, deberá constar en documento escrito o mediante cualquier mecanismo, canal o vía electrónica o digital que permita acreditarlo de manera cierta; todo consentimiento deberá necesariamente que constar en algún soporte que permita su acreditación.

El documento físico o virtual o digital o electrónico mediante el cual el titular de los datos personales concede el consentimiento para el tratamiento de sus datos personales, deberá contener e informar a éste por lo menos lo siguiente:

10.1.- La denominación social, R.U.C. y dirección de la empresa del Grupo Euromotors titular del banco de datos, y el dato de contacto para que el titular de los datos pueda dirigirse para ejercer sus derechos.

10.2.- Los propósitos específicos para las cuales las empresas del Grupo Euromotors solicitarán consentimiento voluntario, libre, previo, expreso, informado e inequívoco para el tratamiento de datos personales.

10.3.- La identidad de los que son o pueden ser sus destinatarios.

10.4.- Se dejará expresa constancia de la existencia del banco de datos personales en que se almacenarán éstos, precisando que está debidamente registrado ante la Autoridad Nacional de Protección de Datos Personales, así como su identificación de registro.

10.5.- Precisar que es facultativo otorgar el consentimiento de los datos, salvo aquellos indispensables para el cumplimiento de las relaciones contractuales o tratativas que se generen, y que estén exceptuados por Ley.

10.6.- Precisar que el otorgar el consentimiento únicamente permitirá el tratamiento de los datos conforme al documento mediante el cual se otorga.

10.7.- Precisar que los datos personales serán objeto de transferencia y encargo nacional e internacional.

10.8.- Precisar que los datos podrían ser objeto de decisiones y tratamientos por medios tecnológicos, automatizados o no, con o sin intervención humana, incluida la elaboración de perfiles, para las finalidades por las cuales se otorgaron los consentimientos.

10.9.- El plazo de conservación de los datos personales será indefinido.

10.10.- Señalar de modo explícito los mecanismos para el ejercicio de los derechos de los titulares de los datos personales.

Artículo 11°: Excepciones al Consentimiento

Sin perjuicio de lo señalado en los artículos 9° y 10°, los datos personales podrán ser tratados sin necesidad de consentimiento, siempre que el mismo está justificado en cualquiera de las excepciones establecidas por ley, como por ejemplo, para el ejercicio de las funciones de las entidades públicas para el cumplimiento de sus deberes, acceso a fuentes de datos públicos, para la celebración, cumplimiento y ejecución de relaciones contractuales, y las demás que legalmente están establecidas, o se establezcan en un futuro.

Artículo 12°: Política de Privacidad

Para el caso detallado en el artículo 11°, las empresas del Grupo Euromotors deberán tratar los datos personales en mérito a una política de privacidad que debe cumplir con los requisitos del artículo 10°, en todo lo que sea aplicable, y en respeto de los derechos de los titulares de los datos personales con arreglo a Ley. Las empresas de Grupo Euromotors podrán guiarse del modelo de Política de Privacidad que como **Anexo 4.1** forma parte de este Código, la cual deberá estar exhibida en sus respectivas páginas web, difundida y a disposición pública cada vez que sea requerido; en el caso de envío de correos electrónicos, podrán guiarse del texto sobre protección de datos personales que como **Anexo 4.2** forma parte de este Código, haciendo uso del mismo al final de los mensajes, y haciendo referencia al cumplimiento de dicha Política de Privacidad. De igual manera, para las interacciones de las empresas del Grupo Euromotors a través de sus plataforma digitales o electrónicas, las mismas se sujetarán a las Condiciones de Uso de Plataformas Virtuales y Digitales básicas que como **Anexo 4.3** se adjuntan.

Para el caso de los locales que cuenten con cámaras de seguridad, deberán tener exhibidos de manera visible, carteles informativos de protección de datos conforme al modelo adjunto como **Anexo 5**.

Esta Política de Privacidad será la que rija el tratamiento de todos los datos de aquellos trabajadores, colaboradores, directivos, ejecutivos, apoderados, empleados, proveedores, visitantes, y demás

personas en general, con las que mantenga algún tipo de relación o vínculo contractual, o tratativas para la celebración de un contrato, cuyos datos son necesarios para el cumplimiento de dichas relaciones, así como respecto de cualquier otra persona cuyos datos sean recabados sin necesidad de consentimiento, con arreglo a las excepciones establecidas por Ley.

TITULO IV

DERECHOS DEL TITULAR DE DATOS PERSONALES

Artículo 13°: Derechos

El titular de datos personales tiene la facultad de ejercer de manera irrestricta los derechos de información, actualización, acceso, rectificación, cancelación, oposición, inclusión, supresión, impedimento de suministro, y tratamiento objetivo de datos personales, los cuales sólo podrán ser ejercidos por el propio titular, o mediante representante especialmente facultado por poder que contenga el encargo específico con firma notarialmente legalizada del poderdante.

En caso los datos hubieran sido transferidos de manera previa al ejercicio de cualquiera de estos derechos, el titular de la base de datos deberá comunicar inmediatamente ello a los receptores de los datos para que efectúen las modificaciones que corresponda.

Mientras dure el procedimiento de ejercicio de los derechos de actualización, inclusión, rectificación o supresión de datos personales, el titular de la base de datos dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos.

Artículo 14°: Requisitos para el Ejercicio de los Derechos

El titular de los datos personales deberá remitir solicitud escrita o virtual al titular del banco de datos personales, dirigida a la dirección física o virtual consignada en los documentos de consentimiento o políticas de privacidad, precisando lo siguiente:

14.1.- Nombres y apellidos del titular del derecho, y en su caso de su representante, adjuntando copia de sus respectivos documentos nacionales de identidad.

14.2.- Determinación concreta del petitorio y del derecho que se ejerce.

14.3.- Domicilio físico o dirección electrónica a efectos de que pueda ser notificado con los actuados del procedimiento.

14.4.- Fecha y firma del solicitante.

14.5.- Documentos que sustenten la solicitud y pretensión, de ser el caso.

Artículo 15°: Procedimiento

Recibida la solicitud de ejercicio de derechos por parte del titular de datos personales, el titular de la base de datos tiene un plazo máximo de cinco días para calificarla; en caso la misma no cumpla con los requisitos establecidos en el artículo 14°, se cumple con notificar al titular de los datos, dentro de esos mismos cinco días, las observaciones que requieran subsanación, para que cumpla con ello en un plazo máximo de cinco días; en caso no se cumpla con la observación, la solicitud se tiene por no presentada.

En el caso que la información o documentación presentada en la solicitud sea insuficiente o equivocada, e impida darle trámite, el titular del banco de datos personales podrá requerir dentro de los siete días siguientes de recibida la solicitud, la documentación e información adicional o correcta al titular de los datos personales para atenderla; este último tendrá diez días para atender el requerimiento, caso contrario, se tendrá por no presentada la solicitud.

Si la solicitud presentada cumple con todos los requisitos, los plazos de atención y repuesta por parte del titular del banco de datos personales serán los siguientes, computados a partir del día siguientes de la fecha de presentación:

15.1.- Ocho días ante el ejercicio del derecho de información.

15.2.- Veinte días ante el ejercicio del derecho de acceso.

15.3.- Diez días ante el ejercicio de los otros derechos como los de actualización, rectificación, cancelación, supresión, inclusión u oposición.

Para el caso de solicitudes observadas, los plazos antes indicados se computarán a partir del día siguiente de la presentación de la subsanación correspondiente.

Con excepción al cumplimiento del plazo fijado para la atención ante el ejercicio del derecho de información, los demás plazos correspondientes a la atención de los demás derechos podrán ser objeto de ampliación por una sola vez, y por un plazo igual, como máximo, en tanto exista justificación para ello, debiendo notificarse tal determinación al titular del dato personal, dentro del plazo que se disponga a ampliar.

Para el ejercicio de derechos por parte del titular de datos personales, éste podrá hacer uso del formato que se adjunta como **Anexo 6.1** al presente Código de Conducta. Asimismo, para la atención de estas solicitudes, se deberá aplicar el Documento de Gestión para Atención de Derechos ARCO y el Instructivo para Respuesta al Ejercicio de Derechos ARCO que como **Anexos 6.2 y 6.3**, respectivamente, se adjuntan.

Artículo 16°: Derecho a la Información y Acceso

El titular de datos personales tiene derecho, en vía de acceso, a que se le brinde toda la información sobre sus datos personales, el tratamiento que se les ha dado, la finalidad para la que los otorgó, cómo, cuándo y los motivos por lo que los otorgó, a solicitud de quién se recopilaron los datos, quiénes son o han sido o podrían ser sus destinatarios (precisando su identidad), la existencia del banco de datos en que están contenidos, la identidad y domicilio del titular del banco, los encargados del tratamiento de sus datos personales, si existe obligatoriedad o no en mantener sus datos, y los motivos de ello, las transferencias de los datos personales que se hayan hecho o se podrían hacer, las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo, el tiempo durante el cual se conservarán

sus datos personales, y las posibilidades y mecanismos que tiene para ejercer los derechos que la ley le concede. La atención a la solicitud deberá estar dirigida a absolver las consultas precisas hechas por el titular de los datos; en caso de solicitar de manera general ejercer el derecho a la información y acceso, se deberá proporcionar toda la información antes descrita, y nunca revelar información de terceros.

Como prerrogativa al derecho de acceso, el titular de los datos personales tendrá el derecho a la portabilidad de sus datos, a través del cual podrá solicitar al titular o responsable del banco de datos sus datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable o titular de banco de datos, cuando: (i) el tratamiento de sus datos haya sido consentido o sea necesario para el cumplimiento de una relación contractual donde el titular de los datos es parte, o (ii) el tratamiento se ejerza mediante medios automatizados.

Artículo 17°: Derecho de Actualización y Rectificación

El titular de datos personales tiene derecho, en vía de rectificación, a actualizar aquellos datos que han sido modificados a la fecha del ejercicio del derecho, así como a rectificar aquellos datos que resulten inexactos, erróneos o falsos; para lo cual, la solicitud deberá acompañar la documentación que sustente la procedencia de la actualización y/o rectificación solicitada.

Artículo 18°: Derecho de Inclusión

El titular de datos personales tiene derecho, en vía de rectificación, a que sus datos sean incorporados a un banco de datos personales, y que sus datos personales faltantes o la información que la hace incompleta, omitida o eliminada, sea incorporada para un debido tratamiento. La solicitud de inclusión deberá precisar los datos personales se piden agregar, acompañando la documentación que sustente.

Artículo 19°: Derecho de Supresión o Cancelación.

El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales, ya sea de manera o total, cuando éstos ya no sean necesarios para cumplir con la finalidad por la cual se obtuvieron, cuando se haya vencido el plazo establecido para su tratamiento, o cuando ha revocado su consentimiento para el tratamiento.

El titular del banco de datos personales tiene obligación de documentar ante el titular de los datos personales haber cumplido con la supresión y cancelación solicitada, y precisar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente.

La supresión no procederá cuando los datos personales deban ser conservados en razón de las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos.

Artículo 20° Derecho de Oposición

El titular de datos personales tiene derecho a oponerse al tratamiento de sus datos personales o al cese de ello, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público. Este derecho también es aplicado aun cuando el titular de datos personales hubiera prestado su consentimiento, acreditando para ello la existencia de motivos que justifiquen ello.

Artículo 21°: Derecho al tratamiento objetivo de datos personales

En el caso del tratamiento de datos personales que estén involucrados en parte de un proceso de toma de decisiones sin participación de su titular, el titular del banco de datos personales deberá informárselo en término máximo de cinco días de tomado conocimiento de ello.

Asimismo, el titular de los datos personales tiene derecho a no ser objeto de decisiones que lo puedan afectar significativamente, le produzcan efectos jurídicos, discriminación, o cualquier efecto negativo que determine aspecto personales del mismo, como su rendimiento profesional, situación económica, orientación o identidad sexual, entre otros.

TITULO V

BANCO DE DATOS

Artículo 22°: Registro

Las empresas del Grupo Euromotors deberán cumplir con inscribir sus respectivos bancos de datos en el Registro Nacional de Protección de Datos Personales. Las bases de datos a ser inscritas podrán ser las de:

22.1.- Base de datos de clientes y prospectos.

22.2.- Base de datos de proveedores.

22.3.- Base de datos de trabajadores, colaboradores y postulantes.

22.4.- Base de datos de cámaras de videovigilancia.

Se podrán incluir, de considerarlo necesario y oportuno, otras bases de datos de acuerdo con las necesidades de cada empresa, así como modificar, separar o estructurar las bases de datos antes propuestas de acuerdo con sus necesidades.

TITULO VI

TRANSFERENCIA DE DATOS PERSONALES

Artículo 23°: Transferencias de Datos

Son transferencias de datos personales las cesiones o comunicaciones que hace el titular de la base de datos a un tercero, sea a nivel nacional o internacional (flujo transfronterizo) a terceros. Estas

transferencias serán permitidas siempre que se cuente con autorización expresa en dicho sentido por parte del titular de los datos personales, o, cuando ello está justificado en cualquiera de las excepciones establecidas por Ley, como por ejemplo, para el ejercicio de las funciones de las entidades públicas para el cumplimiento de sus deberes, acceso a fuentes de datos públicos, para la celebración, cumplimiento y ejecución de relaciones contractuales, y las demás que legalmente están establecidas, o se establezcan en un futuro.

Artículo 24°: Obligación del Receptor de los Datos

El receptor de los datos producto de una transferencia, necesariamente quedará obligado a las regulaciones de la Ley de Protección de Datos Personales, su Reglamento, normas modificatorias o ampliatorias, y al presente Código; debiendo asegurar todas las medidas de protección y prevención a nivel operativo, organizativo, técnico y jurídico, así como la confidencialidad total de los datos, pudiéndolos tratar únicamente para las finalidades para las cuales fueron otorgados por su titular y bajo las estipulaciones informadas y aceptadas por éste, o que tengan justificación en las excepciones de ley para los casos de tratamiento de datos que no requieran consentimiento previo; ello, en tanto el receptor de los datos personales materia de transferencia, asume la condición de titular del banco de datos personales. En tal sentido, los receptores de datos quedarán igualmente obligados a respetar el ejercicio de los derechos que los titulares de datos personales quieran ejercer respecto de sus datos personales.

Artículo 25°: Destinatarios y Convenios

Todas las empresas que conforman el Grupo Euromotors, que previamente hayan aprobado y se hayan acogido al presente Código, podrán transferir entre sí los datos personales de sus respectivas bases de datos. Para ello, en los documentos de Consentimiento Para el Tratamiento de Datos Personales mediante los cuales se recabe el consentimiento para el tratamiento, se deberá informar de las transferencias de datos amparados en este Código, con lo que se garantiza el debido tratamiento de los datos y sus transferencias, con seguridad y confidencialidad; estas transferencias también podrán ser efectuadas sin necesidad de consentimiento previo, en los exceptuados y autorizados por ley. Las transferencias realizadas entre las empresas del Grupo Euromotors garantizarán el debido tratamiento de los datos por el solo mérito de haberse acogido y aprobado este Código para regir sus conductas para el tratamiento de datos personales.

Para el caso de transferencias de datos personales a terceros ajenos al Grupo Euromotors a nivel internacional (flujo transfronterizo), las mismas se harán necesariamente previa suscripción con el receptor de los datos, de un convenio que cumpla con las medidas de protección, confidencialidad y de seguridad requeridas por Ley para el debido tratamiento de los datos personales transferidos, asegurando que se cumpla con la finalidad autorizada y consentida para el tratamiento por parte de su titular, pudiendo utilizar y tomar como referencia el modelo de Convenio de Transferencia de Datos Personales y Condiciones para su Tratamiento y Protección que como **Anexo 7** forma parte de este Código, en respeto de los consentimientos datos por sus titulares, o para el cumplimiento de las finalidades que legalmente no requieran dicho consentimiento, y en protección y defensa de los derechos de los titulares de datos personales. Para el caso de las transferencias nacionales, sin perjuicio

de que se recomienda la suscripción de convenios en este mismo sentido, por lo menos se deberá asegurar que el receptor de los datos esté debidamente informado de las condiciones del consentimiento de éstos, y así asegurar el debido tratamiento.

Estas transferencias de datos que se prevén realizar estarán dirigidas principalmente a satisfacer las necesidades para el cumplimiento de las obligaciones contractuales, de las prestaciones de servicios y cumplimiento de los fines del negocio, relacionamiento con proveedores, y todo aquello necesario para que cada una de las empresas del Grupo Euromotors pueda desarrollar su objeto social, y cumplir con las obligaciones y relaciones sostenidas con sus clientes. En este sentido, considerando que el tipo de negocio que es común denominador del Grupo Empresarial está referido al sector automotriz, las transferencias datos podrán darse con los fabricantes de los vehículos que comercializan éstas, los representantes de las marcas de dichos vehículos en el Perú, los concesionarios y talleres oficiales de dichas marcas a nivel nacional, empresas del sistema financiero y empresas administradoras de fondos colectivos, proveedores necesarios y todos aquellos con los que sean necesario realizar las transferencias para el cumplimiento de obligaciones contractuales. Sin perjuicio de ello, y de acuerdo a sus necesidades, cada titular de base de datos podrá evaluar y determinar la pertinencia de la transferencia de datos, nacional o transfronteriza, de acuerdo a sus necesidades, y siempre que previamente se haya recabado el consentimiento previo e informado expreso por parte del titular de datos, o en los casos exceptuados por Ley que se permita el tratamiento.

TITULO VII

RESPONSABLES DEL TRATAMIENTO - ENCARGADOS DEL TRATAMIENTO - TRATAMIENTOS DE DATOS POR ENCARGO

Artículo 26°: Responsables del Tratamiento

Al interior de cada una de las empresas que conforman el Grupo Euromotors, el Gerente General de cada una de ellas, apoyado por todos los Jefes de todas las áreas de cada organización, será responsable de implementar y aplicar todas las medidas de protección y seguridad organizativa, técnica y jurídica, a efectos de la protección y debido tratamiento de los datos personales. La estructura organizacional y delimitación de responsabilidades es la que se define en el artículo 32° de este Código.

Todo aquel que tenga a su cargo, a su disposición, alcance o acceso a cualquier dato personal, o a cualquier equipo o instrumento que permita dicho acceso, difusión o posibilidad de ser compartido o revelado, realice cualquier tipo de tratamiento de datos personales, o cuya omisión genere cualquier tipo de consecuencia respecto de cualquier dato personal, será directamente responsable de ello, asumiendo las consecuencias civiles, penales, administrativas, funcionales y laborales que ello genere. Cualquier infracción o incumplimiento de la Ley de Protección de Datos Personales o su Reglamento, normas ampliatorias, modificatorias o sustitutorias, o del presente Código de Conducta, o cualquier afectación, por acción u omisión, al derecho a la protección de datos personales de cualquier titular de éstos, se considerará una falta gravísima para todos los efectos.

Artículo 27°: Encargados del Tratamiento

Todo aquel que, al interior de las empresas que conforman el Grupo Euromotors, ya sean sus colaboradores, trabajadores, apoderados, representantes, directivos, u otros, en cumplimiento de sus funciones y obligaciones, para los fines autorizados por ley y/o bajo consentimiento, serán encargados de tratamiento de datos personales; y como tales, están obligados al cumplimiento irrestricto de la Ley de Protección de Datos Personales y su Reglamento, normas ampliatorias o modificatorias, del presente Código, con la debida seguridad y confidencialidad.

Todo tratamiento de datos personales por parte de los encargados del tratamiento se realizará de manera temporal, y únicamente podrá utilizar la información y/o cualquier dato personal para cumplir con los encargos específicos de sus labores, y nunca para otra finalidad, ni mucho menos en otra oportunidad. De esta manera, el encargado del tratamiento queda expresamente prohibido de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuviere acceso o conociera durante la vigencia de su relación con la empresa, para fines no autorizados y/o ajenos a sus obligaciones, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que la empresa le haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno; asumiendo plena responsabilidad por las consecuencias y sanciones que se deriven del uso indebido por parte de él o terceras personas relacionadas.

Toda información o datos personales que sean proporcionados al encargado del tratamiento de datos o a la que tenga acceso para el cumplimiento de sus funciones, sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada, y solo podrá ser usada y tratada para el cumplimiento de sus funciones y para las finalidades autorizadas y permitidas.

Artículo 28°: Tratamiento por Encargo

Las empresas del Grupo Euromotors podrán valerse de terceros ajenos su propia organización para efectos del tratamiento de datos personales de sus bases de datos. La entrega de datos a este tercero encargado del tratamiento no constituye la transferencia de estos a éste, quien únicamente está autorizado a tratar los datos bajo las directivas del encargo realizado.

Para materializar el tratamiento por encargo a cargo de un tercero, las empresas del Grupo Euromotors deberán suscribir un contrato de tratamiento por encargo, que asegure la debida confidencialidad y seguridad jurídica, técnica y organizativa, especificando las únicas finalidades autorizadas para realizar el tratamiento, así como el carácter temporal y determinación clara y precisa de que los datos materia de encargo no son objeto de transferencia.

Los terceros a quienes se les confíe este tratamiento por encargo deberán cumplir con todas las obligaciones descritas en el artículo 27°, y deberán suscribir con estos acuerdos en los que se garantice las medidas de protección, confidencialidad y de seguridad requeridas por Ley para el debido tratamiento de los datos personales transferidos, asegurando que se cumpla con la finalidad autorizada y consentida por el titular para el tratamiento que se encarga, pudiendo utilizar y tomar como referencia el modelo de Convenio de Tratamiento por Encargo que se adjunta como **Anexo 8**.

Culminado el encargo, los datos personales que fueron materia de encargo para su tratamiento, deberán ser restituidos por estos terceros a sus respectivos titulares, o de ser el caso, destruir toda la información, estando dichos terceros terminantemente prohibidos de conservar ningún tipo de dato ni información.

TITULO VIII

MEDIDAS DE SEGURIDAD

Artículo 29°: Medidas de seguridad

Para garantizar los derechos de los titulares de datos personales, se aplicarán medidas técnicas, organizativas y jurídicas apropiadas a los datos tratados y a la naturaleza, alcance, contexto y finalidad del tratamiento.

Para evaluar el nivel de seguridad y las medidas concretas que se deben aplicar para la protección de los datos personales, se considerarán los riesgos a los que estén expuestos los datos personales, contra su destrucción, pérdida o modificación indebida o ilícita, filtración, accesos o invasiones no autorizadas o ilegales.

En el caso de cualquier incidente de seguridad que comprometa los datos personales recopilados, el titular del banco de datos o responsable del tratamiento deberá comunicarlo a la Autoridad Nacional de Datos Personales dentro de las 48 horas siguientes de haber tomado conocimiento de la vulneración de seguridad, salvo que requiera de mayor tiempo que deberá sustentar, aun cuando el incidente se hubiera superado satisfactoriamente; si la vulneración se ha producido en un entorno digital, entonces la comunicación también deberá realizarse al Centro Nacional de Seguridad Digital. La notificación del incidente de seguridad y vulneración de los datos personales deberá incluir la precisión de la naturaleza del mismo, el nombre del Oficial de Datos Personales del titular del banco de datos vulnerado, las posibles consecuencias del incidente, y las medidas adoptadas o propuestas de subsanación para revertir y/o remediar la vulneración. Todo incidente de seguridad deberá documentarse desde su identificación hasta la culminación del mismo con la solución y/o medidas de remediación que correspondan, conforme al **Anexo 10.10** – Procedimiento Para la Atención de Incidencias.

Si el incidente de seguridad produjera la afectación de otros derechos al titular de datos personales, se deberá comunicar a todos los afectados en un plazo de 48 horas siguientes de haber tomado conocimiento del hecho, así como las medidas que se han adoptado o se tomarán mara mitigar dichos efectos.

Artículo 30°: Medidas de Seguridad en el Tratamiento de Datos Personales en Plataformas Digitales

Las medidas de prevención y seguridad en el tratamiento de datos personales en medios digitales, cualquiera la plataforma en la que estén contenidos deberá prever controles permanentes y procedimientos debidamente regulados para su acceso, otorgamiento y gestiones de privilegios, mediante el otorgamiento de usuarios y claves de ingreso a los sistemas que permitan acceder a los

datos personales, mecanismos de autenticación, cumpliendo con verificación y control periódico; así como la configuración de los sistemas de manera idónea, de modo que proporcionen la mínima funcionalidad para el correcto tratamiento de datos, medidas de detección, prevención, control, y eventual recuperación, que permitan eliminar o reducir amenazas de seguridad.

Los servidores que contengan datos personales deberán estar ubicados en ambientes igualmente seguros y protegidos, con acceso restringido y bajo llave u otro mecanismo que impida su acceso a cualquier persona no autorizada.

Toda máquina o terminal o servidor desde la que se pueda acceder a datos personales deberá encontrarse en áreas seguras, debidamente protegidas con restricciones de acceso reservadas únicamente para personal con los privilegios concedidos, y sin posibilidad de puertos o salidas que permitan la reproducción o salida de información no autorizada. Está prohibido retirar los equipos o terminales fuera de las instalaciones, salvo que sean de uso personal asignado y debidamente autorizado para el ejercicio de las labores asignadas, y bajo control y restricciones de acceso para personal con privilegios y mecanismos de autenticación.

Artículo 31°: Medidas de Seguridad en el Tratamiento de Datos Personales en Soporte Físico

Las medidas de prevención y seguridad en el tratamiento de datos personales contenidos en soportes físicos o no automatizados deberán estar protegidos en ambientes debidamente acondicionados y protegidos con cerraduras, llaves u otras medidas de seguridad que impidan su acceso a personas no autorizadas. Únicamente tendrán acceso a estos datos aquellos a los que se les haya otorgado el permiso correspondiente, para el cumplimiento de sus labores y obligaciones.

Artículo 32°: Estructura Organizacional

Cada una de las empresas del Grupo Euromotors que adopte el presente Código de Conducta, deberá implementar dentro de sus propias organizaciones corporativas, la asignación de responsabilidades para la implementación, cumplimiento y control de todas las medidas de confidencialidad, seguridad y de respeto y protección de datos personales, en cumplimiento de la Ley y del presente Código.

Esta estructura organizacional deberá contar por lo menos con la asignación de los siguientes responsables, y cumplir con las siguientes funciones:

32.1.- Responsable del banco de datos: Responsable y encargado de implementar, ejecutar, y dar cumplimiento de la política de protección de datos personales en todos sus niveles, a nivel transversal y como autoridad máxima dentro de la empresa. Esta asignación deberá recaer en el Gerente General.

32.2.- Responsable de Seguridad Tecnológica: Responsable de implementar las medidas de seguridad informática y correcto desenvolvimiento de las plataformas digitales en las que se tratan los datos personales, protección contra sustracción de información automatizada, administración de accesos y privilegios a los sistemas. Responsable de abrir, llevar y controlar los registros de documentos, de personal con accesos, de incidentes y medidas adoptadas, de los accesos concedidos y sus variaciones, a nivel informático y digital.

32.3.- Responsable de Seguridad No Tecnológica: Responsable de llevar el control y debido registro de las bases de datos ante la Autoridad Nacional de Protección de Datos Personales, y de mantener una permanente difusión del cumplimiento de la política de protección de datos personales, de su importancia, de las responsabilidades que ello implica, de los procedimientos, documentación e información que la componen, así como del presente Código y de la Ley. Responsable de abrir, llevar y controlar los registros de documentos, de personal con accesos, de incidentes y medidas adoptadas, de los accesos concedidos y sus variaciones, de auditorías, y de otros que pudieran abrirse.

32.4.- Responsable Jurídico: Responsable de recibir, tramitar, mantener en pleno y eficiente funcionamiento, y resolver todas las solicitudes de ejercicio de los derechos de los titulares de los bancos personales, así como asegurar el respeto y debido ejercicio de estos derechos. Responsable de la implementación, difusión y correcta, debida y oportuna utilización de toda la documentación e información pertinente para la debida protección de los datos personales, tales como documentos para la obtención del consentimiento informado, políticas de privacidad, compromisos de cumplimiento, convenios de transferencia, convenios de tratamiento por encargo, documentos de asignación de equipos y herramientas, cláusulas de confidencialidad, documentos de asignación de archivos, documentos informativos, formatos para el ejercicio de derechos del titular de datos, y otros análogos; tanto de manera física como digital. Responsable de realizar las auditorías y verificaciones periódicas respecto del cumplimiento de las normas legales y la política de protección de datos personales. Asimismo, será el responsable de hacerse cargo de las capacitaciones.

32.5.- Responsables del Tratamiento: Son los jefes de las distintas áreas de las empresas que conforman el Grupo Euromotors quienes tienen a su cargo la responsabilidad de dar el debido tratamiento a los datos personales con los que se cuente con arreglo a Ley.

32.6.- Encargado de Tratamiento: Los definidos en el artículo 27° y 28° de este Código.

En el **Anexo 9** que forma parte integrante del presente Código, se incluye el Manual de Organización y Funciones para la Protección de Datos Personales.

Artículo 33°: Procedimientos

Se cumplirá con los procedimientos respectivos para cumplir de manera debida y con arreglo a Ley con el tratamiento de los datos personales, de accesos y privilegios, otorgamiento y cambios de estos, contraseñas, gestión, control de incidentes, controles y revisiones periódicas de accesos, privilegios y contraseñas; conforme a los formatos que se indican a continuación:

33.1.- **Anexo 10.1:** Políticas o Lineamientos para la protección de datos personales.

33.2.- **Anexo 10.2**: Manual de Seguridad de la Información de los Bancos de Datos Personales.

33.3.- **Anexo 10.3**: Procedimiento de Accesos al Sistema y Recursos Informáticos.

33.4.- **Anexo 10.4:** Procedimiento de Asignación de Privilegios de Acceso.

33.5.- **Anexo 10.5:** Procedimiento de Verificación de Privilegios de Acceso.

33.6.- **Anexo 10.6:** Procedimiento de Acciones Correctivas y Preventivas para la Protección de Datos Personales.

33.7.- **Anexo 10.7:** Procedimiento para la Gestión de Consentimiento.

33.8.- **Anexo 10.8:** Procedimiento de Reproducción o Copias de Datos Personales.

33.9.- **Anexo 10.9:** Procedimiento para Protección de Repositorios Físicos.

33.10.- **Anexo 10.10:** Procedimiento para la Atención de Incidencias.

33.11.- **Anexo 10.11:** Procedimiento de Eliminación de Datos Personales.

33.12.- **Anexo 10.12:** Plan de Sensibilización y Capacitación en Protección de Datos Personales.

33.13.- **Anexo 10.13:** Procedimiento de Auditoría para la Protección de Datos Personales.

33.14.- **Anexo 10.14:** Metodología o Plan de Tratamiento de Riesgos.

33.15.- **Anexo 10.15:** Política de Intercambio de Información Física

33.16.- **Anexo 10.16:** Política de Intercambio de Información por Medios Removibles de Almacenamiento.

33.17.- **Anexo 10.17:** Procedimiento de Seguridad en Sistemas (Acceso, Backups, Ejecución ,etc)

Artículo 34°: Registros

Para todos los efectos en el tratamiento de datos personales, las empresas del Grupo Euromotors deberán llevar los siguientes registros:

34.1.- De ejercicio de derechos ARCO

34.2.- De control de personal con accesos y privilegios, su otorgamiento, variaciones, modificaciones, cancelaciones, accesos realizados, trazabilidad de las interacciones con los datos y su tratamiento.

34.3.- De seguridad e incidentes.

34.4.- De auditorías.

34.5.- De traslado de datos.

34.5.- De realización de copias de respaldo o back up.

34.6.- De capacitaciones.

Artículo 35°: Medidas de seguridad específicas

35.1.- Semestralmente, las empresas del Grupo Euromotors deberán cumplir con realizar una fiscalización y auditoría de control para verificar el cumplimiento de la política de protección de datos personales.

35.2.- Todos los empleados, trabajadores y colaboradores en general de las empresas del Grupo Euromotors, deberán asumir el firme compromiso de cumplimiento de la política de protección de datos personales, para lo cual, deberán suscribir la siguiente documentación, conforme a los formatos adjuntos que sirven de referencia:

35.2.1.- Compromiso de Asignación de Equipos. (**Anexo 11**)

35.2.2.- Cláusula de Confidencialidad. (**Anexo 12**)

35.2.3.- Compromiso de Asignación de Archivo Físico. (**Anexo N° 13**)

35.2.4.- Cláusula de Confidencialidad para Proveedores y Terceros. (**Anexo 14**)

35.3.- En los contratos que suscriban las empresas del Grupo Euromotors con sus proveedores, se deberá procurar incluir una cláusula de protección de datos personales, teniendo como referencia la cláusula que se adjunta como **Anexo 15**.

TITULO IX

EVALUACION Y DIFUSION DEL CODIGO

Artículo 36°: Difusión

Todas las empresas del Grupo Euromotors que se acojan al presente Código de Conducta, deberán cumplir con informar de manera adecuada y efectiva sobre la existencia del mismo, en todos los documentos físicos y virtuales en los que se traten temas sobre protección de datos personales, políticas de privacidad, consentimiento de datos, etc., así como al interior de sus respectivas organizaciones, haciéndolo de conocimiento de todos sus empleados, trabajadores, colaboradores, directivos, apoderados, representantes, colaboradores en general, clientes, proveedores, etc.

Artículo 37°: Control de Aplicación

Todas las empresas del Grupo Euromotors que se acojan al presente Código de Conducta, deberán cumplir con monitorear y evaluar permanentemente el cumplimiento de este y de los formatos y procedimientos que lo conforman y aparecen en los Anexos adjuntos, así como su eficacia e idoneidad para la protección de datos personales y cumplimiento de las normas legales sobre la materia, la satisfacción de los titulares de los datos, y se debida adecuación; ello, a fin de mantenerlo vigente y actualizado a las diversas situaciones y necesidades para la protección de los datos personales de sus titulares, y para asegurar el debido cumplimiento normativo por parte de las mismas empresas de Grupo Euromotors. Las auditorías y fiscalizaciones periódicas de control de seguridad serán los mecanismos adecuados para realizar el control de aplicación de este Código de Conducta, así como para adoptar las medidas de corrección y mejora necesarias, adoptando las medidas técnicas, legales y organizativas a fin de garantizar el cumplimiento efectivo de la normativa que regula y garantiza la protección y debido tratamiento de los datos personales, en cumplimiento del Principio de Responsabilidad Proactiva.

Artículo 38°: Compromiso

Todas las empresas del Grupo Euromotors asumen y se comprometen por el firme compromiso institucional, así como por parte de todas las autoridades, directivos, ejecutivos, trabajadores y personal en general, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndose en una mejora continua y cumplimiento del Principio de Responsabilidad Proactiva. De igual modo, se deberá garantizar el Principio de Transparencia, a fin de que los titulares de los datos personales tengan fácil y debido conocimiento de las condiciones de sus datos personales, así como de los derechos que pueden hacer valer. Asimismo, serán también responsables de fomentar el cumplimiento de la Ley de Protección de Datos Personales, su Reglamento, así como las normas ampliatorias, modificatorias o sustitutorias que se emitan, y del presente Código, así como la difusión de la protección y defensa del derecho a la protección de los datos personales de todo ciudadano.

Para ello, las empresas del Grupo Euromotors implementarán comunicaciones periódicas en su difundiendo el presente Código y la gran importancia de la protección de los datos personales; se entregarán a todos, sea de manera virtual o física, ejemplares del Código de Conducta, haciendo hincapié no solo en su cumplimiento, sino también en la necesidad de su defensa; este Código de Conducta también se publicará en las respectivas páginas web.

Port último, queda establecido que, todo directivo, ejecutivo, empleado, trabajador, colaborador y personal en general, que tenga conocimiento de cualquier afectación al derecho a la protección de los datos personales de cualquier persona al interior de las empresas del Grupo Euromotors, estará obligada a dar parte de ello y ponerlo en conocimiento de su superior y de la gerencia general, a efectos de que adopten las medidas de protección y corrección que correspondan, siendo una falta gravísima para todos los efectos el no hacerlo.

Artículo 39°: Capacitación

Anualmente, las empresas del Grupo Euromotors que adopten el presente Código de Conducta, ya sea manera individual o conjunta, desarrollarán jornadas de capacitación en temas de protección de datos personales, de cumplimiento de la Ley, del presente Código, medidas de prevención, protección del derecho y ejercicio de éstos, y difusión.

Artículo 40°: Oficial de Datos Personales

Las empresas que formen parte del Grupo Euromotors deberán nombrar a un Oficial de Datos Personales, cuyos datos de contacto deberán ser publicados en un lugar visible que permita a los titulares de datos personales conocer los mismos. Igualmente, los datos de contacto del Oficial de Cumplimiento deberán ser informados y actualizados cada vez que sea necesario a la Autoridad de Datos Personales.

El Oficial de Datos Personales se encargará de:

40.1.- Informar y asesorar al titular y responsable del banco de datos personales y a toda la organización, las obligaciones que deben cumplir con arregle a la Ley de Protección de Datos Personales, su Reglamento, y demás normas aplicables, sus modificaciones u otras que se promulguen en el futuro.

40.2.- Verificar e informar sobre el cumplimiento de lo dispuesto en la Ley de Protección de Datos Personales, su Reglamento y demás normas aplicables, así como del cumplimiento de las políticas del titular del banco de datos o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y formación del personal que participa en las operaciones de tratamiento, y las auditorías que se realicen.

40.3.- Brindar la cooperación que corresponda a la Autoridad Nacional de Protección de Datos Personales, y actuar como contacto directo con dicha autoridad para todo lo relacionado al tratamiento de datos personales.

DISPOSICION FINAL

Disposición Final Única – Entrada en Vigor

El presente Código de Conducta entrará en vigor dentro del plazo máximo de 180 días calendario contados a partir del día siguiente de su aprobación por parte del Directorio de la empresa EURO MOTORS S.A., con R.U.C. N° 20168544252, plazo dentro del cual se deberán adoptar las medidas correspondientes para su implementación, aplicación y puesta en práctica.

Para las demás empresas que conforman el Grupo Euromotors que deseen adoptarlo y sujetarse al mismo, este Código de Conducta entrará en vigor dentro del plazo máximo de 180 días calendario contados a partir del día siguiente de su aprobación por parte de los Directorios que lo aprueben, plazo dentro del cual se deberán adoptar las medidas correspondientes para su implementación, aplicación y puesta en práctica. Para los casos de empresa que no cuenten con Directorio, dicha aprobación deberá ser dispuesta por su Gerente General.

ANEXO 1

EMPRESAS QUE CONFORMAN EL GRUPO EUROMOTORS

1.- EURO MOTORS S.A. – R.U.C. N° 20168544252 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 00233196 del Registro de Personas Jurídicas de Lima.

2.- ALTOS ANDES S.A.C. – R.U.C. N° 20296136728 – Av. Tomás Marsano 402-Surquillo-Lima – Partida N° 03007041 del Registro de Personas Jurídicas de Lima.

3.- RENTING S.A.C. – R.U.C. N° 20509031500 – Jr. Domingo Martínez Lujan 1202 - Surquillo-Lima – Partida N° 11667075 del Registro de Personas Jurídicas de Lima.

4.- EUROSHOP S.A., R.U.C. N° 20349065488 – Av. Domingo Orué 989-Surquillo-Lima – Partida N° 03020437 del Registro de Personas Jurídicas de Lima.

5.- SAN BARTOLOME S.A., R.U.C. N° 20125327509 – Av. 1ero. de Mayo 559-Urb. El Puente-El Agustino-Lima – Partida N° 00364037 del Registro de Personas Jurídicas de Lima.

6.- EURO CAMIONES S.A., R.U.C. N° 20550808791 – Av. Los Cipreses 420-Urb. Los Ficus-Santa Anita-Lima – Partida N° 12947841 del Registro de Personas Jurídicas de Lima.

7.- EUROLIFT S.A., R.U.C. N° 20536982559 – Av. República de Argentina 2165-Lima-Lima – Partida N° 12540250 del Registro de Personas Jurídicas de Lima.

8.- EUROINMUEBLES S.A.C., R.U.C. N° 20549632204 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 12907303 del Registro de Personas Jurídicas de Lima.

9.- 1 ONE S.A.C., R.U.C. N° 20520549740 – Av. Tomás Marsano 432-Surquillo-Lima – Partida N° 12225562 del Registro de Personas Jurídicas de Lima.

10.- EUROCONNECT S.A.C., R.U.C. N° 20605166793 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 14348700 del Registro de Personas Jurídicas de Lima.

11.- INTERNATIONAL CAMIONES DEL PERU S.A., R.U.C. N° 20600045521 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 13209869 del Registro de Personas Jurídicas de Lima.

12.- REVO MOTORS S.A., R.U.C. N° 20600137272 – Av. Tomás Marsano 402-Surquillo-Lima – Partida N° 13366991 del Registro de Personas Jurídicas de Lima.

13.- T1 S.A.C., con R.U.C. N° 20612019470 – Jr. Catalino Miranda 278 – Barranco – Lima – Partida N° 15509068 del Registro de Personas Jurídicas de Lima.

ANEXO 2.1

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES – CLIENTES Y PROSPECTOS

En cumplimiento de la Ley de Protección de Datos Personales, quien suscribe, otorga consentimiento voluntario, libre, previo, expreso, informado e inequívoco a **_____**, con R.U.C. N° _____, y con domicilio en la _____ – _____ – Lima – Perú, para que realice por plazo indefinido, el tratamiento, en cualquiera de sus modalidades, medios o soportes, local o transfronterizo, de los datos personales que haya podido proporcionar, incluyendo nombres, apellidos, datos de identificación, perfiles, dirección, números telefónicos, correos electrónicos, imagen y/o voz, cualidades, información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales, características e información de vehículos, incidencias de servicio, comportamiento del conductor y del vehículo, estilo de manejo, ajustes de confort, data del sistema de entretenimiento, de navegación y de usos e incidentes del vehículo, recorrido, placas, récord de servicios y reportes de necesidad de servicios, recorridos, estado del vehículo, y todo aquello que registren los módulos informáticos de a bordo de estos y aquella que se almacene en las llaves, incluyendo los videos, imágenes y audio; información de citas, facturación y reclamos por los servicios prestados; artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, encuestas, preferencias e intereses, datos económicos y de seguros, y relaciones sociales; para ser utilizados para fines administrativos, comerciales, de publicidad, de segmentación, estadísticos, elaboración y manejo de perfiles automatizados o no de cualquier tipo de dato personal, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; pudiendo formar también parte estos datos de las campañas, avisos, difusiones y publicaciones que haga el receptor de los datos. Los datos podrán ser objeto de decisiones y tratamientos por medios tecnológicos, automatizados o no, con o sin intervención humana, incluida la elaboración de perfiles, para las finalidades por las cuales se otorga el presente consentimiento. Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos.

El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones contractuales, tratativas o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento. Con el objeto de poder asegurar un debido y oportuno servicio técnico, soporte de postventa, y para mantener el uso y disfrute de todas las funcionalidades, beneficios y prestaciones que a nivel mundial ofrece la marca del vehículo del titular de los datos personales, y siendo obligación contractual asegurar que todos los usuarios de dicha marca puedan acceder a ello, se informa al titular que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte por ser usuario de dicha marca de vehículo, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, incluyendo el tratamiento compartido con el fabricante, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales, incluyendo para ello las transferencias de datos, a nivel nacional e internacional que sean necesarias.

Los datos serán tratarlos con veracidad, calidad y proporcionalidad; la negativa a otorgarlos impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, a la portabilidad de sus datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a **_____**@**_____**, haciendo precisión de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es **_____**, y su destino será el mismo Banco de Datos, sin perjuicio de la autorización expresa de flujo nacional e internacional que también se otorga. En tal sentido, el otorgante autoriza y presta su consentimiento previo, expreso, libre e informado, para que se compartan sus datos personales o se realice tratamiento compartido mediante la transferencia y/o encargo de tratamiento, local y/o transfronterizo con las empresas que conforman el grupo **EUROMOTORS** al cual pertenece y se rigen bajo el Código de Conducta que se puede consultar en www.euromotors.com.pe; así como también, con las personas y entidades que se lista en el siguiente enlace _____. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para las mismas finalidades y destino regulado en el presente documento, y para cumplir con el encargo efectuado, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Finalmente, se ratifica el compromiso institucional, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua. Consulte nuestra Política de Privacidad en _____. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

Firmado en la fecha	:	Dirección	:
Nombre del Cliente	:	Teléfonos (Fijo/Cel)	:
Documento de Identidad	:	Correo electrónico	:
Firma del Cliente	:		

ANEXO 2.2

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES – CLIENTES Y PROSPECTOS

En cumplimiento de la Ley de Protección de Datos Personales y su Reglamento, quien suscribe, otorga consentimiento voluntario, libre, previo, expreso, informado e inequívoco a **_____**, con R.U.C. N° _____, y con domicilio en _____ – _____ – Lima – Perú, para que realice por plazo indefinido, el tratamiento los datos personales proporcionados, para ser utilizados para fines administrativos, comerciales, de publicidad, de segmentación, estadísticos, elaboración y manejo de perfiles automatizados o no de cualquier tipo de dato personal, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; pudiendo formar también parte estos datos de las campañas, avisos, difusiones y publicaciones que haga el receptor de los datos. Los datos podrán ser objeto de decisiones y tratamientos por medios tecnológicos, automatizados o no, con o sin intervención humana, incluida la elaboración de perfiles, para las finalidades por las cuales se otorga el presente consentimiento.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad y responsabilidad **_____**, y el destino de los datos será el mismo Banco, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose de manera expresa las medidas de seguridad técnica, organizativa y legal para el tratamiento, y confidencialidad.

El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones contractuales, tratativas o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento.

Los datos otorgados serán tratados con veracidad, calidad y proporcionalidad; la negativa a otorgar dichos datos personales impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de ejercer los derechos ARCO (acceso, a la portabilidad de sus datos, información, actualización, inclusión, rectificación, supresión, cancelación, oposición, revocación, denegación, o reclamaciones) enviando una comunicación escrita al domicilio indicada al inicio de este documento, o un correo electrónico a _____@_____. Asimismo, podrá consultar nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe. Consulte nuestra Política de Privacidad en _____. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

ANEXO 2.3

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES – COLABORADORES Y TERCEROS EN GENERAL

En cumplimiento de la Ley de Protección de Datos Personales, quien suscribe, otorga consentimiento voluntario, libre, previo, expreso, informado e inequívoco a **_____**, con R.U.C. N° _____, y con domicilio en la _____ – _____ – Lima – Perú, para que realice por plazo indefinido, el tratamiento, en cualquiera de sus modalidades, medios o soportes, local o transfronterizo, de los datos personales que haya podido proporcionar, incluyendo nombres, apellidos, datos de identificación, perfiles, dirección, números telefónicos, correos electrónicos, imagen y/o voz, cualidades, información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales, características e información de vehículos, incidencias de servicio, comportamiento del conductor y del vehículo, estilo de manejo, ajustes de confort, data del sistema de entretenimiento, de navegación y de usos e incidentes del vehículo, recorrido, placas, récord de servicios y reportes de necesidad de servicios, recorridos, estado del vehículo, y todo aquello que registren los módulos informáticos de a bordo de estos y aquella que se almacene en las llaves, incluyendo los videos, imágenes y audio; información de citas, facturación y reclamos por los servicios prestados; artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, encuestas, preferencias e intereses, datos económicos y de seguros, relaciones sociales, laborales, contractuales , profesionales; para ser utilizados para fines administrativos, laborales, contractuales, de locación de servicios, obligacionales, comerciales, de publicidad, de segmentación, estadísticos, elaboración y manejo de perfiles automatizados o no de cualquier tipo de dato personal, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; pudiendo formar también parte estos datos de las campañas, avisos, difusiones y publicaciones que haga el receptor de los datos. Los datos podrán ser objeto de decisiones y tratamientos por medios tecnológicos, automatizados o no, con o sin intervención humana, incluida la elaboración de perfiles, para las finalidades por las cuales se otorga el presente consentimiento.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos.

El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones contractuales, laborales, de locación de servicios, tratativas o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento.

Los datos serán tratarlos con veracidad, calidad y proporcionalidad; la negativa a otorgarlos impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, a la portabilidad de sus datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a **_____@_____**, haciendo precisión de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es **_____**, y su destino será el mismo Banco de Datos, sin perjuicio de la autorización expresa de flujo nacional e internacional que también se otorga. En tal sentido, el otorgante autoriza y presta su consentimiento previo, expreso, libre e informado, para que se compartan sus datos personales o se realice tratamiento compartido mediante la transferencia y/o encargo de tratamiento, local y/o transfronterizo con las empresas que conforman el grupo **EUROMOTORS** al cual pertenece y se rigen bajo el Código de Conducta que se puede consultar en www.euromotors.com.pe; así como también, con las personas y entidades que se lista en el siguiente enlace _____. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para las mismas finalidades y destino regulado en el presente documento, y para cumplir con el encargo efectuado, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Finalmente, se ratifica el compromiso institucional, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua. Consulte nuestra Política de Privacidad en _____. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

Firmado en la fecha	:	Dirección	:
Nombre del Cliente	:	Teléfonos (Fijo/Cel)	:
Documento de Identidad	:	Correo electrónico	:
Firma del Cliente	:		

ANEXO 3
POLITICA DE PRIVACIDAD GENERAL – PROTECCION DE DATOS PERSONALES

Política General

En cumplimiento de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, **_____**, con R.U.C. N° _____, y con domicilio en _____ – _____ – Lima – Perú, asegura y garantiza que, todo y cualquier dato personal que haya recopilado de manera legítima y con arreglo a ley, será tratado única y exclusivamente para cumplir con la finalidad para lo cual haya sido otorgado según consentimiento libre, previo, expreso, informado e inequívoco, y en los casos permitidos por ley cuyo tratamiento no requiere de consentimiento previo, para cumplir con las finalidades respectivas en ese sentido, tales como, uso de datos de acceso público, uso de datos para la preparación, celebración y ejecución de relaciones contractuales o profesionales necesarias para su desarrollo o cumplimiento, para fines de cumplimiento de las normas contra el lavado de activos y el financiamiento del terrorismo, por mandato legal, por orden de autoridad en ejercicio de sus funciones expresamente establecidas por ley, entre otras que legalmente estén establecidas. De esta manera, con el objeto de poder asegurar un debido y oportuno servicio técnico, soporte de postventa, cumplimiento de garantías ofrecidas, así como para mantener el uso y disfrute de todas las funcionalidades, beneficios y prestaciones que a nivel mundial ofrece la marca del vehículo adquirido por el titular de los datos personales, y siendo obligación contractual asegurar que todos los usuarios de dicha marca puedan acceder a ello, se informa al titular que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte por ser usuario de la marca del vehículo adquirido, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, incluyendo el tratamiento compartido con el fabricante, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales. En virtud de dicha excepción, entre otros casos debidamente justificados y amparados por la misma Ley, los datos podrían ser comunicados o tratarse de modo compartido o transferidos o tratados por encargo de modo local y/o transfronterizo, con las personas y entidades que se lista en el siguiente enlace _____, y demás entidades privadas y públicas necesarias para el cumplimiento de las relaciones contractuales sostenidas. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para el cumplimiento de las finalidades contractuales y demás excepciones reguladas por ley por las que no se requiera consentimiento, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, que es automatizado y no automatizado, garantizándose de manera expresa las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos de carácter personal facilitados por sus clientes. Seguridad y confidencialidad que se asegura igualmente para la transferencia y/o flujo transfronterizo de los mismos, cuando ello haya sido autorizado por su titular. Los datos se conservarán por plazo indefinido.

Se informa a los titulares de los datos personales que no están obligados a otorgarlos, siendo ello algo de carácter facultativo, a excepción de aquellos datos de identificación personal destinados y necesarios para la ejecución de las relaciones contractuales que pueda sostener, y demás que por mandato legal no se requiere consentimiento de acuerdo a ley. Todo tratamiento de datos personales será efectuado con veracidad, calidad y proporcionalidad para las finalidades antes indicadas y para la ejecución de las relaciones contractuales, y demás permitidas por ley; la negativa a otorgar dichos datos personales impedirá su tratamiento.

Todo titular de datos personales tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, a la portabilidad de sus datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a la dirección _____@_____, haciendo la precisión clara y expresa de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es **_____**, por lo que el destino de los datos será el mismo Banco de Datos y para que ésta los pueda tratar conforme a lo autorizado, para los fines específicos antes indicados, todo con arreglo a ley. En tal sentido, se garantiza la absoluta confidencialidad, privacidad y protección de los datos personales

que se formen parte del Banco de Datos, así como la idoneidad de su tratamiento, siendo que la información permanecerá protegida y segura, y no será compartida, transferida ni divulgada, salvo que se cuente con permiso expreso de su titular, o sea necesaria para la ejecución de las relaciones contractuales que pueda sostener, y demás que por mandato legal no se requiera consentimiento.

Finalmente, se deja expresa constancia del firme compromiso institucional, así como por parte de todas las autoridades, directivos, ejecutivos, trabajadores y personal en general, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua.
Para más información consulte nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

Nuestro Compromiso con la Privacidad.
La privacidad de nuestros usuarios es importante para nosotros. Para protegerla mejor, adoptamos esta Política de Privacidad, la cual contiene nuestras prácticas de intercambio de información por internet y las decisiones que el aceptante puede tomar en relación con la manera en que se obtiene y utiliza la información. Para facilitar la localización de esta Política de Privacidad, la colocamos a disposición en nuestra página de inicio y en todo punto donde se puedan solicitar datos de identificación personal.

El usuario puede registrarse en nuestro sitio web de manera voluntaria, si desea recibir nuestros catálogos y actualizaciones sobre nuestros nuevos productos y servicios. Podemos usar información conjunta, que no permite la identificación del titular, para diseñar mejor nuestro sitio web y compartir con nuestras agencias de publicidad. Por ejemplo, podemos informar a una agencia de publicidad que una cantidad de usuarios visitaron cierta zona de nuestro sitio web, que una cantidad de hombres y una cantidad de mujeres completaron nuestro formulario de inscripción, pero no divulgaremos nada que pudiera usarse para identificar personalmente a las personas.
Si el usuario elige inscribirse para que el envío de productos o materiales, o entregarnos de otro modo información personal, almacenaremos toda esa información personal o parte de ella y podríamos usarla con fines de promoción o para investigación de mercadeo, lo cual puede incluir compartirla. Nunca comercializaremos información personal a ninguna otra compañía. Tampoco usaremos ni compartiremos la información personalmente identificable que el usuario nos brinde, de formas que no tengan relación con la autorización brindada. En el caso de una investigación penal o de una presunta actividad delictiva, las autoridades competentes pueden exigirnos que compartamos cierta información personal.
La aceptación de los presentes términos y condiciones constituye el consentimiento previo, informado, expreso e inequívoco, para la recepción de promociones de productos y servicios a través de servicios de telemercadeo, centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos, en los términos del Código de Defensa y Protección del Consumidor. Este consentimiento podrá ser revocado, en cualquier momento, enviando una comunicación escrita simple vía correo electrónico a la dirección _____@_____, haciendo la precisión clara y expresa de la revocación del consentimiento, el cual será procesado dentro de plazos razonables.

Acerca de las "Cookies".
Las "cookies" son pequeños elementos de datos que algunos sitios web escriben en el disco duro del dispositivo del usuario cuando visita sus sitios o guarda la dirección en el navegador. Estos archivos de datos contienen información que el sitio puede usar para organizar las páginas visitadas en un sitio web particular. Es posible que algunos de nuestros sitios web usen tecnología de "cookies" para medir la actividad del sitio y personalizar la información a fin de que se adapte a los intereses personales del usuario, lo que nos permite brindarle información personalizada que se adapte a sus intereses la próxima vez que visite nuestro sitio. Por lo tanto, el uso que hacemos de la tecnología de "cookies" es para brindar información más individualizada y una experiencia de visualización óptima.

Pixel Tags.
Es posible que usemos "pixel tags", es decir, pequeños archivos gráficos que nos permiten monitorear el uso de nuestros sitios web. Un pixel tag puede reunir información tal como la dirección IP (Protocolo de Internet) de la computadora que descargó la página en la cual aparece el pixel tag, el URL (Localizador Uniforme de Recursos) de la página en la que aparece el pixel tag, el horario en que se visitó la página que contiene el pixel tag, el tipo de navegador que captó el pixel tag y el número de identificación de cualquier cookie (consulta Acerca de las "cookies") en el dispositivo previamente colocado por ese servidor. Cuando intercambiamos correspondencia con el usuario mediante e-mails que admiten HTML, podemos usar tecnología de detección de formato, que permite que los pixel tags nos informen la recepción y apertura de nuestro e-mail.

Nuestro Compromiso con la Privacidad de los Niños.
Proteger la privacidad de los más jóvenes es sumamente importante. Por ese motivo ninguna parte de nuestro sitio web está estructurada como para atraer a menores de 14 años.

Consentimiento de Tratamiento de Datos Personales
En cumplimiento de la Ley de Protección de Datos Personales, quien suscribe, otorga consentimiento voluntario, libre, previo, expreso, informado e inequívoco a _____, con R.U.C. N° _____, y con domicilio en la _____ – _____ – Lima – Perú, para que realice por plazo indefinido, el tratamiento, en cualquiera de sus modalidades, medios o soportes, local o transfronterizo, de los datos personales que haya podido proporcionar, incluyendo nombres, apellidos, datos de identificación, perfiles, dirección, números telefónicos, correos electrónicos, imagen y/o voz, cualidades, información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales, características e información de vehículos, incidencias de servicio, comportamiento del conductor y del vehículo, estilo de manejo, ajustes de confort, data del sistema de entretenimiento, de navegación y de usos e incidentes del vehículo, recorrido, placas, récord de servicios y reportes de necesidad de servicios, recorridos, estado del vehículo, y todo aquello que registren los módulos informáticos de a bordo de estos y aquella que se almacene en las llaves, incluyendo los videos, imágenes y audio; información de citas, facturación y reclamos por los servicios prestados; artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, encuestas, preferencias e intereses, datos económicos y de seguros, y relaciones sociales; para ser utilizados para fines administrativos, comerciales, de publicidad, de segmentación, estadísticos, elaboración y manejo de perfiles automatizados o no de cualquier tipo de dato personal, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; pudiendo formar también parte estos datos de las campañas, avisos, difusiones y publicaciones que haga el receptor de los datos. Los datos podrán ser objeto de decisiones y tratamientos por medios tecnológicos, automatizados o no, con o sin intervención humana, incluida la elaboración de perfiles, para las finalidades por las cuales se otorga el presente consentimiento. Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad _____, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos.
El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones contractuales, tratativas o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento. Con el objeto de poder asegurar un debido y oportuno servicio técnico, soporte de postventa, y para mantener el uso y disfrute de todas las funcionalidades, beneficios y prestaciones que a nivel mundial ofrece la marca del vehículo del titular de los datos personales, y siendo obligación contractual asegurar que todos los usuarios de dicha marca puedan acceder a ello, se informa al titular que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte por ser usuario de dicha marca de vehículo, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, incluyendo el tratamiento compartido con el fabricante, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales, incluyendo para ello las transferencias de datos, a nivel nacional e internacional que sean necesarias.
Los datos serán tratarlos con veracidad, calidad y proporcionalidad; la negativa a otorgarlos impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, a la portabilidad de sus datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a _____@_____, haciendo precisión de su pedido, el cual será atendido dentro del plazo de ley.
El responsable de este Banco de Datos es _____, y su destino será el mismo Banco de Datos, sin perjuicio de la autorización expresa de flujo nacional e internacional que también se otorga. En tal sentido, el otorgante autoriza y presta su consentimiento previo, expreso, libre e informado, para que se compartan sus datos personales o se realice tratamiento compartido mediante la transferencia y/o encargo de tratamiento, local y/o transfronterizo con las

empresas que conforman el grupo **EUROMOTORS** al cual pertenece y se rigen bajo el Código de Conducta que se puede consultar en www.euromotors.com.pe; así como también, con las personas y entidades que se lista en el siguiente enlace _____. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para las mismas finalidades y destino regulado en el presente documento, y para cumplir con el encargo efectuado, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Finalmente, se ratifica el compromiso institucional, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua. Consulte nuestra Política de Privacidad en _____. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

ANEXO 4.1
POLITICA DE PRIVACIDAD GENERAL – PROTECCION DE DATOS PERSONALES

En cumplimiento de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, **_____**, con R.U.C. N° _____, y con domicilio en _____ – _____ – Lima – Perú, asegura y garantiza que, todo y cualquier dato personal que haya recopilado de manera legítima y con arreglo a ley, será tratado única y exclusivamente para cumplir con la finalidad para lo cual haya sido otorgado según consentimiento libre, previo, expreso, informado e inequívoco, y en los casos permitidos por ley cuyo tratamiento no requiere de consentimiento previo, para cumplir con las finalidades respectivas en ese sentido, tales como, uso de datos de acceso público, uso de datos para la preparación, celebración y ejecución de relaciones contractuales o profesionales necesarias para su desarrollo o cumplimiento, para fines de cumplimiento de las normas contra el lavado de activos y el financiamiento del terrorismo, por mandato legal, por orden de autoridad en ejercicio de sus funciones expresamente establecidas por ley, entre otras que legalmente estén establecidas. De esta manera, con el objeto de poder asegurar un debido y oportuno servicio técnico, soporte de postventa, cumplimiento de garantías ofrecidas, así como para mantener el uso y disfrute de todas las funcionalidades, beneficios y prestaciones que a nivel mundial ofrece la marca del vehículo adquirido por el titular de los datos personales, y siendo obligación contractual asegurar que todos los usuarios de dicha marca puedan acceder a ello, se informa al titular que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte por ser usuario de la marca del vehículo adquirido, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, incluyendo el tratamiento compartido con el fabricante, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales. En virtud de dicha excepción, entre otros casos debidamente justificados y amparados por la misma Ley, los datos podrían ser comunicados o tratarse de modo compartido o transferidos o tratados por encargo de modo local y/o transfronterizo, con las personas y entidades que se lista en el siguiente enlace _____, y demás entidades privadas y públicas necesarias para el cumplimiento de las relaciones contractuales sostenidas. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para el cumplimiento de las finalidades contractuales y demás excepciones reguladas por ley por las que no se requiera consentimiento, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, que es automatizado y no automatizado, garantizándose de manera expresa las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos de carácter personal facilitados por sus clientes. Seguridad y confidencialidad que se asegura igualmente para la transferencia y/o flujo transfronterizo de los mismos, cuando ello haya sido autorizado por su titular. Los datos se conservarán por plazo indefinido.

Se informa a los titulares de los datos personales que no están obligados a otorgarlos, siendo ello algo de carácter facultativo, a excepción de aquellos datos de identificación personal destinados y necesarios para la ejecución de las relaciones contractuales que pueda sostener, y demás que por mandato legal no se requiere consentimiento de acuerdo a ley. Todo tratamiento de datos personales será efectuado con veracidad, calidad y proporcionalidad para las finalidades antes indicadas y para la ejecución de las relaciones contractuales, y demás permitidas por ley; la negativa a otorgar dichos datos personales impedirá su tratamiento.

Todo titular de datos personales tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, a la portabilidad de sus datos, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a la dirección **_____@_____**, haciendo la precisión clara y expresa de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es **_____**, por lo que el destino de los datos será el mismo Banco de Datos y para que ésta los pueda tratar conforme a lo autorizado, para los fines específicos antes indicados, todo con arreglo a ley. En tal sentido, se garantiza la absoluta confidencialidad, privacidad y protección de los datos personales que se formen parte del Banco de Datos, así como la idoneidad de su tratamiento, siendo que la información permanecerá protegida y segura, y no será compartida, transferida ni divulgada, salvo que se cuente con permiso expreso de su titular, o sea necesaria para la ejecución de las relaciones contractuales que pueda sostener, y demás que por mandato legal no se requiera consentimiento.

Finalmente, se deja expresa constancia del firme compromiso institucional, así como por parte de todas las autoridades, directivos, ejecutivos, trabajadores y personal en general, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua.
Para más información consulte nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

ANEXO 4.2
PROTECCION DE DATOS PERSONALES - MAILING

En cumplimiento de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, **_____**, con R.U.C. N° _____, y con domicilio en _____ – _____ – Lima – Perú, asegura y garantiza que, todo y cualquier dato personal que haya recopilado de manera legítima y con arreglo a ley, será tratado única y exclusivamente para cumplir con la finalidad para lo cual haya sido otorgado según consentimiento libre, previo, expreso, informado e inequívoco, y en los casos permitidos por ley cuyo tratamiento no requiere de consentimiento previo, para cumplir con las finalidades respectivas en ese sentido, tales como, uso de datos de acceso público, uso de datos para la preparación, celebración y ejecución de relaciones contractuales o profesionales necesarias para su desarrollo o cumplimiento, para fines de cumplimiento de las normas contra el lavado de activos y el financiamiento del terrorismo, por mandato legal, por orden de autoridad en ejercicio de sus funciones expresamente establecidas por ley, entre otras que legalmente estén establecidas.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad de **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, siendo éste el responsable y el destino de los datos será el mismo Banco de Datos. Se garantiza de manera expresa las medidas de seguridad técnica, organizativa y legal para el tratamiento, así como su confidencialidad. Todo tratamiento de datos personales será efectuado con veracidad, calidad y proporcionalidad. Para el ejercicio de sus derechos ARCO (acceso, a la portabilidad de sus datos, información, actualización, inclusión, rectificación, supresión, cancelación, oposición, revocación, denegación, o reclamaciones), contacte a **_____@_____**. Para más información consulte nuestra Política de Privacidad en _____. Asimismo podrá consultar nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe. Consulte nuestra Política de Privacidad en _____. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

ANEXO 4.3

CONDICIONES DE USO DE PLATAFORMAS VIRTUALES Y DIGITALES

Al hacer uso de aquellos servicios de comunicación y consulta que prestamos de manera virtual y a través de nuestras plataformas digitales, tales como mensajería de texto, correo electrónico, salones de conversación (Chat), mensajes a través de aplicaciones como WhatsApp, mensajes celulares, contacto web, y otros digitales y/o virtuales análogos, está aceptando las condiciones que se describen a continuación, así como nuestra política de privacidad, las cuales el usuario se obliga a respetar y cumplir.

Los servicios y contactos digitales que brindamos están a cargo de nuestra empresa, _____, con R.U.C. N° _____, con domicilio _____, y se sujetan a las siguientes condiciones de uso:

1.- Nuestros servicios digitales son prestados mediante fuertes condiciones de seguridad y privacidad, protegiendo en todo momento los datos que nos proporciones en un ambiente libre de intrusiones y fugas de información.

2.- Los servicios que prestamos en nuestras plataformas digitales están destinados a tomar contacto virtual para atender pedidos de información, solicitudes y consultas respecto de nuestros productos y servicios.

3.- Se deja expresa constancia que nuestros únicos canales de comunicación virtual son a través de nuestro correo de atención al cliente _____@_____, nuestro chat web www._____, y nuestro número de contacto WhatsApp _____. Todos ellos verifican su autenticidad haciendo uso del logo de nuestra empresa y/o marca, y únicamente a través de dichos contactos. Nuestra empresa no asume ningún tipo de responsabilidad si el usuario comparte o brinda sus datos personales a otra persona o entidad fuera de los canales de atención oficiales de nuestra marca.

4.- Los datos que nos proporciones para tomar contacto con nosotros a través de las plataformas digitales que disponemos, serán conservados en un base de datos de clientes y/o prospectos de clientes, la cual será tratada de conformidad con nuestra política de privacidad que podrás consultar en www._____, con la finalidad de atender única y exclusivamente los pedidos, consultas, requerimientos y demás tratativas que tengamos contigo de acuerdo con el contacto que tengas con nosotros. Tus datos no podrán ser utilizados para otra finalidad, a menos que, en caso quieras disfrutar de un contacto más cercano, ayudarnos a mejorar y estar enterado de nuestras novedades, podrás también autorizarnos a tratar tus datos para otras finalidades, aceptando el formato de Consentimiento de Datos Personales que podrás consultar y analizar a detalle en www._____.

5.- Los datos que recopilamos y que te solicitamos completes para tomar contacto con nosotros son esenciales e indispensables para poder atenderte y brindar nuestros servicios, y si no nos los dan, no podremos atenderte. Sin perjuicio de la información inicial solicitada, tales como nombre, D.N.I. o C.E. o pasaporte, domicilio, teléfono y correo electrónico, al tomar contacto con nosotros te podríamos solicitar mayores datos e información para brindarte la atención que solicitas.

6.- Para hacer contacto con nosotros y solicitarnos la información que necesitas o realizar cualquier otro pedido o consulta, deberás ser mayor de edad (mayor de 18 años), y llenar los campos de información y contacto con los datos que te son requeridos. La información que nos proporciones deberá ser verdadera y fidedigna, y deberá ser mantenida actualizada, siendo que tú asumes la responsabilidad íntegra sobre ello; en tal sentido, nuestra empresa no asume ningún tipo de responsabilidad por el ingreso de información o datos falsos, inexactos, incompletos o indebidos, ni de las consecuencias que ello pueda generar. En tal sentido, todas las interacciones realizadas por los usuarios a través de nuestras plataformas de atención digital se presumen en todos los casos realizados por sus mismos titulares y bajo su responsabilidad. Sin perjuicio de ello, nuestra empresa podrá realizar validaciones de identidad y controles de seguridad para un mejor servicio.

7.- Nuestra empresa no asume ninguna responsabilidad por la utilización por parte de los usuarios de dispositivos o redes no seguras que puedan ser objeto de intervenciones externas o virus, o por extracción no autorizada de su información, ni por acciones que puedan derivar en dichas consecuencias.

8.- La información y conversaciones que sostengas con nosotros a través de nuestras plataformas digitales de contacto, podrán ser guardadas como respaldo de la atención y comunicación brindada a tus solicitades e interrelaciones por ello, y como antecedentes de tales contactos.

9.- En caso de uso indebido de los canales y plataformas digitales de contacto, o detectar conductas fraudulentas, ilegales, inaceptables, que atenten contra la seguridad y privacidad o los derechos de cualquier persona, sean obscenas, difamatorias, amenazantes, que suplanten la identidad de otras personas, o que resulten indebidas bajo cualquier concepto, o que atenten contra la moral o las buenas costumbres, serás eliminado de nuestra red de contactos, tu contacto con nosotros será cancelado, no podrás hacer uso de nuestros servicios, y serás reportado a las autoridades competentes.

10.-No asumimos ningún tipo de responsabilidad en caso nuestros sistemas digitales presenten cualquier tipo de malfuncionamiento o error. En caso suceda, haremos nuestro mayor esfuerzo por solucionarlo; sin embargo, cualquier retardo o falta de comunicación por estos desperfectos no nos será imputable, y no asumimos ninguna responsabilidad por sus consecuencias.

11.- Se deja sentado que los servicios de contacto e información digital a través de nuestras plataformas o modalidades de contacto digital podrían cambiar, ser modificadas, mejoradas, ser interrumpidos o suspendidos total o parcialmente, canceladas o desactivadas total o temporalmente, en cualquier momento y sin previo aviso, sin que ello genere ningún tipo de responsabilidad para nuestra empresa.

12.- Las presentes condiciones de uso podrán ser ampliadas y modificadas en cualquier momento, por lo que, para continuar haciendo uso de nuestros servicios, se entiende que, al hacerlo, estarás aceptando las nuevas condiciones.

ANEXO 5

Área Videovigilada

LO ESTAMOS FILMANDO POR MOTIVOS DE SEGURIDAD
LEY DE PROTECCIÓN DE DATOS PERSONALES N°29733

_____, con R.U.C. N° _____, con domicilio en _____ – _____ – Lima – Perú, asegura y garantiza el respeto de sus derechos y datos personales. El ingreso a nuestro establecimiento implica su aceptación a que sea filmado por motivos de seguridad. Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad de **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, siendo éste el responsable y el destino de los datos será el mismo Banco de Datos. Se garantiza de manera expresa las medidas de seguridad técnica, organizativa y legal para el tratamiento, así como su confidencialidad. Todo tratamiento de datos personales será efectuado con veracidad, calidad y proporcionalidad. Para el ejercicio de sus derechos ARCO (acceso, a la portabilidad de los datos, información, actualización, inclusión, rectificación, supresión, cancelación, oposición, revocación, denegación, o reclamaciones), contacte a **_____@_____**. Para más información consulte nuestra Política de Privacidad en _____. Asimismo podrá consultar nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe. Consulte los datos de contacto de nuestro Oficial de Datos Personales en _____.

ANEXO 6.1

FORMATO PARA EL EJERCICIO DE DERECHOS ARCO

_____, con RUC N° _____, con domicilio en _____ – _____ – Lima – Perú, en cumplimiento de lo dispuesto por la Ley de Protección de Datos Personales y su Reglamento, se pone a su disposición a fin de que pueda ejercer los derechos que la Ley le confiere para la protección de sus datos personales contenidos en los bancos de datos de nuestra titularidad. Con el objeto de poder servirlo de la mejor manera, le rogamos completar los campos que a continuación se precisan:

DATOS DEL TITULAR DE LOS DATOS PERSONALES QUE EJERCE EL DERECHO

Nombre Completo :

Documento de Identidad :

Domicilio :

Correo electrónico :

DATOS DEL REPRESENTANTE DEL TITULAR DE LOS DATOS PERSONALES QUE EJERCE EL DERECHO -de corresponder-

Nombre del Representante :

Documento de Identidad del Representante :

Domicilio del Representante :

Correo electrónico del Representante :

DIRECCION PARA LAS NOTIFIACIONES

Domicilio Procesal -puede ser electrónico- :

DERECHO QUE ES EJERCIDO

-marcar la opción correspondiente-

* ACCESO: con el objeto de obtener información sobre sus propios datos personales y su tratamiento, así como a su portabilidad.

* RECTIFICACIÓN: con el objeto de actualizar sus datos, corregirlos o rectificarlos, y/o incluir información, mediante el sustento respectivo.

* CANCELACIÓN: con el objeto de suprimir y cancelar datos del banco cuando su tratamiento ya no sea necesario o pertinente, o cuando haya revocado el consentimiento otorgado.

* OPOSICIÓN: con el objeto de impedir el tratamiento de datos personales o cese de éste, cuando el titular no hubiere prestado su consentimiento o cuando acredite justificación para ello.

DETERMINACIÓN CONCRETA DEL PETITORIO Y DEL DERECHO QUE SE EJERCE.

-describa brevemente su pedido y susténtelo-

_____

_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

ANEXOS Y EVIDENCIAS

-adjunte los documentos que sustenten su solicitud-

1.- Documento de Identidad

2.- Documento de Identidad del Representante -de ser el caso-

3.- Poder del Representante -de ser el caso-

4.- Documentos que sustenten su solicitud:

4.1.- _____

4.2.- _____

4.3.- _____

4.4.- _____

4.5.- _____

Mientras dure el procedimiento de ejercicio de los derechos de actualización, inclusión, rectificación o supresión de datos personales, se dispone el bloqueo de los datos.

Recibida la solicitud de ejercicio de derechos por parte del titular de datos personales, en un plazo máximo de cinco días hábiles será calificada; en caso la misma no cumpla con los requisitos, se le notificará, dentro de estos mismos cinco días hábiles, las observaciones que requieran subsanación, para que cumpla con ello en un plazo máximo de cinco días hábiles adicionales; en caso no se cumpla con la observación, su solicitud se tendrá por no presentada.

En el caso que la información o documentación presentada en su solicitud sea insuficiente o equivocada, e impida darle trámite, se le requerirá dentro de los siete días hábiles siguientes de recibida su solicitud, la documentación e información adicional o correcta; usted tendrá diez días hábiles para atender dicho requerimiento, caso contrario, se tendrá por no presentada su solicitud.

Si su solicitud cumple con todos los requisitos, los plazos de atención y repuesta serán los siguientes, computados a partir del día siguientes de la fecha de presentación:

* Ocho días ante el ejercicio del derecho de información.

* Veinte días ante el ejercicio del derecho de acceso.

* Diez días ante el ejercicio de los otros derechos como los de actualización, rectificación, cancelación, supresión, inclusión u oposición.

Para el caso de solicitudes observadas, los plazos antes indicados se computarán a partir del día siguiente de la presentación de la subsanación correspondiente.

Con excepción al cumplimiento del plazo fijado para la atención ante el ejercicio del derecho de información, los demás plazos correspondientes a la atención de los demás derechos podrán ser objeto de ampliación por una sola vez, y por un plazo igual.

Para mayor información podrá consultar nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe.

Firma :

Lugar y fecha :

Nombres :

Documento de Identidad :

ANEXO 6.2

DOCUMENTO DE GESTION PARA LA ATENCIÓN DE DERECHOS ARCO

1. OBJETIVO

El presente documento tiene como objetivo establecer el proceso de atención a las solicitudes de información, actualización, rectificación, cancelación y oposición, de datos personales de los Titulares de Datos en cumplimiento a la Ley de Protección de Datos personales N° 29733 (En adelante: "la Ley"), como la documentación necesaria para cumplir con el objetivo.

2. ALCANCE

El Procedimiento de Atención de Derechos ARCO, inicia con el Ingreso del Formato de Solicitud de Ejercicio a los Derechos Arco (En adelante, "Formato de Ejercicio") por parte del Titular de Datos Personales, hasta la emisión de la respuesta por parte del Titular de Banco de Datos.

3. DEFINICIONES

3.1 **Acceso:** Derecho que tiene un Titular de Datos Personales para obtener la información que disponga sobre él, en bancos de datos de administración pública o privada.

3.2 **Cancelación:** Derecho que tiene un Titular de Datos Personales con la finalidad de ejercer acciones o medidas que se describen en la Ley como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.

3.3 **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

3.4 **Datos del representante:** Datos de la Persona Natural debidamente acreditado para representar a una persona Jurídica, ante entidades administrativas.

3.5 **Días**: Se refiere a días hábiles.

3.6 **Encargado del tratamiento:** Es aquella persona, que realiza el tratamiento de los datos personales, pudiendo ser el propio Titular del Banco de Datos personales o el Encargado del Banco de Datos Personales u otra persona por encargo del Titular del Banco de Datos Personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.

3.7 **Formato de Ejercicio:** Solicitud para la Atención de Derechos Arco

3.8 **Ley:** Ley N° 29733, Ley de Protección de Datos Personales

3.9 **Repositorio físico:** Es un lugar donde se almacena documentación física como: Ordenes de Taller, Pedidos de Ventas, Ofertas, etc., En cuyo contenido alberga información de carácter personal.

3.1 **Rectificación:** Derecho que tiene el Titular de Datos Personales, para ejecutar acciones genéricas destinada a afectar o modificar su información un banco de datos personales, ya sea para actualizarlo, incluir información en él o específicamente rectificar su contenido con datos exactos.

3.2 **Reglamento:** Reglamento de la Ley N° 29733 (Decreto Supremo N° 003-2013-JUS).

3.10 **Repertorio de jurisprudencia:** Es el banco de resoluciones judiciales o administrativas que se organizan como fuente de consulta y destinadas al conocimiento público.

3.11 **Responsable del tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

3.12 **Titular de banco de datos personales:** Persona natural, persona jurídica de derecho privado o entidad pública que decide o determina la finalidad y contenido del banco de datos personales, el tratamiento de los datos almacenados en éste y las medidas de seguridad.

3.13 **Titular de datos personales:** Persona natural a quien corresponde los datos personales.

3.14 **Oposición:** Es el derecho que tiene el Titular de Datos Personales, sobre la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

4. DOCUMENTOS A CONSULTAR

4.1 Ley N° 27933, “Ley de Protección de Datos Personales” y su reglamento.
4.2 Guía de Inscripción de Bancos de Datos Personales, “Autoridad Nacional de Protección de Datos Personales”.
4.3 Derecho Fundamental a la Protección de Datos Personales, “Guía para el Ciudadano”.

5. RESPONSABILIDADES

5.1 El Titular del Banco de Datos representado por el gerente general de la empresa es responsable de asegurar el cumplimiento del presente procedimiento, incluyendo la aprobación e implementación y acciones de mejora del mismo

5.2 El recepcionista es el encargado de recibir las solicitudes de atención a los derechos ARCO, registrar en el “Formato digital Atención de Derechos ARCO_DRIVE”.

5.3 Responsable del tratamiento, es el encargado de atender las solicitudes ingresadas, de los “Titulares”.

5.4 Todo el personal en el ámbito de su competencia es responsable de cumplir el presente procedimiento.

6. CONDICIONES GENERALES

6.1 El proceso de atención de derechos ARCO se inicia con la presentación de la Solicitud de Atención de derechos ARCO, por el Titular de Datos personales, de acuerdo al Art. 50 del Reglamento.

6.2 Para las atenciones de derecho Arco, en forma presencial deberá efectuarse en la dirección siguiente: _____ o mediante comunicación al correo electrónico _____

6.3 Se debe tener en cuenta los plazos de repuestas a las Solicitudes de Atención de derechos ARCO, son variables, en ningún caso se pueden exceder de los mismos.

6.4 Previo al envío, se debe revisar que por ningún motivo se revelen datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

6.5 En el caso de respuestas total o parcialmente negativas, se debe justificar detalladamente los motivos e indicar al titular de datos personales el derecho que le asiste al mismo para recurrir ante la Dirección General de Protección de Datos Personales en vía de reclamación.

6.6 En todos los casos se debe obtener evidencia de la recepción de la respuesta a la solicitud.

6.7 Para los casos en que no se pueda realizar una entrega de la respuesta, esta deberá ser comunicada mediante carta notarial a la dirección registrada por el titular de los datos personales ante la RENIEC.

6.8 El proceso de atención de derechos ARCO, se basa en los principios de “la Ley”

6.9 Todo participante involucrado en el proceso debe conocer la Legislación correspondiente a este procedimiento, además del proceso de atención de Derechos ARCO.

6.10 El documento debe ser revisado cuando cambian los procesos, condiciones de trabajo, por exigencias legales o al menos una vez al año a fin de evaluar si cumplen con los objetivos previstos.

6.11 En casos muy excepcionales se debe recurrir a “la Ley”, para verificar si es posible modificar alguno de los plazos regulares establecidos por la Ley.

7. DESARROLLO

Descripción	Responsable	Documento
1. <u>Presentación del "Formato de Ejercicio", por el "Titular".</u> a.- <u>Presentación Presencial</u> Proporcionar "Formato de Ejercicio" a la persona que desea Ejercer sus Derechos ARCO, realizar la consulta que si viene a nombre de algún titular de Datos Personales o a título personal. En caso de ser a título personal, se debería presentar los siguientes documentos: - Documento de Identificación Personal. - Copia de Documento de Identificación Personal. - Formato de Ejercicio. - Documentación adicional que sustente su requerimiento. En caso de venir en representación de un "Titular", se debería presentar los siguientes documentos: - Documento de Identificación Personal del representante debidamente acreditado. - Copia de Documento de Identificación Personal de representante debidamente acreditado. - Formato de Ejercicio. - Título que acredite representación. - Documentación adicional que sustente su requerimiento. Recepcionar la documentación a pesar de no haber todos los documentos, para realizar la respectiva atención. Entregar una copia del "Formato de ejercicio", al "Titular", dejando evidencia de la recepción. b.- <u>Presentación vía correo Electrónico</u> Una vez recibido el correo electrónico se: - Verificará que la información registrada en la solicitud y los documentos anexados cumplan con lo requerido en el párrafo anterior. - Responderá vía correo electrónico la solicitud, para dejar constancia de su recepción.	Recepcionista/ Cajera	- Documento de Identificación Personal. -Formato de Ejercicio. -Documentación Adicional.
2. <u>Registrar las Solicitudes de Ejercicio de los Derechos Arco</u> Se registrará en el DRIVE los siguientes datos: Nombre del Titular de datos Personales, Número del Documento de identificación Personal, medio por el cual se hará llegar la respuesta, dirección, correo electrónico, teléfono de contacto, derecho a reclamar, fecha de ingreso del documento, finalmente, a quien será derivado para su respectiva atención.	Recepcionista/ Cajera	Formato digital Atención de Derechos ARCO_DRIVE

Descripción	Responsable	Documento
3. <u>Entregar la documentación física al Responsable de dar tratamiento.</u> La recepcionista/cajera, tendrá que entregar dicho documento al Responsable del tratamiento de dato. El plazo máximo de entrega es al día siguiente de la recepción de la Documentación de ejercicio de atención de derechos ARCO, la entrega es en medio físico. En caso la comunicación sea enviada al correo electrónico, esta deberá ser derivada o atendida por el Responsable del tratamiento de datos.	Recepcionista/ Cajera	Documentación de ejercicio de atención de derechos ARCO.
4. <u>Analizar y Procesar el requerimiento</u> Ejecutar la atención al pedido del "Titular", para realizar dicha actividad consultar el INSTRUCTIVO DE EVALUACIÓN Y ELABORACIÓN DE RESPUESTA DE ATENCIÓN A DERECHOS ARCO.	Responsable de tratamiento	- Formato digital Atención de Derechos ARCO_DRIVE -Documentación de ejercicio de atención de derechos ARCO
5. <u>Remitir respuesta al titular de los datos personales por correo electrónico.</u> Remitir con atención al "Titular", según el medió de contacto especificado en el documento, copiar el correo de respuesta al encargado de la recepción, luego se debe etiquetar el correo para tener trazabilidad adecuada de dichas respuestas. La respuesta debe tener como asunto: "Atención a derechos ARCO – NUMERO DE DOCUMENTO DE IDENTIFICACIÓN PERSONAL"	Responsable de tratamiento	- E-mail de respuesta a la Solicitud de Atención de Derechos ARCO.
6. <u>Remitir respuesta al titular de los datos personales por medio físico.</u> Remitir la respuesta al "Titular", en caso de no encontrar la dirección señalada en el formato, la empresa de Courier, debe reportar que no se logró entregar el documento de manera formal.	Responsable de tratamiento	- Documento de respuesta al "Formato de Ejercicio".
7. <u>Registro de repuestas no contactadas.</u> Se registrará en el Formato digital compartido en el DRIVE las Respuesta a las solicitudes que no fueron entregadas por no existir la dirección establecida o estar errada, deberán ser serán archivada, como una prueba de atención.	Responsable de tratamiento	- Formato digital Atención de Derechos ARCO_DRIVE.

8. REGISTROS Y ANEXOS:

Código	Nombre	Responsable del Control
Anexo N°1	Formato digital Atención de Derechos ARCO_DRIVE	Recepcionista Responsable de Tratamiento de datos

N°	TITULAR DE DATOS PERSONALES	DOCUMENTO DE IDENTIFICACIÓN PERSONAL	MEDIO DE RESPUESTA A LA SOLICITUD	DIRECCIÓN	CORREO ELECTRÓNICO	TELÉFONO DE CONTACTO	DERECHO ARCO A RECLAMAR	FECHA DE INGRESO DEL DOCUMENTO	STATUS DE ATENCIÓN
1									
2									
3									

Código	Nombre	Responsable del Control
Anexo N°2	Formato solicitud de ejercicio a los Derechos ARCO.	Responsable de Tratamiento de datos

FORMATO PARA EL EJERCICIO DE DERECHOS ARCO

_____, con RUC N° _____, con domicilio en _____ – _____ – Lima – Perú, en cumplimiento de lo dispuesto por la Ley de Protección de Datos

Personales y su Reglamento, se pone a su disposición a fin de que pueda ejercer los derechos que la Ley le confiere para la protección de sus datos personales contenidos en los bancos de datos de nuestra titularidad. Con el objeto de poder servirlo de la mejor manera, le rogamos completar los campos que a continuación se precisan:

DATOS DEL TITULAR DE LOS DATOS PERSONALES QUE EJERCE EL DERECHO

Nombre Completo :

Documento de Identidad :

Domicilio :

Correo electrónico :

DATOS DEL REPRESENTANTE DEL TITULAR DE LOS DATOS PERSONALES QUE EJERCE EL DERECHO -de corresponder-

Nombre del Representante :

Documento de Identidad del Representante :

Domicilio del Representante :

Correo electrónico del Representante :

DIRECCION PARA LAS NOTIFIACIONES

Domicilio Procesal -puede ser electrónico- :

DERECHO QUE ES EJERCIDO

-marcar la opción correspondiente-

* ACCESO: con el objeto de obtener información sobre sus propios datos personales y su tratamiento.

* RECTIFICACIÓN: con el objeto de actualizar sus datos, corregirlos o rectificarlos, y/o incluir información, mediante el sustento respectivo.

* CANCELACIÓN: con el objeto de suprimir y cancelar datos del banco cuando su tratamiento ya no sea necesario o pertinente, o cuando haya revocado el consentimiento otorgado.

* OPOSICIÓN: con el objeto de impedir el tratamiento de datos personales o cese de éste, cuando el titular no hubiere prestado su consentimiento o cuando acredite justificación para ello.

DETERMINACIÓN CONCRETA DEL PETITORIO Y DEL DERECHO QUE SE EJERCE.

-describa brevemente su pedido y susténtelo-

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

ANEXOS Y EVIDENCIAS

-adjunte los documentos que sustenten su solicitud-

1.- Documento de Identidad

2.- Documento de Identidad del Representante -de ser el caso-

3.- Poder del Representante -de ser el caso-

4.- Documentos que sustenten su solicitud:

4.1.- _____

4.2.- _____

4.3.- _____

4.4.- _____

4.5.- _____

Mientras dure el procedimiento de ejercicio de los derechos de actualización, inclusión, rectificación o supresión de datos personales, se dispone el bloqueo de los datos.

Recibida la solicitud de ejercicio de derechos por parte del titular de datos personales, en un plazo máximo de cinco días hábiles será calificada; en caso la misma no cumpla con los requisitos, se le notificará, dentro de estos mismos cinco días hábiles, las observaciones que

requieran subsanación, para que cumpla con ello en un plazo máximo de cinco días hábiles adicionales; en caso no se cumpla con la observación, su solicitud se tendrá por no presentada.

En el caso que la información o documentación presentada en su solicitud sea insuficiente o equivocada, e impida darle trámite, se le requerirá dentro de los siete días hábiles siguientes de recibida su solicitud, la documentación e información adicional o correcta; usted tendrá diez días hábiles para atender dicho requerimiento, caso contrario, se tendrá por no presentada su solicitud.

Si su solicitud cumple con todos los requisitos, los plazos de atención y repuesta serán los siguientes, computados a partir del día siguientes de la fecha de presentación:

* Ocho días ante el ejercicio del derecho de información.

* Veinte días ante el ejercicio del derecho de acceso.

* Diez días ante el ejercicio de los otros derechos como los de actualización, rectificación, cancelación, supresión, inclusión u oposición.

Para el caso de solicitudes observadas, los plazos antes indicados se computarán a partir del día siguiente de la presentación de la subsanación correspondiente.

Con excepción al cumplimiento del plazo fijado para la atención ante el ejercicio del derecho de información, los demás plazos correspondientes a la atención de los demás derechos podrán ser objeto de ampliación por una sola vez, y por un plazo igual.

Para mayor información podrá consultar nuestro Código de Conducta para la protección de datos personales en www.euromotors.com.pe.

Firma :

Lugar y fecha :

Nombres :

Documento de Identidad :

9. CONTROL DE CAMBIOS

N° de Revisión	Sección y/o Página	Fecha de revisión	Motivo	Autorizado por:

ANEXO 6.3

INSTRUCTIVO PARA RESPUESTA ANTE EL EJERCICIO DE DERECHOS ARCO

1. OBJETIVO

El presente documento tiene como objetivo establecer las Instrucciones que deben ejecutarse para realizar la evaluación y elaboración de respuesta a la solicitud de atención a derechos ARCO.

2. ALCANCE

El Instructivo de Evaluación y Elaboración de Respuesta de Atención a Derechos ARCO, comienza con la recepción del Formato de Solicitud para el Ejercicio de Derechos ARCO por parte del Responsable de Tratamiento, y culmina con la emisión de la respuesta.

3. DOCUMENTOS A CONSULTAR

3.1 Ley N° 29733, “Ley de Protección de Datos Personales y su reglamento”.
3.2 Guía de Inscripción de Datos Personales.
3.3 Derecho fundamental a la Protección de Datos Personales, “Guía para el ciudadano”.

3. DEFINICIONES

3.1 **Acceso:** Derecho que tiene un Titular de Datos Personales para obtener la información que disponga sobre él, en bancos de datos de administración pública o privada.

3.2 **Cancelación:** Derecho que tiene un Titular de Datos Personales con la finalidad de ejercer acciones o medidas que se describen en la Ley como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.

3.3 **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

3.4 **Días**: Se refiere a días hábiles

3.5 **Encargado del tratamiento:** Es aquella persona, que realiza el tratamiento de los datos personales, pudiendo ser el propio Titular del Banco de Datos personales o el Encargado del Banco de Datos Personales u otra persona por encargo del Titular del Banco de Datos Personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.

3.6 **Ley:** Ley N° 29733, Ley de Protección de Datos Personales

3.7 **Rectificación:** Derecho que tiene el Titular de Datos Personales, para ejecutar acciones genéricas destinada a afectar o modificar su información un banco de

datos personales, ya sea para actualizarlo, incluir información en él o específicamente rectificar su contenido con datos exactos.

3.8 **Reglamento**: Reglamento de la Ley N° 29733 (Decreto Supremo N° 003-2013-JUS)

3.9 **Responsable del tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

3.10 **Titular de banco de datos personales:** Persona natural, persona jurídica de derecho privado o entidad pública que decide o determina la finalidad y contenido del banco de datos personales, el tratamiento de los datos almacenados en éste y las medidas de seguridad.

3.11 **Titular de datos personales:** Persona natural a quien corresponde los datos personales.

3.12 **Oposición:** Es el derecho que tiene el Titular de Datos Personales, sobre la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

4. DESARROLLO DEL INSTRUCTIVO

Descripción	Documento Asociado
1. <u>Verificar los documentos del Formato de Solicitud de Atención a los Derechos ARCO.</u> En caso que el Titular de Datos Personales se aproxime personalmente o se comunique vía correo electrónico, deberá presentar los siguientes documentos: -Formato de solicitud de ejercicio de Derechos ARCO o documento donde solicite ejercer sus derechos ARCO. -Copia de documento de Identificación Personal (Documento Nacional de Identidad, Carnet de extranjería, Pasaporte). -Verificar que se encuentren anexados los documentos que se declararon en el Formato de Solicitud de Atención de Derechos ARCO. En caso de representante legal debidamente acreditado como tal: -Formato de solicitud de ejercicio de Derechos ARCO o documento donde solicite ejercer sus derechos ARCO -Copia de documento de Identificación Personal del representante legal (Documento Nacional de Identidad, Carnet de extranjería, Pasaporte). -Poder de representación que figure la finalidad de manera expresa, que el Representante Legal, representará al Titular de Datos Personales. -Verificar que se encuentren anexados los documentos que se declararon en el Formato de Solicitud de Atención de Derechos ARCO En caso carecer de alguno de los requisitos antes mencionados, en el plazo de 5 días luego de haberse ingresado la documentación, debe formular observaciones que no puedan ser salvadas de oficio. El Titular de Datos Personales, deben brindar una respuesta como máximo en un plazo de 5 días, en caso de transcurrido el plazo señalado, sin que ocurra la subsanación se tendrá por no presentada la solicitud.	-Formato de Solicitud de Atención a los Derechos ARCO -Documentos adjuntos a la solicitud

Descripción	Documento Asociado
2. <u>Verificar que los documentos adjuntos al Formato de Solicitud de Atención a los Derechos ARCO, cuenten con la información necesaria para dar atención a la solicitud.</u> En caso la información proporcionada en la solicitud, es insuficiente o errónea, de forma que no permita su atención. Se podrá solicitar información adicional al Titular de Datos Personales, dentro de los siete (7) días siguientes de haberse recibida la solicitud; en el plazo de diez (10) días de haber recibido las consultas por parte del responsable de tratamiento, el Titular de Datos Personales acompañará la respuesta con la documentación adicional, en caso contrario, se tendrá por no presentada dicha solicitud.	- Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud
3. <u>Analizar el Formato de Solicitud de Atención a los Derechos ARCO.</u> Existen 5 tipos de solicitud que pueden ser presentadas por los Titulares de Datos Personales, según el tipo de solicitud se tendrá un procedimiento para ser atendidos. **Derecho a la Información:** Para efectos de la atención de este derecho , se deberá preparar un documento en donde se especifique la siguiente información: - La identidad y domicilio del Titular del Banco de Datos Personales, para dirigirse, revocar el consentimiento o ejercer sus derechos. - Finalidades del tratamiento al que sus datos serán sometidos. - Identidad de los que son o pueden ser sus destinatarios, de ser el caso. - Existencia del banco de datos personales, en que se almacenarán, cuando corresponda. - El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso. - Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo. - Transferencia de Datos Personales a dentro o Fuera del territorio Nacional. Se dispone de ocho (8) días contados desde el día siguiente de la presentación del formato de atención a los derechos ARCO, para la atención al derecho de la Información.	- Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud
Derecho de Acceso: Implica brindar información de datos Personales, así como las condiciones y generalidades del tratamiento de los mismos. Para efectos de la atención de este derecho, se deberá preparar un documento en el que se especifique la siguiente información: - Los registros de los datos personales del solicitante. - La forma en que estos datos fueron recopilados. - Las razones que motivaron a su recopilación. - A solicitud de quién se realizó dicha recopilación - Transferencias realizadas o que se prevén hacer de ellos, de ser el caso. Para conocer cada uno de los puntos se debe revisar el Consentimiento de TDP del titular solicitante, así como los archivos y sistema(s) donde se realizan los tratamientos. Podrá suministrarse por escrito, por medios electrónicos, telefónicos, de	- Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud

Descripción	Documento Asociado
imagen u otro idóneo para tal fin. El titular de los datos personales podrá optar a través de algunos o varios de las siguientes formas: - Visualización en sitio. - Escrito, copia, fotocopia o facsímil. - Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información. - Cualquier otra forma o medio que sea adecuado a la configuración o implantación material del banco de datos personales o a la naturaleza del tratamiento, establecido por el titular de Banco de Datos Personales. El informe no podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. Se dispone de veinte (20) días contados desde el día siguiente de la presentación del formato de solicitud de Atención a los derechos ARCO, para la atención del derecho de Acceso,	
Derecho de Rectificación: Implica modificar datos personales, por motivos de actualización, corrección e Inclusión. La solicitud de actualización: deberá señalar a qué datos personales se refiere, así como la modificación que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la actualización solicitada. La solicitud de corrección: deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la rectificación solicitada. La solicitud de inclusión: deberá indicar a qué datos personales se refiere, así como la incorporación que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia e interés fundado para el mismo. Para proceder con la rectificación se deberán seguir las siguientes actividades: - Validar que los documentos anexos a la solicitud confirmen que los datos personales a los que se hace referencia, serán correctamente rectificados. - Buscar todo los datos personales del solicitante dentro de los diferentes bancos de datos bajo la titularidad de la organización. - Obtener evidencia de a qué datos personales se le ha estado dando tratamiento a la fecha; o de ser el caso, que no se había estado dando tratamiento a ninguno. - Rectificar los datos según la solicitud del titular de datos personales. - Obtener evidencia de los nuevos datos personales a los que se les dará tratamiento. - Elaborar un documento que confirme la realización de la(s) rectificación(es) solicitadas; o de ser el caso, que no se ha dado tratamiento a los datos personales del titular. Se dispone de Diez (10) días contados desde el día siguiente de la presentación del formato de solicitud de Atención a los derechos ARCO,	-_Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud

Descripción	Documento Asociado
para la atención del derecho de Rectificación.	
Derecho de Cancelación: Se podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al presente reglamento. Se podrá suprimir o cancelar una parte o todos los Datos Personales contenidos en un banco de datos personales. Deberá documentar ante el titular de los datos personales, haber cumplido con lo solicitado e indicar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente. La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos	-Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud
Para proceder con la Cancelación se deberán seguir las siguientes actividades: - Buscar todos los datos personales del solicitante dentro de los diferentes bancos de datos bajo la titularidad de la organización. - Obtener evidencia de a qué datos personales se le ha estado dando tratamiento a la fecha; o de ser el caso, que no se había estado dando tratamiento a ninguno. - Cesar el tratamiento de los datos personales a partir de un bloqueo de los mismos y su posterior eliminación. - Identificar que transferencias se realizaron con los datos personales. - Obtener evidencia de los nuevos datos personales, actualizados, corregidos o incluidos a los que se les dará tratamiento a partir de ahora. - Elaborar un documento en el que se especifique la siguiente información: • Confirmación de la cancelación de los datos personales. • Transferencias realizadas previas a la cancelación. • Receptor(es) de las transferencias realizadas. Si por algún motivo, los datos personales no pueden ser eliminados, se deberá ver la factibilidad de emplear medios de disociación o anonimización para continuar el tratamiento - Se dispone de Diez (10) días contados desde el día siguiente de la presentación del formato de solicitud de Atención a los derechos ARCO, para la atención del derecho de Cancelación.	-Formato de Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud
Derecho de Oposición: Podrá oponerse a que no se lleve a cabo el tratamiento de datos personales o se cese en el mismo, cuando no	-Formato de

Descripción	Documento Asociado
hubiese prestado su consentimiento para su recopilación, a pesar de haberse tomado de fuente de acceso público; incluso cuando hubiera prestado su consentimiento, el titular de datos personales tiene derecho a oponerse a sus tratamientos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho. Para atender el Derecho a la Oposición se deberán seguir las siguientes actividades: - Buscar todo los datos personales del solicitante dentro de los diferentes bancos de datos bajo la titularidad de la organización. - Identificar, el momento, la forma, razones y a solicitud de quien se recopilaron los datos personales. - Evaluar si el tratamiento dado a los datos personales incumple con alguno de los puntos dentro del consentimiento brindado por el titular de datos personales. - De resultar justificada la oposición, proceder con el cese del tratamiento: marcar el consentimiento como anulado y actualizarlo en el sistema y otros bancos de datos. Se dispone de Diez (10) días contados desde el día siguiente de la presentación del formato de solicitud de Atención a los derechos ARCO, para la atención del derecho de Oposición.	Solicitud de Atención a los Derechos ARCO. -Documentos adjuntos a la solicitud

ANEXO 7

CONVENIO DE TRANSFERENCIA DE DATOS PERSONALES
Y CONDICIONES PARA SU TRATAMIENTO Y PROTECCION

Conste por el presente documento el **Convenio de Transferencia de Datos Personales y Condiciones para su Tratamiento y Protección**, que celebran de un lado, _____, con R.U.C. N° _____, con domicilio en _____, quien procede representada por su _____ señor _____, identificado con D.N.I. N° _____, según facultades que obran inscritas en la Partida Electrónica N° _____ del Registro de Personas Jurídicas de _____, en adelante el **TRANSFERENTE**; y de otro lado, _____, con R.U.C. N° _____, con domicilio en _____, quien procede representada por su _____ señor _____, identificado con D.N.I. N° _____, según facultades que obran inscritas en la Partida Electrónica N° _____ del Registro de Personas Jurídicas de _____, en adelante el **RECEPTOR**; en las condiciones y estipulaciones siguientes:

PRIMERO: El **TRANSFERENTE** es titular del Banco de Datos Personales de administración privada en el cual ha recopilado y continua recopilando información de sus clientes proporcionada de manera consentida e informada para las finalidades y destino autorizados, y bajo las condiciones, restricciones derechos y deberes convenidos con los mismos, que las partes declaran conocer; base de datos que también se nutre sin necesidad de consentimiento, siempre que el mismo está justificado en cualquiera de las excepciones establecidas por ley, como por ejemplo, para el ejercicio de las funciones de las entidades públicas para el cumplimiento de sus deberes, acceso a fuentes de datos públicos, para la celebración, cumplimiento y ejecución de relaciones contractuales, y las demás que legalmente están establecidas, o se establezcan en un futuro.
Los datos personales recopilados por el **TRANSFERENTE** están incorporados en un Banco de Datos Privados que garantizan las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos. Asimismo, el **TRANSFERENTE** cuenta con autorización expresa de los titulares de los datos personales proporcionados y recopilados, para el flujo y transferencia de dichos datos a terceras personas, incluyendo el flujo transfronterizo de los mismos, lo cual se podrá realizar igualmente sin consentimiento, siempre y cuando ello esté justificado en cualquiera de las excepciones de ley.
El **TRANSFERENTE** tiene el deber de cumplir y hacer cumplir las condiciones y estipulaciones bajo las cuales ha conseguido el consentimiento para el tratamiento de datos personales de los titulares de éstos, de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, del Código de Conducta para la protección de datos personales del **TRANSFERENTE** (publicado en www.euromotors.com.pe), y de su Política de Privacidad (publicada en _____), que el **RECEPTOR** declara conocer; manteniendo la seguridad y confidencialidad de dichos datos, así como garantizando el debido ejercicio y atención de los derechos de los titulares de los mismos. Obligaciones y deberes legales que se deben asegurar igualmente al momento de realizar la transferencia o flujo de los datos, y que el receptor de los mismos debe cumplir de igual manera que el que los trasmite.

SEGUNDO: En atención a lo indicado en la cláusula precedente, por el presente convenio se regulan las relaciones jurídicas que enmarcan los procesos de transferencia o flujo de datos personales que proporcione y comparta el **TRANSFERENTE** con el **RECEPTOR**, los cuales se podrán realizar indistintamente en cualquier momento, y conforme a las relaciones y/o requerimientos que tengan ambos; asimismo, este documento regula el tratamiento y protección de dichos datos. Para ello, el **TRANSFERENTE** transfiere y transferirá datos personales de sus clientes al **RECEPTOR**, contando con la autorización expresa de sus titulares, y también sin consentimiento, para los casos exceptuados por ley.

TERCERO: Por el presente documento, las partes se obligan a asegurar que el flujo de datos personales se realice manteniendo el más alto grado de seguridad y confidencialidad, tanto a nivel técnico, organizativo como jurídico.

CUARTO: El **RECEPTOR** se obliga a respetar y cumplir de manera irrestricta absolutamente todas las condiciones para la protección y tratamiento de los datos personales que le son transferidos, conforme a las estipulaciones y finalidades de los consentimientos otorgados por sus titulares, a la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, y del Código de Conducta para la protección de datos personales del **TRANSFERENTE**, que el **RECEPTOR** también declara conocer y se obliga a cumplir. En tal sentido, el **RECEPTOR** deberá asegurar que los datos personales que recibe sean tratados con seguridad y confidencialidad, conforme a la finalidad y destino para los que fueron otorgados. En este sentido, para el caso del tratamiento de datos que se transfieran, obtenidos mediante el consentimiento de su titular, el **RECEPTOR** deberán respetar y sujetarse a las condiciones del documento modelo adjunto como **ANEXO** mediante el cual se obtuvo dicho consentimiento; para el caso de datos transferidos que no hayan requerido consentimiento, su tratamiento se deberá circunscribir y limitar a su tratamiento conforme a la causal legal que lo permite sin dicho consentimiento.

QUINTO: El **RECEPTOR** deberá cumplir de manera inmediata con proporcionar acceso a la información de los datos personales proporcionados a sus titulares, la forma y razones por la que los otorgaron, las transferencias realizadas, así como asegurar a los titulares el derecho a actualizar sus datos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos, en cuanto el **TRANSFERENTE** y/o el titular de los datos personales se lo soliciten.

SEXTO: El **RECEPTOR** será responsable directo por la vulneración de los derechos de los titulares de los datos personales que le sean transferidos, en caso incumpla las obligaciones que asume en el presente documento o contravenga las condiciones o finalidades que delimitan el tratamiento de los datos, la Ley de Protección de Datos Personales, su Reglamento, o el Código de Conducta, liberando desde ya al **TRANSFERENTE** de toda responsabilidad por acto u omisiones que le sean imputables, ya sea por dolo o negligencia o por la causa que fuera.

SEPTIMO: El presente documento tendrá duración temporal, el cual estará sujeto de manera accesoria a cualquier tipo de relación comercial y/o contractual que pudiera tener el **TRANSFERENTE** con el **RECEPTOR**. Por lo tanto, terminada la relación comercial y/o contractual principal entre dichas partes, el presente convenio concluirá de manera indefectible. Sin perjuicio de lo anterior, el **TRANSFERENTE** podrá también poner término al presente convenio y resolverlo en cualquier momento y sin expresión de causa, y sin que ello le genere ningún tipo de responsabilidad, para lo cual bastará una comunicación escrita en dicho sentido.

OCTAVO: El **RECEPTOR** únicamente podrá utilizar la información y/o cualquier dato personal proporcionado por el **TRANSFERENTE** para cumplir con el objetivo de sus relaciones comerciales y/o contractuales principales, y siempre en pleno respeto de las estipulaciones y finalidades por las cuales de otorgó el consentimiento de los datos, de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, y del Código de Conducta para la protección de datos personales del **TRANSFERENTE**; nunca para otra finalidad. En tal sentido, el **RECEPTOR** queda expresamente prohibido de transferir los datos personales que el **TRANSFERENTE** le haya podido proporcionar a terceros, a excepción de aquellos expresamente autorizados, y de aquellos que se puedan tratar sin consentimiento bajo las excepciones establecidas por ley, lo cual no enerva el derecho de realizar el tratamiento por encargo que pueda confiar a terceros bajo estrictas medidas de seguridad y confidencialidad, así como de destinarlos para fines permitidos conforme a las excepciones de ley, bajo responsabilidad exclusiva del **RECEPTOR**, por el incumplimiento, por acción u omisión, de sus obligaciones. De esta manera, el **RECEPTOR** asegura al **TRANSFERENTE** que cuenta con las medidas de seguridad y protección técnica, organizativa y legal para el tratamiento, seguridad, protección y confidencialidad de los datos personales e información que le son confiados. Toda información o datos personales que sean proporcionados al **RECEPTOR** sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada.

NOVENO: El **RECEPTOR** deberá asegurar el cumplimiento del presente convenio en todos los niveles de su organización, personal, trabajadores, representantes, adscritos, colaboradores, y en general, cualquier persona que pueda tener acceso a los datos personales que se transfieren.

DECIMO: El presente convenio no generará contraprestación de ningún tipo entre las partes, no existiendo obligación de retribución alguna entre las mismas. De igual forma, el presente convenio no genera vínculo laboral alguno, beneficios sociales ni compensación alguna contemplada en las leyes laborales, entre el **TRANSFERENTE** y el **RECEPTOR** y/o sus empleados, personal, representantes, adscritos, colaboradores, y general, de cualquier persona relacionada con éstos, quienes no se encuentran bajo relación de dependencia o subordinación respecto del **TRANSFERENTE**.

DECIMO PRIMERO: El **RECEPTOR** se obliga a mantener confidencialidad absoluta sobre la celebración de este convenio, y especialmente sobre toda y cualquier información y datos que pueda manejar o recibir en mérito al mismo. Asimismo, el **RECEPTOR** se obliga a mantener absoluta confidencialidad sobre toda información comercial, operativa, financiera, legal y societaria que conozca como consecuencia del desarrollo de sus actividades; así como respecto de los usos, procedimientos, instalaciones, equipos, estrategias, estructuras, costos, mercadeo, diseños, programas, especificaciones técnicas y toda otra clase de información que él, sus operarios o personal puedan conocer, y que esté relacionada con las actividades de la organización, sistemas informáticos, procedimientos, clientes, proveedores, accionistas, empleados y ejecutivos del **TRANSFERENTE**.

Queda estrictamente prohibido al **RECEPTOR** y a sus empleados, personal, representantes, adscritos, colaboradores, y general, de cualquier persona relacionada con éstos, la reproducción, impresión o copia, parcial o total, de la información a la que tuviere acceso o conociera durante la vigencia de este convenio; asumiendo plena responsabilidad por las consecuencias que se deriven del uso indebido por parte de él o terceras personas relacionadas. En tal sentido, el **RECEPTOR** asume plena responsabilidad directa e indirecta respecto de sus propias acciones y aquellas desplegadas por sus accionistas, socios, directivos, representantes, gerentes, empleados, trabajadores, contratistas y personas vinculadas y adscritas, para el debido cumplimiento del presente convenio, debiendo tratarse los datos para los fines autorizados, y nunca para otra finalidad, estando expresamente prohibidos de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuvieren acceso, para fines no autorizados y/o ajenos a sus obligaciones, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que se les haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno al autorizado. La obligación de confidencialidad y de protección de datos personales contenidas en este convenio subsistirá indefinidamente con fuerza y vigor aún después de terminado el vínculo contractual por cualquier causa.

Suscrito en dos ejemplares de idéntico valor legal, en Lima a los _____ días del mes de _____ del _____.

ANEXO

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES – CLIENTES Y PROSPECTOS

En cumplimiento de la Ley de Protección de Datos Personales, quien suscribe, otorga consentimiento voluntario, libre, previo, expreso, informado e inequívoco a **_____**, con R.U.C. N° _____, y con domicilio en la _____ – _____ – Lima – Perú, para que realice por plazo indefinido, el tratamiento, en cualquiera de sus modalidades, medios o soportes, local o transfronterizo, de los datos personales que haya podido proporcionar, incluyendo nombres, apellidos, datos de identificación, perfil, dirección, números telefónicos, correos electrónicos, imagen y/o voz, características e información de vehículos, incidencias de servicio, comportamiento del conductor y del vehículo, estilo de manejo, ajustes de confort, data del sistema de entretenimiento, de navegación y de usos e incidentes del vehículo, recorrido, placas, récord de servicios y reportes de necesidad de servicios, recorridos, estado del vehículo, y todo aquello que registren los módulos informáticos de a bordo de estos y aquella que se almacene en las llaves, incluyendo los videos, imágenes y audio; información de citas, facturación y reclamos por los servicios prestados; artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, encuestas, preferencias e intereses, datos económicos y de seguros, y relaciones sociales; para ser utilizados para fines administrativos, comerciales, de publicidad, de segmentación, estadísticos, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; pudiendo formar también parte estos datos de las campañas, avisos, difusiones y publicaciones que haga el receptor de los datos.

Los datos personales recogidos serán incorporados y tratados en un Banco de Datos de titularidad **_____**, declarado ante la Autoridad de Datos Personales con Código de Registro N° _____, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos.

El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones contractuales, tratativas o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento. Con el objeto de poder asegurar un debido y oportuno servicio técnico, soporte de postventa, y para mantener el uso y disfrute de todas las funcionalidades, beneficios y prestaciones que a nivel mundial ofrece la marca del vehículo del titular de los datos personales, y siendo obligación contractual asegurar que todos los usuarios de dicha marca puedan acceder a ello, se informa al titular que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte por ser usuario de dicha marca de vehículo, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, incluyendo el tratamiento compartido con el fabricante, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales, incluyendo para ello las transferencias de datos, a nivel nacional e internacional que sean necesarias.

Los datos serán tratarlos con veracidad, calidad y proporcionalidad; la negativa a otorgarlos impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, o una comunicación vía correo electrónico a **_____@_____**, haciendo precisión de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es **_____**, y su destino será el mismo Banco de Datos, sin perjuicio de la autorización expresa de flujo nacional e internacional que también se otorga. En tal sentido, el otorgante autoriza y presta su consentimiento previo, expreso, libre e informado, para que se compartan o se realice tratamiento compartido sus datos personales mediante la transferencia y/o encargo de tratamiento, local y/o transfronterizo con las empresas que conforman el grupo **EUROMOTORS** al cual pertenece y se rigen bajo el Código de Conducta que se puede consultar en www.euromotors.com.pe; así como también, con el representante en el Perú de las marcas de vehículos _____, _____, _____, _____, la empresa peruana **_____**, y también al fabricante de estos, a quienes se le podrán transferir los datos por intermedio del citado representante y cuyo detalle se aprecia en el siguiente enlace _____; así como también, con las empresas que conforman la **RED DE CONCESIONARIOS OFICIALES o TALLERES AUTORIZADOS** de dichas marcas (cuyo detalle se verifica en **_____**, **_____**, **_____**, **_____**), a quienes se le podrán transferir los datos directamente o por intermedio del citado representante; de igual manera, el otorgante autoriza la transferencia de sus datos personales a las empresas del sistema financiero peruano identificadas y acreditadas por la Superintendencia de Banca, Seguros y AFP del Perú (cuyo detalle se verifica en www.sbs.gob.pe), así como a empresas Administradoras de Fondos Colectivos autorizadas por la Superintendencia del Mercado de Valores (cuyo detalle se verifica en www.smv.gob.pe). Del mismo modo, se otorga consentimiento a fin de que, se pueda realizar el encargo de tratamiento de datos personales a quienes se detallan en el siguiente enlace **_____**. Los receptores de datos personales asumen las mismas obligaciones y/o responsabilidades que **_____**, estableciéndose que dichos receptores podrán utilizar los datos personales del cliente únicamente para las mismas finalidades y destino regulado en el presente documento, y para

cumplir con el encargo efectuado, garantizándose que los mismos respeten igualmente la protección, seguridad y confidencialidad de dichos datos, así como el ejercicio pleno ante estos de sus derechos.

Finalmente, se ratifica el compromiso institucional, de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndonos en una mejora continua. Consulte nuestra Política de Privacidad en _____.

ANEXO 8

CONVENIO DE TRATAMIENTO DE DATOS POR ENCARGO

Conste por el presente documento el **Convenio de Tratamiento de Datos por Encargo**, que celebran de un lado, _____, con R.U.C. N° _____, con domicilio en _____, quien procede representada por su _____ señor _____, identificado con D.N.I. N° _____, según facultades que obran inscritas en la Partida Electrónica N° _____ del Registro de Personas Jurídicas de _____, en adelante el **TITULAR**; y de otro lado, _____, con R.U.C. N° _____, con domicilio en _____, quien procede representada por su _____ señor _____, identificado con D.N.I. N° _____, según facultades que obran inscritas en la Partida Electrónica N° _____ del Registro de Personas Jurídicas de _____, en adelante el **ENCARGADO**; en las condiciones y estipulaciones siguientes:

PRIMERO: El **TITULAR** es titular del Banco de Datos Personales de administración privada en el cual ha recopilado y continua recopilando información de sus clientes proporcionada de manera consentida e informada para las finalidades y destino autorizados, y bajo las condiciones, restricciones, derechos y deberes convenidos con los mismos, que las partes declaran conocer; base de datos que también se nutre sin necesidad de consentimiento, siempre que el mismo está justificado en cualquiera de las excepciones establecidas por ley, como por ejemplo, para el ejercicio de las funciones de las entidades públicas para el cumplimiento de sus deberes, acceso a fuentes de datos públicos, para la celebración, cumplimiento y ejecución de relaciones contractuales, y las demás que legalmente están establecidas, o se establezcan en un futuro.
Los datos personales recopilados por el **TITULAR** están incorporados en un Banco de Datos Privados que garantizan las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos. Asimismo, el **TITULAR** cuenta con autorización expresa de los titulares de los datos personales proporcionados y recopilados, para el flujo y transferencia de dichos datos a terceras personas, incluyendo el tratamiento por encargo, lo cual se podrá realizar igualmente sin consentimiento, siempre y cuando ello esté justificado en cualquiera de las excepciones de ley.
El **TITULAR** tiene el deber de cumplir y hacer cumplir las condiciones y estipulaciones bajo las cuales ha conseguido el consentimiento para el tratamiento de datos personales de los titulares de éstos, de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, del Código de Conducta para la protección de datos personales del **TITULAR** (publicado en www.euromotors.com.pe), y de su Política de Privacidad (publicada en _____), que el **ENCARGADO** declara conocer; manteniendo la seguridad y confidencialidad de dichos datos. Obligaciones y deberes legales que se deben asegurar igualmente al momento de realizar el tratamiento por encargo, y que el **ENCARGADO** debe de cumplir de igual manera.

SEGUNDO: En atención a lo indicado en la cláusula precedente, por el presente convenio se regulan las relaciones jurídicas que enmarcan los procesos de entrega de datos personales que proporcione el **TITULAR** al **ENCARGADO**, los cuales se podrán realizar indistintamente en cualquier momento, y conforme a los requerimientos que tenga el primero de ellos, para que el segundo los trate vía encargo con el único objeto de _____; asimismo, este documento regula la protección de dichos datos. Para ello, el **TITULAR** dispone el tratamiento por encargo de datos personales al **ENCARGADO** para una finalidad debidamente autorizada y consentida, y también sin consentimiento, para los casos exceptuados por ley.

TERCERO: Por el presente documento, las partes se obligan a asegurar que el flujo de datos personales se realice manteniendo el más alto grado de seguridad y confidencialidad, tanto a nivel técnico, organizativo como jurídico, y con el único objetivo de que el **ENCARGADO** pueda cumplir con el tratamiento de datos que le es confiado específica y concretamente por el **TITULAR**. Queda expresamente establecido y comprendido por las partes que el presente convenio no constituye una transferencia de datos, por lo que el **ENCARGADO** nunca asumirá titularidad de los datos que le son confiados para tratamientos específicos, cumpliendo este último únicamente un encargo temporal y transitorio sin adquirir derecho alguno sobre los datos.

CUARTO: El **ENCARGADO** se obliga a respetar y cumplir de manera irrestricta absolutamente todas las condiciones para la protección y tratamiento de los datos personales que le son encargados para una tratamiento específico y temporal, conforme a las estipulaciones y finalidades de los consentimientos otorgados por sus titulares, de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, y del Código de Conducta para la protección de datos personales del **TITULAR**, que el **ENCARGADO** también declara conocer y se obliga a cumplir. En tal sentido, el **ENCARGADO** deberá asegurar que los datos personales que recibe para cumplir con el encargo del tratamiento sean tratados con seguridad y confidencialidad, conforme a la finalidad y destino específico que delimita dicho encargo.

QUINTO: El **ENCARGADO** será responsable directo por la vulneración de los derechos de los titulares de los datos personales que le sean encargados para su tratamiento, en caso incumpla las obligaciones que asume en el presente documento o contravenga las condiciones o finalidades que delimitan el tratamiento de los datos, o en la Ley o en el Código de Conducta, liberando desde ya al **TITULAR** de toda responsabilidad por acto u omisiones que le sean imputables, ya sea por dolo o negligencia o por la causa que fuera.

SEXTO: El presente documento tendrá duración temporal de ____ meses, que constituye el periodo de tiempo que se requiere para cumplir con el tratamiento por encargo materia de este documento. Por lo tanto, terminado el plazo contractual, el presente convenio

concluirá de manera indefectible. Sin perjuicio de lo anterior, el **TITULAR** podrá también poner término al presente convenio y resolverlo en cualquier momento y sin expresión de causa, y sin que ello le genere ningún tipo de responsabilidad, para lo cual bastará una comunicación escrita en dicho sentido. Concluido el presente convenio, sea por la causa que fuera, el **ENCARGADO** deberá cumplir con devolver y restituir toda la información, documentación y datos personales que el **TITULAR** le haya podido proporcionar, así como con eliminar y cancelar por completo todas las copias o respaldos que se hubiera podido crear, sin dejar rastro alguno de los mismos, estando prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en cualquier tipo de soporte, sea cual fuere su naturaleza, así como también, estando prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir, así como de realizar cualquier tratamiento respecto de los mismos, debiendo asumir las consecuencias legales por su incumplimiento. Debiendo, asimismo, recuperar, devolver, cancelar y/o eliminar de manera inmediata y definitiva, conforme a lo antes indicado, toda información de datos personales que hubiera podido compartir y/o encargar y/o transferir.

SEPTIMO: El **ENCARGADO** únicamente podrá utilizar la información y/o cualquier dato personal proporcionado por el **TITULAR** para cumplir con el objetivo preciso, concreto y temporal del encargo que le es conferido, y bajo esa única finalidad detallada en la cláusula segunda, y siempre en pleno respeto de las estipulaciones y finalidades por las cuales de otorgó el consentimiento de los datos, de la Ley de Protección de Datos Personales y su Reglamento, y/o sus normas complementarias, modificatorias, sustitutorias y demás disposiciones aplicables, y del Código de Conducta para la protección de datos personales del **TITULAR**; nunca para otra finalidad. En tal sentido, el **ENCARGADO** queda expresamente prohibido de transferir los datos personales que el **TITULAR** le haya podido confiar para el tratamiento por encargo, bajo responsabilidad exclusiva del **ENCARGADO**, por el incumplimiento, por acción u omisión, de sus obligaciones. De esta manera, el **ENCARGADO** asegura al **TITULAR** que cuenta con las medidas de seguridad y protección técnica, organizativa y legal para el tratamiento por encargo que recibe. Toda información o datos personales que sean proporcionados al **ENCARGADO** para cumplir con el encargo que le es confiado, sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada.

OCTAVO: El **ENCARGADO** deberá asegurar el cumplimiento del presente convenio en todos los niveles de su organización, personal, trabajadores, representantes, adscritos, colaboradores, y en general, cualquier persona que pueda tener acceso a los datos personales que se confían para el tratamiento por encargo.

NOVENO: En contraprestación por los servicios de tratamiento por encargo, el **TITULAR** pagará al **ENCARGADO** una contraprestación _____.

DECIMO: El presente convenio no genera vínculo laboral alguno, beneficios sociales ni compensación alguna contemplada en las leyes laborales, entre el **TITULAR** y el **ENCARGADO** y/o sus empleados, personal, representantes, adscritos, colaboradores, y general, de cualquier persona relacionada con éstos, quienes no se encuentran bajo relación de dependencia o subordinación respecto del **TITULAR**.

DECIMO PRIMERO: El **ENCARGADO** se obliga a mantener confidencialidad absoluta sobre la celebración de este convenio, y especialmente sobre toda y cualquier información y datos que pueda manejar o recibir en mérito al mismo. Asimismo, el **ENCARGADO** se obliga a mantener absoluta confidencialidad sobre toda información comercial, operativa, financiera, legal y societaria que conozca como consecuencia del desarrollo de sus actividades; así como respecto de los usos, procedimientos, instalaciones, equipos, estrategias, estructuras, costos, mercadeo, diseños, programas, especificaciones técnicas y toda otra clase de información que él, sus operarios o personal puedan conocer, y que esté relacionada con las actividades de la organización, sistemas informáticos, procedimientos, clientes, proveedores, accionistas, empleados y ejecutivos del **TITULAR**.

Queda estrictamente prohibido al **ENCARGADO** y a sus empleados, personal, representantes, adscritos, colaboradores, y general, de cualquier persona relacionada con éstos, la reproducción, impresión o copia, parcial o total, de la información a la que tuviere acceso o conociera durante la vigencia de este convenio; asumiendo plena responsabilidad por las consecuencias que se deriven del uso indebido por parte de él o terceras personas relacionadas. En tal sentido, el **ENCARGADO** asume plena responsabilidad directa e indirecta respecto de sus propias acciones y aquellas desplegadas por sus accionistas, socios, directivos, representantes, gerentes, empleados, trabajadores, contratistas y personas vinculadas y adscritas, para el debido cumplimiento del presente convenio, debiendo tratarse los datos estrictamente para los fines temporales autorizados y precisos que constituyen el encargo, y nunca para otra finalidad, estando expresamente prohibidos de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuvieren acceso, para fines no autorizados y/o ajenos al encargo confiado , así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que se les haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno al autorizado. La obligación de confidencialidad y de protección de datos personales contenidas en este convenio subsistirá indefinidamente con fuerza y vigor aún después de terminado el vínculo contractual por cualquier causa.

Suscrito en dos ejemplares de idéntico valor legal, en Lima a los _____ días del mes de _____ del _____.

ANEXO 9

MANUAL DE ORGANIZACIÓN Y FUNCIONES PARA LA PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVO

Determinar claramente la estructura organizacional con roles y responsabilidades para liderar y hacer cumplir la política de seguridad para la protección de datos personales.

2. ALCANCE

La aplicación del presente documento involucra a todas las gerencias, áreas y personal de la organización que participe en procesos donde se realicen tratamiento de datos personales.

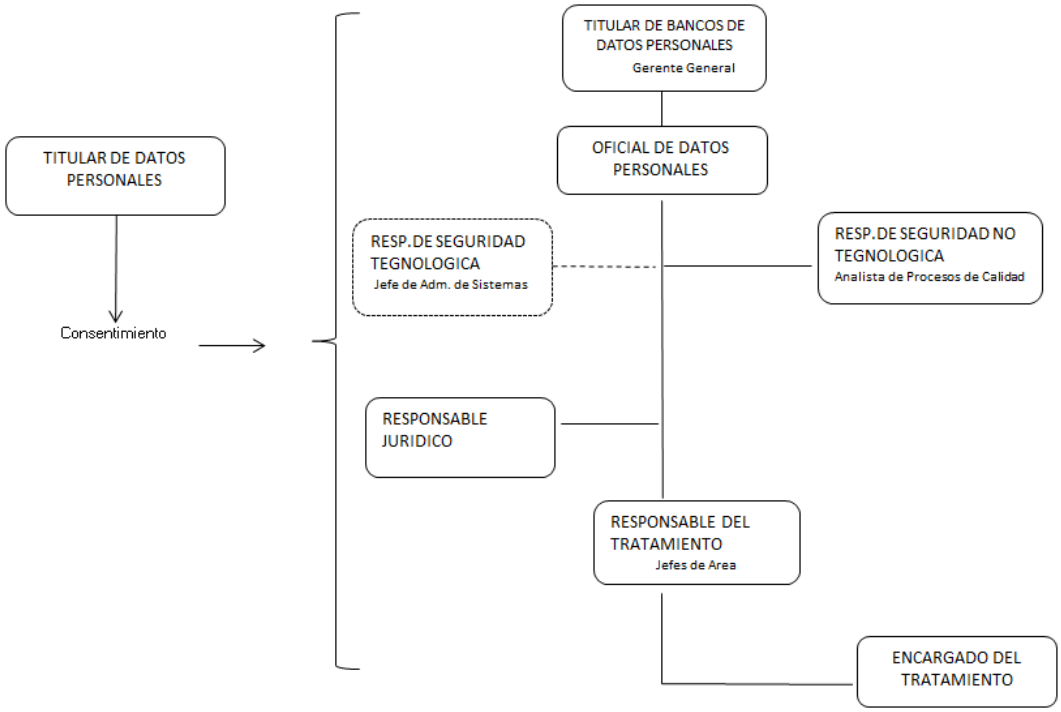
3. RESPONSABILIDADES

- Gerente General: Titular de Bancos de Datos Personales.
- Jefe de Administración de Sistemas: Responsable de Seguridad Tecnológica.
- Analista de Procesos de Calidad : Responsable de Seguridad No Tecnológica
- Contador: Responsable Jurídico.
- Jefaturas de área: Responsable del Tratamiento.
- Todo el personal que interactúa con datos personales: Encargado del Tratamiento.

4. DESARROLLO

4.1. Organización de la protección de datos personales

Los roles que componen la estructura organizacional para la protección de datos personales está dada según el siguiente esquema:



4.2. Responsabilidades y funciones

En términos generales todo el personal de la empresa está obligado a cumplir con la Política de Protección de Datos Personales, manteniendo la observancia y cumplimiento a nivel ético, contractual y legal de las estipulaciones dadas.

De forma particular, los roles definidos dentro de la estructura organizacional deben de cumplir mínimamente las funciones que se detallarán más adelante.

Todos los actores de la organización de la protección de datos personales son pasibles de las sanciones que se definan de acuerdo a la gravedad del incumplimiento del que sean protagonistas y en función de los resultados de las investigaciones y/o pericias pertinentes:

4.2.1. Titular del Banco de Datos Personales:

El rol lo asume el Gerente General, como representante legal, quien en relación a la protección de datos personales tiene las siguientes funciones:

- Asegurar que se obtenga el consentimiento del titular de los datos personales para realizar su tratamiento.
- Identificar los bancos de datos personales que se manejan en la empresa, así como los datos personales que contendrán.
- Determinar el tipo de tratamiento que se dará a los datos personales, así como el tiempo y finalidad del mismo.
- Solicitar ante la Dirección Nacional de PDP la inscripción, modificación y cancelación, de ser el caso, de los bancos de datos personales de la empresa.
- Determinar las medidas de seguridad que garanticen la protección de los datos personales incluidos en los bancos de datos.
- Garantizar la aplicación de los principios rectores normados por la LPDP.
- Asegurar que el personal involucrado en el tratamiento de datos personales conoce las implicancias de la ley, así como su aplicación en la organización.
- Velar por el cumplimiento, dentro de lo legal, de la inscripción de la transferencia de datos, que se dé lugar producto de las operaciones con otras entidades
- Otorgar todas las facilidades para la atención de los derechos ARCO.
- Responsable y encargado de implementar, ejecutar, y dar cumplimiento de la política de protección de datos personales en todos sus niveles, a nivel transversal y como autoridad máxima dentro de la empresa.

4.2.2. Responsable de Seguridad Tecnológica

El rol es asignado al Jefe de Administración de Sistemas y que dentro de lo relacionado a la PDP tiene las siguientes funciones:

- Implementar las medidas de seguridad necesarias en las redes e infraestructura informática y digital que intervengan en el tratamiento de datos personales.
- Implementar las medidas de seguridad en las aplicaciones informáticas y digitales donde se da tratamiento a los datos personales.

- Asegurar que los servicios tecnológicos que se prestan y reciben cumplan con todos los requisitos que establece la LPDP.

- Gestionar de forma activa, la mejora continua en las medidas de seguridad implementadas.

- Garantizar que el proveedor de servicios tecnológicos mantenga el secreto profesional correspondiente a los datos personales que maneja.

- Administrar los accesos y privilegios a los sistemas, así como su verificación y fiscalización.

- Abrir, llevar y controlar los registros de documentos, de personal con accesos, de incidentes y medidas adoptadas, de los accesos concedidos y sus variaciones, a nivel informático y digital.

- Asegurar que toda la documentación relacionada con la protección de datos personales publicada en las plataformas virtuales esté vigente y disponible para los usuarios.

4.2.3. Analista de Procesos de Calidad

El rol es asignado al Analista de Procesos de Calidad , quien dentro de lo relacionado a la PDP tiene las siguientes funciones:

- Encargarse de la identificación de los bancos de datos personales, así como de su registro, modificación, control y/o cancelación ante la Dirección Nacional de PDP.

- Implementar las Medidas de Seguridad Organizativas, Jurídicas y Técnicas requeridas por la LPDP, con el apoyo de la Gerencia de Sistemas y Procesos.

- Elaborar los documentos, procedimientos y registros, relacionados con las medidas de seguridad implementadas en todo nivel.

- Validar que se estén ejecutando adecuadamente las medidas de seguridad implementadas, e informar a la Gerencia General de los resultados.

- Promover un ciclo de mejora continua en el sistema de protección de datos personales implementado.

- Mantener informado al Gerente acerca de las incidencias y el cumplimiento de la Ley 29733, Ley de Protección de Datos Personales.

- Abrir, llevar, controlar y fiscalizar los registros de documentos no automatizados, de personal con accesos, de incidentes y medidas adoptadas, de los accesos concedidos y sus variaciones, de auditorías, y de otros que pudieran abrirse.

4.2.4. Responsable Jurídico

El rol recae en el Contador, quien deberá coordinar con los asesores legales de la organización para cumplir con las siguientes funciones relacionadas a la PDP:

- Realizar la adecuación y/o modificación de las cláusulas de contratos, acuerdos y todo documento que esté relacionado con el tratamiento de datos personales.

- Apoyar y asesorar en la estructuración de los formatos de consentimiento.

- Atender, analizar y difundir las notificaciones que emita la APDP.

- Realizar los trámites o gestiones que se deban realizar ante la APDP.

- Resolver las solicitudes de derechos ARCO que merezcan una respuesta desde el enfoque legal.
- Acompañar a las comisiones de fiscalización que envíe la APDP.
- Estar actualizado respecto a las disposiciones o modificaciones de la Ley 29733, así como comunicarlas oportunamente al personal involucrado.
- Manejar los casos de negativa del titular de datos personales a brindar su consentimiento de tratamiento, para evitar perjudicar la relación comercial.
- Realizar las auditorías y verificaciones periódicas respecto del cumplimiento de las normas legales y la política de protección de datos personales.
- Gestionar las capacitaciones.

4.2.5. Responsable del Tratamiento

Está representado por los Jefes de las diferentes áreas en que se realice tratamiento de datos personales y cuyas funciones en el ámbito de la PDP son las siguientes:

- Participar de las decisiones acerca del tratamiento de datos personales y controlar que el tratamiento sea debido y apropiado.
- Asegurar la aplicación de la finalidad de tratamiento del banco de datos personales definida por la organización.
- Gestionar operativamente el consentimiento por parte de los titulares de datos personales para su tratamiento.
- Mantener los registros que evidencien el otorgamiento de consentimiento por parte de los titulares de datos personales.
- Comunicar a las terceras partes (proveedores), cuando fuera el caso, las condiciones de tratamiento de datos que le sea encargado.
- Aplicar el secreto profesional a los datos personales a los que se le haya autorizado tener acceso.
- Velar por el cumplimiento de los principios rectores de la LPDP.

4.2.6. Encargado del Tratamiento

Está representado por todo el personal a nivel operativo que participe del tratamiento de datos personales y cuyas funciones en el ámbito de la PDP son las siguientes:

- Velar en todo momento por la seguridad de los datos personales.
- Cumplir con los principios rectores de la LPDP.
- Obtener el consentimiento desde los medios no automatizados que sean puestos a su disposición para tal fin.
- Aplicar el secreto profesional a los datos personales a los que se le haya autorizado tener acceso.
- Velar por el cumplimiento y otorgamiento de los derechos de los titulares de datos personales.

4.3. Titular de Datos Personales

Es responsable de sus propios datos personales, debe tomar en cuenta que su consentimiento debe ser libre, previo e informado, así como validar que sea registrado en los términos en que expresa e inequívocamente lo ha dado.

Es responsable de conocer y ejercer los derechos conferidos por la LPDP.

5. CONTROL DE CAMBIOS

N° de Revisión	Fecha	Motivo
03	21/03/2025	Formalización del Manual de Organización y Funciones en la Protección de Datos Personales

ANEXO 10.1

POLITICAS O LINEAMIENTOS PARA LA PROTECCION DE DATOS PERSONALES

1. OBJETIVO

Establecer el mandato y el compromiso de la alta dirección y de toda la organización con relación al cumplimiento de los lineamientos de la Ley 29733 – Ley de Protección de Datos Personales.

2. ALCANCE

La aplicación del presente documento involucra a todas las gerencias, áreas y personal de la organización que participe en procesos donde se realicen tratamiento de datos personales.

3. DEFINICIONES

- PDP: Abreviatura para el término "Protección de Datos Personales".
- LPDP: Abreviatura para referirnos a la Ley 29733 – Ley de Protección de Datos Personales.

4. CONDICIONES GENERALES

En todas las sucursales y/o locales comerciales se deberá exhibir de forma visible el enunciado de la Política Rectora de Protección de Datos Personales. Ver Anexo 1.

5. DESARROLLO

En función del cumplimiento obligatorio de la LPDP y existiendo el total compromiso de la Alta Dirección, se establece el cumplimiento de los siguientes lineamientos y compromisos:

5.1. Lineamientos generales para el cumplimiento de la política:

a. Establecer la organización de PDP en la que se detallen las responsabilidades de los actores, con la finalidad de dar cumplimiento a la LPDP aplicando los lineamientos de la presente Política de Protección de Datos Personales.

b. Es obligatorio el cumplimiento, por parte de todos los actores en el tratamiento de datos personales, de los principios rectores de LPDP.

c. En cumplimiento del principio de legalidad, se prohíbe la recopilación de datos personales por medios fraudulentos, desleales o ilícitos; solo debe realizarse por los medios que la empresa establece para sus procesos y que se rigen de este principio.

d. En cumplimiento con el principio de consentimiento, para el tratamiento de los datos personales, debe mediar obligatoriamente el consentimiento del titular de manera libre, previa, expresa, informada e inequívoca.

e. Se prohíbe el uso de fórmulas de consentimiento en la que se requiera presumir o asumir la existencia de una voluntad que no ha sido expresa.

f. En cumplimiento del principio de finalidad, se establece el tratamiento de datos personales solo y exclusivamente para la finalidad que da motivo a la recopilación de datos personales, se prohíbe el tratamiento de datos personales para otras finalidades.

g. Todo cambio en la finalidad debe ser informado oportuno y comunicado al titular de datos personales.

h. Todos los procesos de la empresa están obligados al cumplimiento de medidas de seguridad para la protección de datos personales.

i. Toda finalidad de negocio para el tratamiento de datos personales debe ser expresada con claridad, sin dar lugar a confusión y ser objetiva respecto del objeto que tendrá el tratamiento de los datos personales.

j. Todo colaborador o tercero, encargado de un banco de datos personales, que realice el tratamiento de algún banco de datos personales, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional.

k. En cumplimiento del principio de proporcionalidad, el tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados, además los datos personales que se recaben deben ser estrictamente los necesarios para las finalidades consentidas.

l. En cumplimiento del principio de calidad, todos los datos personales, tratados en la empresa, deben ser exactos, ajustarse con precisión a la realidad, y en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto a la finalidad para las que fueron recopilados.

m. Será de presunción que los datos personales directamente facilitados por su titular son exactos.

n. En cumplimiento del principio de seguridad, todo titular de bancos de datos personales y las partes externas a las que asigne por encargo su tratamiento, deben adoptar medidas de seguridad apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

o. En cumplimiento del principio de disposición de recursos, todos los procesos de la empresa, deben adoptar y brindar a los titulares de datos personales las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos cuando estos sean vulnerados por el tratamiento de sus datos personales.

p. En cumplimiento del principio de nivel de protección adecuado, referido al flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar, al menos en un nivel equiparable a lo previsto por la LPDP.

q. Respeto de los principios rectores de la LPDP:

- Principio de legalidad.
- Principio de consentimiento.
- Principio de finalidad.
- Principio de proporcionalidad.
- Principio de calidad.
- Principio de disposición de recurso.
- Principio de nivel de protección adecuado.

5.2. Lineamientos operativos para el registro de información en el sistema:

a. En cumplimiento al principio de calidad, los datos personales registrados en el sistema por parte de los encargados de tratamiento de datos personales, que se encargan de recopilar información, deben ser exactos y ajustarse con precisión a la realidad.

b. Los datos personales previamente ya recopilados, deben ser actualizados de manera periódica, con el objetivo de tener la información actualizada del cliente.

c. Los datos personales solo deben ser recopilados en los sistemas de información autorizados y de acuerdo a las finalidades consentidas previamente.

d. Los datos personales que sean registrados en el sistema, deben ser autorizados por el Titular de Banco de Datos, no se deberán registrar información adicional a la autorizada.

5.3. Lineamientos operativos para la protección de los datos personales ante falsificaciones o sustitución de documentos fidedignos:

a. Los repositorios físicos que almacenen datos personales deben contar con las suficientes medidas de seguridad.

b. Los repositorios físicos que se encuentran en mal estado, deben ser reportados inmediatamente.

c. Se debe reportar el acceso no autorizado de alguna persona ajena al área.

d. Se debe reportar indicios de sustituciones o falsificación de datos personales al responsable de banco de datos.

e. Sobre los escritorios se debe contar solamente con información de datos personales necesarias para poder realizar las labores en dicho periodo, de lo contrario debe encontrarse resguardo en un lugar seguro.

f. En los repositorios físicos de información debe ser publicado "El Enunciado de la Política de Protección de Datos Personales".

5.4. Lineamientos operativos sobre la protección de base de datos personales:

a. En cumplimiento del principio de legalidad, se prohíbe el uso de bases de datos personales de origen fraudulento, desleal e ilícito.

b. Las bases de datos personales solo pueden ser proporcionados por el Jefe Inmediato o Colaborador autorizado para proporcionar dicha información.

c. Las bases externas proporcionadas o accesos a los sistemas en las que se gestionen datos personales, son de uso estrictamente personal, no deberán ser compartidos si no se tiene consentimiento del colaborador responsable de compartirlo.

d. La adquisión de bases de datos, para el cumplimiento de los objetivos empresariales, debe estar celebrada a través de un contrato que comprenda cláusulas donde la empresa proveedora, se encuentre comprometida y alienada a la LPDP.

e. Las Bases de Datos personales, deben ser protegidas a través de dispositivos físicos o lógicos, que permitan su fácil accesibilidad.

f. La adquisición de bases de datos, para el cumplimiento de los objetivos empresariales, deberán estar acompañados con un convenio de transferencia de datos personales, en la cual la empresa proveedora haya cumplido con lo establecido en la Ley.

g. Las bases de Datos de Acceso Público deberán ser usadas de acuerdo a las finalidades para las que fueron creadas.

5.5. Lineamientos operativos para el uso de equipos de cómputo:

a. En caso de ausentarse de la posición de trabajo, deberá bloquear para evitar actos maliciosos (robos de información, alteración de información, etc.).

b. Se debe informar a la jefatura del área en caso de encontrar un equipo que no se encuentre desbloqueado, por un tiempo prolongado.

c. Los usuarios deben resguardar su contraseña con la mayor confiabilidad, para evitar el ingreso por terceros que puedan ejecutar acciones maliciosas, que podría involucrar el acceso a la información.

d. Los equipos de cómputo debe estar asegurados con sus respectivos dispositivos de seguridad para poder ser utilizados.

5.6. Lineamientos operativos para la custodia de los dispositivos de reproducción:

a. Los equipo de reproducción como fotocopiadoras, multifuncionales, escáneres, deben ser vigilados en el momento de ejecutar las tareas de reproducción.

b. La información con datos personales ubicados en las bandejas o lugares próximos a estos, debe ser trasladados de manera inmediata a sus respectivos depósitos de repositorios de información.

c. En caso de encontrar documentos desatendidos en las bandejas o próximos a estos equipos, los colaboradores deben informar inmediatamente al personal a cargo de dicho equipo de reproducción, sobre la existencia de dichos documentos.

d. En caso de no haber suministros para los dispositivos reproducción, las impresiones deben ser canceladas inmediatamente, para evitar que sean reproducidas.

e. En caso de encontrarse dispositivos de almacenamiento desatendidos conectados o próximos a dichos equipos, los colaboradores deben trasladar dichos dispositivos al personal a cargo del dispositivo de reproducción.

5.7. Compromiso de cumplimiento de los requisitos de seguridad de la LPDP

Compromiso para cumplir los requisitos de seguridad Organizativos, Jurídicos y Técnicos dados por la Directiva de Seguridad de la Información de la LPDP, de aquellas que se adopten de estándares de seguridad de la información y que sean aplicables a la categoría de banco de datos personales de los que se es titular.

5.8. Compromiso de mejora continua

Compromiso para mantener la protección de datos personales dentro del ciclo de mejora continua, mediante la planificación, operación, medición y mejora de las medidas de seguridad organizativa, jurídica y técnicas que sean implementadas en función de la categoría de los bancos de datos personales de los que la empresa es titular.

5.9. Responsabilidad de la organización de PDP

Es responsabilidad y obligación de todos Responsables de Tratamiento, Encargados de Tratamiento y Encargados de Bancos de Datos Personales, el cumplir con la Política de Protección de Datos Personales, Lineamientos y compromisos con los requisitos de seguridad, con el respeto a los principio de la LPDP y de mejora continua, a través de acciones coherentes y conformes con dicha Ley, además de trabajar con la ética ante el otorgamiento de los derechos de acceso, rectificación, cancelación o supresión y oposición de los Titulares de los Datos Personales, así como de guardar la confidencialidad de los datos personales con la debida observancia del Secreto Profesional que la LPDP demanda.

6. CONTROL DE CAMBIOS

N° de Revisión	Fecha	Motivo

ANEXO 10.2
MANUAL DE SEGURIDAD DE LA INFORMACIÓN DE LOS BANCOS DE DATOS PERSONALES

1. OBJETIVO

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales de la organización.

Cumplir con la función de **Documento Maestro de Seguridad de la Información** de los Bancos de Datos Personales que se gestionan en la organización.

2. ALCANCE

La aplicación del presente documento involucra a todas las gerencias, áreas, personal y procesos donde se realicen tratamiento de datos personales.

3. DEFINICIONES

En el Anexo A: Glosario de términos relacionado a la PDP, se detallan las definiciones necesarias para la correcta comprensión del presente documento, así como otra documentación relacionada a la Protección de Datos Personales.

4. DOCUMENTOS A CONSULTAR

- Ley 29733 – Ley de Protección de Datos Personales.
- Reglamento de la Ley 29733 – Ley de Protección de Datos Personales.
- Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales.

5. RESPONSABILIDADES

Las responsabilidades se detallan en el documento “Manual de Organización y Funciones en la Protección de Datos Personales”.

6. CONDICIONES GENERALES

La Política de Protección de Datos Personales es el marco general y el compromiso de la Alta Dirección de la organización respecto a la Seguridad de la Información de los Bancos de Datos.

En ese sentido, se deben cumplir las siguientes condiciones de seguridad:

6.1. Condiciones de seguridad externas

6.1.1. Como marco legal para la protección de datos personales, se tiene la LPDP, y su reglamento.

6.1.2. El conocimiento y conciencia acerca de la importancia de la protección de datos personales, la Ley 29733 y su reglamento, son abordados en el Plan de Capacitación y Sensibilización de la LPDP. Es responsabilidad de la Gerencia General velar por el cumplimiento del plan, en conjunto con la Gerencia de Gestión y Desarrollo Humano:

6.2. Condiciones de seguridad internas

6.2.1. La Alta Dirección se compromete a brindar todos los recursos necesarios y la dirección activa en la protección de los datos personales contenidos y destinados a ser contenidos en los bancos de datos personales de los que como persona jurídica de derecho privado es titular.

Así mismo, en la Política de Protección de Datos Personales, se encuentra establecido el compromiso con el cumplimiento de la LPDP y su reglamento mediante las acciones de mejora continua y el respeto a los principios rectores de la Ley.

6.2.2. La Alta Dirección comprende el contexto institucional de la empresa, como titular de banco de datos personales, en el que se tratan datos personales dentro del marco de las actividades propias del rubro automotriz.

En este sentido, el contexto de la organización se evidencia de acuerdo a los siguientes documentos que contienen la información clara para su comprensión:

- Análisis de Brechas de Cumplimiento de la LPDP.
- Manual de Organización y Funciones.
- Mapa de Procesos.
- Políticas
- Procedimientos.

6.2.3. La organización y sus responsabilidades están establecidas en el Manual de Organización y Funciones en la Protección de Datos Personales; en el que se enuncia la responsabilidad de cada actor dentro de la protección de datos personales y en especial del Responsable de Seguridad de la información, a quien se le deben otorgar todas las facultades, recursos y autoridad para liderar y hacer cumplir la Política de Protección de Datos Personales.

6.2.4. Los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales se mantienen dentro de un enfoque de gestión de riesgos en concordancia con la Metodología de Gestión de Riesgos de Privacidad de Datos Personales.

En esta metodología, se consideran los riesgos latentes que pueden afectar a los bancos de datos personales y en consecuencia provocar impacto tanto a los titulares de datos personales como a la empresa.

7. DESARROLLO

7.1. Requisitos de Seguridad

7.1.1. Mediante la Política de Protección de Datos Personales, se da cumplimiento al requisito 1.3.1.1 de la Directiva de Seguridad de la Información de la LPDP y su complemento aplicable 1.4.1; teniéndose detallados y cumplidos todos los aspectos y características requeridas.

7.1.2. La gobernabilidad de los procesos involucrados en el tratamiento de los datos personales debe darse mediante las siguientes actividades preliminares básicas para el entendimiento que deben ser lideradas por los Responsables de la Seguridad de los Bancos de Datos Personales:

- Identificación del flujo de los datos personales.
- Identificación de los procesos en los que se tratan datos personales.
- Identificación de los responsables y Encargados de Tratamiento.
- Identificación de los encargados de los bancos de datos personales o terceras partes que acceden a los bancos de datos personales.
- Aplicar, con la debida aprobación por parte de la Alta Dirección, la Política de Protección de Datos Personales con la finalidad de que se cumplan sus lineamientos en toda la organización.
- Aplicar lo establecido en las medidas organizativas a fin empoderar a los Responsables de Seguridad en sus funciones como voz autorizada sobre la seguridad de los bancos de datos personales.
- Aplicar lo establecido en las medidas organizativas a fin de asignar las responsabilidades allí detalladas a todos los actores de los procesos en los que se tratan datos personales, con la

finalidad de que las asuman y tengan la potestad de decidir en forma controlada sobre los bancos de datos personales que les corresponda.

7.1.3. Las medidas de seguridad para la protección de datos personales a ser implementadas se detallan en las secciones 7.3, 7.4 y 7.5: Medidas Organizativas, Medidas Jurídicas y Medidas Técnicas respectivamente, del presente documento.

7.1.4. De acuerdo al requisito de seguridad 1.3.1.4 de la Directiva de Seguridad y en forma equivalente a lo sugerido en el punto 1.4.4 de la información complementaria sobre los requisitos, en nuestra organización se mantiene la seguridad de los datos personales dentro del marco de un Sistema de Protección de Datos Personales (SPDP) que se desenvuelve dentro de un ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar), el cual se ilustra en el Gráfico N°01.

7.1.5. Rige para la protección de los bancos de datos personales los siguientes procedimientos documentados:

- Procedimiento de Gestión de Documentos.
- Procedimiento para Brindar Accesos al Sistema y Recursos Informáticos.
- La Política de Control de Accesos establece las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garantizan la seguridad del tratamiento de los datos personales.
- La Gerencia de Sistemas y Procesos debe mantener un Registro de Control de Acceso que se encuentre debidamente documentado en un procedimiento y que contemple lo siguiente:
  - La gestión de acceso desde el registro de un usuario.
  - La identificación de un usuario.
  - La gestión de los privilegios del usuario.
  - La identificación del usuario ante el sistema.
  - Registro de la revisión periódica de los privilegios asignados.
- Para fines de trazabilidad la Gerencia de Sistemas y Procesos, debe contar con el Registro de Accesos a Bancos de Datos Personales que provea evidencias sobre las interacciones de los Encargados de Tratamiento con los datos lógicos.
- En la medida de seguridad técnica 12.1.1.6, se detallan los campos mínimos que debe contener el Registro de Accesos a Bancos de Datos Personales.
- Los registros deben ser legibles, oportunos y tener un procedimiento de disposición que debe ser elaborado por los responsables de los Bancos de Datos, entre los que se encuentran el destino de los registros, una vez que estos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros que puedan realizarse.
- Procedimiento de Auditoría de LPDP que incluye los registros de auditoría del SGSI que contempla dentro de su alcance la Seguridad de los Bancos de Datos Personales.
- Procedimiento de Gestión de Incidentes y Problemas que incluye el correspondiente registro de incidentes y problemas del SGSI; el SGSI contempla dentro de su alcance la Seguridad de los Bancos de Datos Personales.

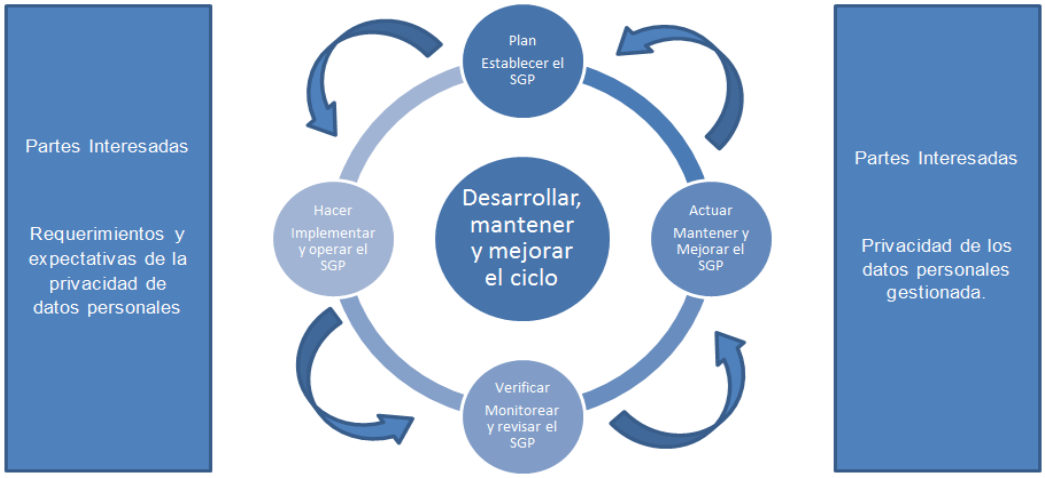


Gráfico N° 01 – Ciclo de Mejora Continua del Sistema de Gestión de la Privacidad

7.1.6. Enfoque de riesgos de la protección de datos personales. La organización cuenta con un enfoque de riesgos de privacidad de datos personales que comprende lo siguiente:

- Los datos personales se mantienen dentro de medios específicos, que son los bancos de datos personales, los mismos que a su vez son procesados por sistemas cuando son automatizados o procesados en forma manual cuando son no automatizados, en dicho sentido existe co-relación entre activos de información siendo los datos personales activos de información primarios que heredan su valor de importancia a los activos de apoyo que los contengan.
- Se establece que debe considerarse en la evaluación de riesgo de datos personales el análisis de impacto en la privacidad, los criterios correspondientes se encuentran definidos en la Metodología de Gestión de Riesgos que es de aplicación en todos los casos en que se evalúen riesgos a la privacidad de los datos personales y los medios en que éstos son tratados.
- El resultado del análisis de impacto en la privacidad debe ser considerado dentro del cálculo del valor real de riesgo a la privacidad de los datos personales.
- El valor real de riesgo de privacidad de datos personales, que comprometa a los bancos de datos personales, que se obtenga y que resulten no aceptables de acuerdo al apetito de riesgo de seguridad de la información; deben ser tratados de acuerdo a lo que se establezca en el Plan de Tratamiento de Riesgos de la organización. en base al cual se establecerán las decisiones sobre acciones a tomar que corresponda a cada tipo de riesgo identificado.

7.1.7. El presente manual, al representar el Documento Maestro de Seguridad de la Información del Banco de Datos Personales de la organización debe ser mantenido e incluido en el ciclo de mejora continua del SPDP, en el que se contemplan las revisiones periódicas por parte de la dirección y las auditorías internas correspondientes a los puntos que establezca en concordancia con el SPDP.

Este documento es de responsabilidad del Gerente General, quien lo utilizará en calidad de guía para la implementación y mantenimiento de la protección de los datos personales.

7.1.8. Todo personal de la organización que esté relacionado con el tratamiento de datos personales debe firmar un Compromiso de Confidencialidad en el tratamiento de datos personales en señal de conformidad y aceptación.

El compromiso de confidencialidad, obliga al personal firmante a guardar la confidencialidad de los datos personales y de sus antecedentes, esta obligación subsiste aun después de finalizadas las relaciones con la empresa.

El obligado puede ser relevado de la obligación de confidencialidad si se da cualquiera de los casos que indica el artículo 17 de la Ley N°29733.

7.2. Disposiciones Específicas de Seguridad

7.2.1. Para el tratamiento de los bancos de datos personales se implementan los controles adecuados de la Directiva de Seguridad emitida por la APDP y desarrollado dentro de un Marco de Privacidad de acuerdo a lo indicado en las secciones 7.3, 7.4 y 7.5: Medidas Organizativas, Medidas Jurídicas y Medidas Técnicas respectivamente, del presente documento.

7.2.2. Se ha designado dos responsables de seguridad de los bancos de datos personales, uno para la seguridad tecnológica y otro para la seguridad no tecnológica; quienes coordinarán la aplicación de las medidas de seguridad.

7.2.3. Los registros y documentos que evidencian el cumplimiento o que forman parte de las medidas de seguridad de datos personales que sean implementadas pueden estar en cualquier formato o tipo de medio de información.

7.2.4. Todos los bancos de datos personales existentes deben ser limitados a los datos que sean estrictamente necesarios para cumplir con la finalidad para la cual fueron recabados.

7.2.5. En todos los casos en los que sea pertinente y no se requiera del detalle de los datos personales se deben aplicar mecanismos de anonimización o disociación de acuerdo con las facilidades técnicas existentes.

7.3. Medidas de Seguridad Organizativas

La implementación de las medidas organizativas es de responsabilidad del Directorio, quien tiene que aprobar y apoyar la estructura organizacional de la protección de datos personales; y, en forma operativa, es responsabilidad de la Gerencia General que debe disponer de los recursos necesarios para llevar a cabo la implementación**.**

7.3.1. Organización de la protección de datos personales

La Estructura Organizacional, los roles y responsabilidades respecto de la protección de datos personales están definidos de acuerdo con el Gráfico N°02.

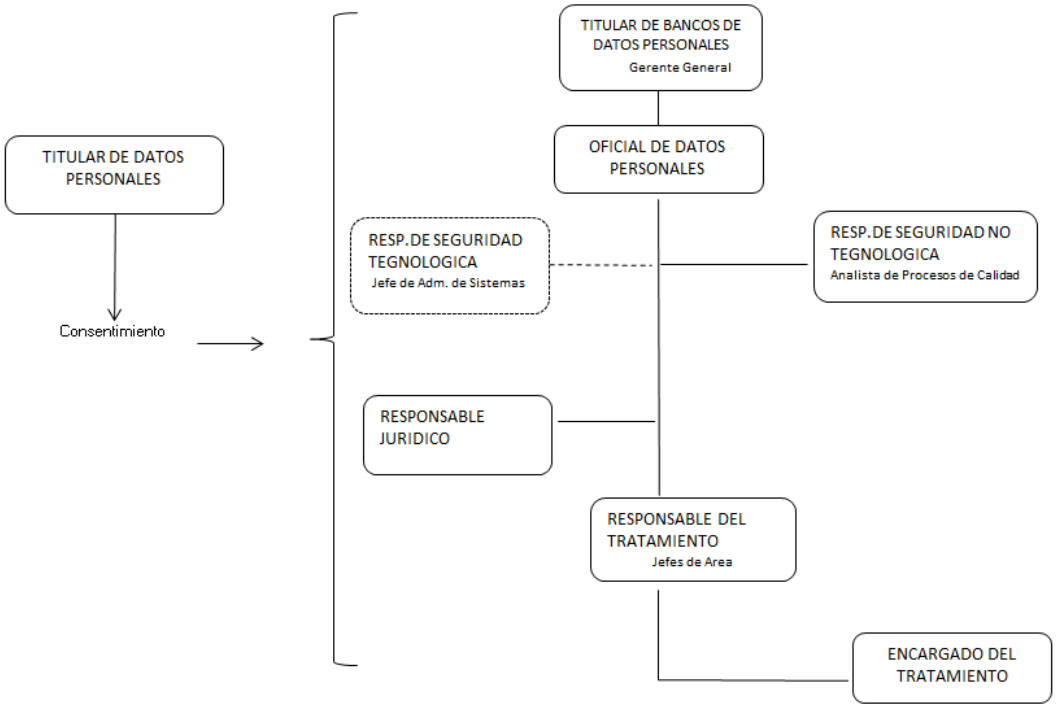


Grafico N° 02 – Organización de la Protección de Datos Personales

7.3.2. Responsabilidades

Las funciones de cada uno de los roles definidos están detalladas en el Manual de Organización y Funciones en la Protección de Datos Personales.

7.3.3. La Política de Protección de Datos Personales

Es donde se establece el compromiso de la Alta Dirección y de toda la organización de la empresa con el respeto a los principios rectores de la LPDP.

Debe estar debidamente entendida y aceptada por todos los colaboradores y debe estar archivada por el Responsable de Seguridad No Tecnológica.

7.3.4. Es responsabilidad de la Gerencia y Responsable Jurídico, de realizar todos los trámites ante la APDP que correspondan a los bancos de datos de titularidad de la empresa y de atender todas las solicitudes y denuncias que puedan emitir los titulares de datos personales.

7.3.5. Todo banco de datos personales que sea creado en la empresa debe ser inscrito ante la ANPDP de manera previa a su puesta en producción y a la recopilación de datos.

7.3.6. El Gerente de Contraloría y Procesos debe realizar la revisión de los formularios de inscripción de bancos de datos provistos por las Gerencias de la empresa.

7.3.7. Es responsabilidad de cada Gerencia, proporcionar a la Gerencia de Contraloría y Procesos el formulario de inscripción de bancos de datos personales debidamente llenado para su validación y posterior inscripción por parte del Responsable Jurídico ante la APDP.

7.3.8. La descripción del llenado del formulario de inscripción se encuentra en el Título IV ¿Cómo completar el formulario? de la Guía de Inscripción de Bancos de Datos Personales que se encuentra publicada en la página web del MINJUS:

7.3.9. Los procesos de modificación y cancelación de bancos de datos personales que hayan sido inscritos ante la APDP deben ser reportados por cada Gerencia al Gerente de Contraloría y Procesos a través del llenado de los siguientes formularios:

- Formulario de modificación de banco de datos personales.
- Formulario de cancelación de banco de datos personales.

7.3.10. Los Responsables de Seguridad Tecnológica y No Tecnológica deben mantener y compartir un control y registro de los operadores con acceso a cada banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento que se requiera realizar la trazabilidad.

7.3.11. Los Responsables de Seguridad Tecnológica y No Tecnológica deben revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales (si es lógico, en el servidor; y, si es físico, en el contenedor de documentos).

- La medida de seguridad debe ser identificada de acuerdo con una bitácora que deben mantener y administrar los Responsables de Seguridad Tecnológica y No Tecnológica.
- El nivel de efectividad puede ser bajo, medio y alto.

7.3.12. Toda aplicación de tratamiento de datos personales debe ser adaptada mediante la configuración de accesos y perfiles acordes a los cargos, el desarrollo de mecanismos de seguridad en el acceso y en la transferencia de datos personales; esta actividad es responsabilidad de la Gerencia de Sistemas y Procesos cuya implementación debe ser monitoreada por el Responsable de Seguridad Tecnológica.

7.3.13. Todos los procesos de negocio involucrados en el tratamiento de datos personales deben adecuarse al cumplimiento de la LPDP contemplando:

- Implementación de procesos administrativos suficientes, en todas las gerencias de negocio, para brindar acceso a los derechos ARCO y al derecho de acceso a la información a los titulares de datos personales; en esta implementación deben intervenir todas las gerencias a las se canaliza las solicitudes de los Titulares de Datos Personales.
- En complemento al párrafo anterior, se deben establecer los tiempos de atención de los procesos que estén comprendidos en el acceso a los derechos ARCO y los derechos de acceso a la información por parte de los titulares de datos personales de acuerdo a lo estipulado en el reglamento de la LPDP.
- Es responsabilidad de la Gerencia General, velar por la publicación, en los medios telemáticos de recopilación de datos personales, de las políticas de privacidad.
- Se debe implementar un canal de autorización de creación de nuevos bancos de datos personales; estos deben tener el Visto Bueno por la Gerencia de Contraloría y Procesos previo a su lanzamiento y a la recopilación de datos personales.
- Todos los colaboradores identificados como Responsables de Tratamiento y Encargados de Tratamiento de datos personales de todos los niveles de la organización deben asumir sus responsabilidades respecto de la protección de datos personales, para ello, deben participar activamente en las actividades de capacitación y concienciación de la LPDP.
- Todas las gerencias de la empresa deben tener definidos los procesos de obtención de consentimiento de datos personales al momento de recabarlos en cualquiera de los procesos de la empresa según sea el caso y siempre con la observancia de las características de consentimiento indicadas en el reglamento de la LPDP.
- Si los datos personales son recogidos en línea a través de redes de comunicaciones

electrónicas, se debe publicar una política de privacidad, que debe ser fácilmente accesible e identificable por los usuarios, esto sin perjuicio de la obtención obligatoria del consentimiento de tratamiento.

7.3.14. Todas las Gerencias que traten datos personales deben mantener documentados sus procedimientos para el tratamiento de datos personales, al mismo tiempo estos deben ser anexados al Documento Maestro de Seguridad de la Información de los Bancos de Datos Personales.

7.3.15. El Gerente de Contraloría y Procesos es responsable de elaborar el programa de creación de conciencia y entrenamiento en materia de protección de datos.

7.3.16. La empresa cuenta con un Procedimiento de Auditoría Interna que contempla en su alcance a los bancos de datos personales y como referencia las medidas de seguridad de la Directiva de Seguridad de la Información de la LPDP, este procedimiento debe ser aplicado en forma periódica por la Gerencia de Contraloría.

7.3.17. La empresa debe Gestionar los de Incidentes y Problemas que afecten a la confidencialidad, integridad y disponibilidad de los bancos de datos personales, debe ser de aplicación permanente por parte de todos los colaboradores de las gerencias adjuntas y atendido por los responsables de seguridad, dependiendo de su ámbito de alcance.

7.3.18. La asignación de privilegios de acceso a los aplicativos de la empresa en los que se tratan datos personales se da mediante los lineamientos y actividades establecidos en el Procedimiento de Administración de Accesos.

7.4. Medidas de Seguridad Jurídicas

La implementación de las medidas Jurídicas, son de responsabilidad exclusiva del Responsable Jurídico de la empresa, la Gerencia debe disponer de los recursos necesarios para su cumplimiento**.**

7.4.1. Todas las gerencias son responsables de implementar los consentimientos por cada banco de datos y que estén de acuerdo con la finalidad de la recopilación de los datos personales, estos formatos deben contener las características de consentimiento, libre, previo, expreso, inequívoco e informado que pide la LPDP y su reglamento.

Las gerencias deben valerse del apoyo del Responsable Jurídico para elaborar sus formatos de consentimiento adecuados de manera específica para los bancos de datos que traten en sus procesos de recopilación de datos personales

7.4.2. El Responsable Jurídico debe asistir a la GDH en la elaboración de cláusulas para la contratación de colaboradores, en especial para aquellos que estén destinados a ocupar cargos relacionados con el tratamiento de datos personales, que contemple cláusulas de compromiso con la protección de datos personales y las medidas correctivas que correspondan y a los que se rige todo colaborador a través de la comprensión y aceptación del Reglamento Interno de Trabajo (RIT).

En forma seguida, GDH debe recabar la firma del compromiso de confidencialidad en el tratamiento de datos personales cuyo tenor debe estar acorde a la obligación de guardar confidencialidad respecto de los bancos de datos personales y de sus antecedentes.

7.4.3. Al igual que con los contratos de los colaboradores, el Responsable Jurídico debe asistir a la GDH en la elaboración de los contratos para la contratación de terceros que contemple cláusulas de compromiso con la protección de datos personales, con la confidencialidad de los datos personales y sus antecedentes, y las medidas correctivas que correspondan de acuerdo a las leyes vigentes.

Debe regir así mismo, en los contratos con terceros, que la obligación de mantener la confidencialidad sobre los datos personales subsiste aún después de finalizada la relación contractual con la empresa

avalado por el Artículo 17 de la Ley 29733.

7.5. Medidas de Seguridad Técnicas

7.5.1. Relacionadas al acceso no autorizado al Banco de Datos Personales

A. Gestión de contraseñas cuando el tratamiento se realice con medios informáticos.

Mediante los siguientes lineamientos se controla la asignación y el uso de las contraseñas de los usuarios de los sistemas de información incluyendo aquellos que realizan tratamiento de datos personales, estos documentos normativos incluyen:

- Todos los usuarios de sistemas operativos y de negocio deben mantener en secreto las contraseñas que les han sido asignadas.
- Se debe adaptar todo dispositivo y sistema informático para que los usuarios tengan la libertad de cambiar la contraseña cuando lo crea conveniente.
- Las contraseñas de acceso a los sistemas operativos y aplicaciones de negocio deben ser complejas y contener al menos 8 caracteres considerando el uso de caracteres alfanuméricos y caracteres especiales.
- Se deben configurar los aplicativos de negocio para que las cuentas se bloqueen luego de cinco (05) intentos fallidos de autenticación consecutivos.

B. Revisión y registro de los privilegios de acceso.

El Responsable de Seguridad Tecnológica en conjunto con el Gerente de Sistemas y Procesos son responsables de efectuar la revisión de privilegios de acceso a los aplicativos que procesan datos personales que correspondan al personal autorizado; esta revisión debe ser realizada con una periodicidad semestral programada y en forma aleatoria.

Producto de la revisión de los privilegios de acceso a los aplicativos se debe generar un registro de revisión que evidencie su realización, este registro debe ser mantenido por el Responsable de Seguridad Tecnológica en forma adjunta al Documento Maestro de Seguridad de la Información del Banco de Datos Personales.

La revisión debe confidencialidad sus el registro de asignación de privilegios de acceso que a su vez debe estar alineado a las funciones del cargo del usuario de acuerdo al Manual de Organización y Funciones.

El Responsable de Seguridad Tecnológica debe mantener plenamente identificados a los responsables y Encargados de Tratamiento y los privilegios de acceso asignados a los aplicativos de negocio.

C. Protección del banco de datos personales contra acceso físico no autorizado.

- El Responsable de Seguridad No Tecnológica, debe velar por que cada una de las gerencias que traten datos personales conserven los bancos de datos personales físicos en ambientes aislados protegidos por cerradura.
- La responsabilidad de mantener el mecanismo de seguridad del ambiente es de cada Responsable de Tratamiento de datos personales de acuerdo con el área o departamento y la ubicación en la que el banco de datos físico se encuentre.
- Los ambientes aislados en los que se encuentren los bancos de datos físicos deben ser sólo de acceso estricto y autorizado del Responsable de Tratamiento y de los Encargados de Tratamiento y que se encuentren debidamente identificados.
- Si, por tareas de revisión o auditoría, sea requerido el acceso de personal ajeno a los procesos y al tratamiento de los datos personales en bancos de datos físicos, los Responsables de

Tratamiento o a quien se designe deben autorizarlo y deben mantenerse vigilantes del accionar de dicho personal.
- El Responsable de Tratamiento debe llevar el correspondiente registro de acceso autorizados a los bancos de datos personales que se encuentren en forma física.

D. Protección del banco de datos personales contra acceso lógico no autorizado.

La Gerencia de Sistemas y Procesos debe velar por que el Responsable de Seguridad Tecnológica mantenga protegido y limitado el acceso a los sistemas informáticos utilizados sólo a los involucrados en el tratamiento de datos personales debidamente autorizados.

El Responsable de Seguridad Tecnológica, debe garantizar el cumplimiento de los siguientes lineamientos:

- Todos los usuarios de los sistemas informáticos deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de estos perfiles.
- Todos los sistemas informáticos deben contar con mecanismos de restricción de acceso a recursos del sistema no autorizados.
- Se establece que el acceso a través de cuentas de usuario y contraseñas sea configurado a todos los aplicativos que se utilizan en la empresa.
- Los bancos de datos personales que se encuentren en archivos de ofimática deben ser configurados para que su acceso sea por medio de contraseñas.
- La Transferencia de la información lógica fuera de las redes del dominio de la empresa debe realizarse por medios seguros a prueba de interceptaciones.

E. Autorización de acceso a los bancos de datos personales.

Los Responsables de Tratamiento de los bancos de datos personales son los designados, por la empresa, como titular del banco de datos personales para autorizar o retirar el acceso de los Encargados de Tratamiento de datos personales a los bancos de datos personales de los procesos en los que sean partícipes.

El Responsable de Seguridad Tecnológica debe mantener el registro de las autorizaciones de acceso brindados por los Responsables de Tratamiento a los Encargados de Tratamiento a los bancos de datos personales contenidos en los sistemas informáticos.

Es obligatorio que como mínimo este registro contenga:

- Identificador de usuario.
- Fecha y hora de asignación y/o retiro de autorización del usuario.
- Responsable de tratamiento que autoriza.

Toda autorización de acceso a los sistemas debe ser dada en función del cargo que ocupe cada Encargado de Tratamiento y que deba tratar datos personales.

F. Identificación de los accesos realizados a los datos personales para su tratamiento.

El Responsable de Seguridad Tecnológica debe implementar y mantener el Registro de Accesos a Bancos de Datos Personales, el cual debe contener al menos los siguientes campos:

- Cuenta de usuario con acceso al sistema.
- Fecha y hora de inicio y cierre de sesión.
- Nombres y apellidos de la persona o personas quienes realizan el acceso.
- Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación

aplicado).
- Motivo del acceso.
- Acciones relevantes (consulta, registro, modificación, supresión, transacciones).

7.5.2. Relacionadas a la alteración no autorizada del Banco de Datos Personales

A. Autorización para el retiro o traslado de datos personales.

Todo traslado de datos personales contenidos en soportes físicos o lógicos hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del Responsable de Seguridad Tecnológica y al Responsable de Seguridad No Tecnológica.

Es obligación de los Responsables de Tratamiento informar a los Responsables de Seguridad Tecnológica y No Tecnológica sobre el traslado de datos personales fuera de los ambientes donde se ubica el banco de datos personales, contemplando como mínimo la siguiente información:

- Origen.
- Motivo del traslado.
- Finalidad del traslado.
- Responsable del traslado.
- Destino.

Asimismo, el Responsable de Tratamiento debe mantener un registro trazable del traslado, que contenga como mínimo:

- Banco de datos al que pertenecen los datos personales.
- Responsable del traslado.
- Fecha y hora de traslado.
- Registro con un identificador disociado de los datos identificativos de los titulares de datos personales que son trasladados.

B. Traslado de datos personales.

Debe establecerse medidas de seguridad para los datos personales que son trasladados en soporte físico, los cuales deben regirse bajo lineamientos estipulados en una Política Intercambio de Información Física.

Los datos contenidos en soporte informático deben regir conforme a los lineamientos estipulados en una Política de Intercambio de Información por Medios Removibles de Almacenamiento que restrinja el traslado de información en dichos soportes, es posible realizar el traslado previa encriptación y se utiliza un mecanismo de verificación de la integridad.

C. Eliminación de la información contenida en medios informáticos removibles.

Cuando se requiera eliminar la información contenida en un medio informático removible se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que no se permita la recuperación de los datos, para ello las gerencias adjuntas se deben valer del apoyo de la Gerencia de Contraloría y Procesos.

Los Responsables de Tratamiento del banco de datos personales debe designar y autorizar a los Encargados de Tratamiento a eliminar la información de datos personales contenida en los medios informáticos removibles. El Responsable de Tratamiento debe contar con un listado de Encargados de Tratamiento autorizados a realizar la eliminación segura de la información.

El Responsable de Tratamiento, debe mantener un registro de eliminación de datos personales contenidos en medios removibles de almacenamiento, este registro debe contener en forma mínima.

- Banco de datos al que corresponde la información a eliminar.
- Nombres y apellidos de la persona que autoriza la eliminación.
- Nombres y apellidos de la persona que elimina la información.
- Registro de la serie/descripción del medio removible del cual es borrada la información.
- Fecha y hora de la eliminación.
- Motivo de la eliminación.

Cuando se proceda a eliminar información personal de medios removibles de almacenamiento, los Encargados de Tratamiento deben notificar al Responsable de Seguridad Tecnológica, quien a su vez debe garantizar que la información sea eliminada en forma segura.

Ningún medio removible de almacenamiento que contenga datos personales debe salir de las instalaciones de la empresa sin autorización del Responsable de Seguridad Tecnológica y sin haber sido autorizado su traslado ni empleados mecanismos de encriptación y validación de integridad.

D. Seguridad en la copia o reproducción de documentos

Toda Gerencia, debe contar con Encargados de Tratamiento autorizados a generar y/o eliminar las copias o reproducciones de los datos personales; por lo que el Responsable de Tratamiento debe designarlos y mantener un listado de ellos.

Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales:

- Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados que incluyan mecanismos de seguridad y control que permitan rastrear las actividades de reproducción.
- Todo Encargado de Tratamiento es responsable de supervisar el proceso de copia o reproducción de los documentos. No se debe dejar desatendido el equipo.
- Los Encargados de Tratamiento deben retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.
- El Responsable de Seguridad No Tecnológica debe promover campañas de concientización respecto a la seguridad en las actividades de copia y reproducción de datos personales.

Los Responsables de Tratamiento, deben registrar las copias o reproducciones de los documentos con datos personales realizadas, indicando como mínimo:

- Nombre de la persona que solicita la copia.
- Nombre de la persona autorizada a realizar copias.
- Descripción de los datos personales copiados.
- Número de copias.
- Motivo.
- Nombre de la persona que recibe la copia.
- Lugar de destino.
- Periodo de validez de la copia.

Toda copia o reproducción de los documentos deben tener una marca que identifique su periodo

de validez.

E. Autorización de Privilegios de Acceso a bancos de datos personales

El Responsable de Tratamiento, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo:

- Usuario (en sistemas informáticos el identificador de usuario)
- Privilegio asignado o retirado al privilegio
- Fecha y hora de asignación y/o retiro de privilegios del usuario.
- Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos, el identificador de usuario)

7.5.3. Relacionadas a la pérdida del Banco de Datos Personales

Se deben realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, para dicha finalidad de seguridad, se debe establecer una Política de Copia de Respaldo.

Toda copia de respaldo de los datos personales debe estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal; esta disposición debe regirse en forma complementaria con los lineamientos que sean dados por la Política de Copia de Respaldo.

La frecuencia de realización de las copias de respaldo y su periodo de conservación deben ser acordes con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales; la finalidad de tratamiento es definida por el Responsable de Tratamiento, por lo tanto, es a su vez, responsable de brindar estos parámetros al Responsable de Seguridad Tecnológica.

El Responsable de Seguridad Tecnológica es responsable de establecer lineamientos de la mano con mecanismos de seguridad que garanticen la continuidad del tratamiento de los datos personales en los medios tecnológicos.

Toda recuperación de datos personales, desde su copia de respaldo, debe contar con la autorización del Responsable de Tratamiento de datos personales y el Responsable de Seguridad Tecnológica.

El Responsable de Seguridad Tecnológica debe realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requeridas; esta disposición debe regirse en forma complementaria con los lineamientos dados en la Política de Copia de Respaldo.

Estas pruebas deben realizarse en forma semestral y se debe mantener el registro de los resultados de las pruebas incluyendo:

- Fecha y hora de la prueba.
- Nombre de la persona que realizó la prueba.
- Banco de datos personales recuperado.
- Archivo recuperado y fecha de los datos recuperados.
- Tiempo de recuperación.
- Resultados de las pruebas.
- Acciones tomadas en caso de pruebas insatisfactorias.

Este registro debe ser mantenido por el Responsable de Seguridad Tecnológica.

7.5.4. Relacionadas al tratamiento no autorizado del Banco de Datos Personales

A. Medidas Generales

1. Todas las Gerencias en la que se traten datos personales, y que cuenten con bancos de datos físicos, deben tenerlos independizados e individualizados por cada titular de datos personales sin exponer información de otro.

2. Cada gerencia, es el responsable de adecuar los procesos administrativos de la empresa de manera que sea posible la comunicación a los titulares de datos personales, de la ocurrencia de incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho.

   El informe de incidentes al titular de datos personales debe contener en forma mínima la siguiente información:

   - Naturaleza del incidente.
   - Datos personales comprometidos.
   - Recomendaciones al titular de datos personales.
   - Medidas correctivas implementadas.

B. Medidas Específicas

1. Mantenimiento de equipos utilizados para el tratamiento de datos personales.

   Es responsabilidad de cada Gerencia, reportar al Gerente de Contraloría y Procesos y al Responsable de Seguridad Tecnológica la identificación de equipos en los que se tratan datos personales.

   El Responsable de Seguridad Tecnológica es el responsable de llevar a cabo el mantenimiento preventivo y correctivo de los equipos utilizados para el tratamiento de los datos personales.

   El Responsable de Seguridad Tecnológica debe realizar el mantenimiento preventivo y correctivo de los equipos en forma acorde a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad.

   El Responsable de Seguridad Tecnológica es responsable de desarrollar el Plan de Mantenimiento Anual de Equipos.

   El Responsable de Seguridad Tecnológica es responsable de generar y mantener el registro de la realización del mantenimiento preventivo y/o correctivo; las rutinas de mantenimiento de equipos deben ser de conocimiento y autorizadas por el Gerente Procesos y Sistemas de la empresa.

2. Protección contra software malicioso.

   Los equipos utilizados para el tratamiento de los datos personales deben contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.) para proteger la integridad de los datos personales. El software de protección debe ser actualizado frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor; esta disposición debe regirse por una Política Código Malicioso.

3. Almacenamiento seguro de la información personal.

Toda información electrónica que contenga datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.

En el caso de los sistemas informáticos, el Responsable de Seguridad Tecnológica, debe aplicar las medidas de control de acceso y cifrado a las bases de datos que contengan datos personales.

Para el caso de archivos de ofimática que contengan datos personales, los Encargados de Tratamiento son responsables de cifrar la información mediante una contraseña de apertura.

4. Seguridad en la transmisión electrónica de datos personales.

   La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad; esta disposición debe regirse por una Política de Intercambio de Información.

   Es imprescindible que se valide la identidad de quien emita datos personales hacia la empresa, para lo cual se deben implementar los mecanismos de autenticación correspondientes.

5. Seguridad en el flujo transfronterizo de datos Personales

   Cuando se dé el caso de la existencia de un flujo transfronterizo de datos personales, el Responsable de Seguridad Tecnológica debe velar por que exista una homologación con las medidas de seguridad empleadas producto de la aplicación de la Ley 29733, Ley de Protección de Datos Personales.

   La entidad extranjera receptora de datos personales contenidos en bancos de datos de titularidad de la empresa debe aceptar las medidas de seguridad mediante la firma de un contrato o acuerdo que avale dicha aceptación.

6. Seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados.

   Para que sea posible que la empresa, contrate servicios de tratamiento de datos personales por medios tecnológicos tercerizados, el Responsable de Seguridad No Tecnológica debe velar por el cumplimiento de lo siguiente:

   - Que el proveedor no tenga acceso a la información de datos personales que utilicen su infraestructura.
   - Que el proveedor no brinde acceso a terceros a los datos personales que utilicen su infraestructura.
   - La destrucción o imposibilidad de recuperación de los datos alojados en el servicio una vez concluida la relación con el proveedor.
   - Uso de canales seguros para la transferencia de datos personales.
   - Garantizar el cumplimiento de las medidas de seguridad en todo lugar donde se encuentre distribuida la infraestructura del proveedor.

   Todos estos aspectos técnicos, deben estar debidamente incorporados en los términos y condiciones contractuales, en los que se debe incluir la potestad de realizar revisiones de cumplimiento en forma inopinada de cada aspecto.

   Estas condiciones deben ser validadas y aplicadas con el apoyo del Responsable de Seguridad Tecnológica y el Responsable Jurídico.

7. Gestión de incidentes de seguridad de los datos personales.

Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al Responsable de Tratamiento; esta disposición debe regirse de un Procedimiento de Gestión de Incidentes y Problemas.

El Responsable de Tratamiento o quien sea designado debe coordinar las acciones requeridas para analizar y responder en forma rápida y efectiva a los incidentes de seguridad presentados.

Se deben registrar los incidentes de seguridad relacionados con los bancos de datos personales, incluyendo como mínimo:

- Fecha y hora del incidente.
- Nombre de la persona que lo reporta.
- Naturaleza del incidente.
- Datos personales comprometidos.
- Nombres de las personas involucradas en la resolución del incidente.
- Consecuencias del incidente.
- Medidas correctivas implementadas.
- Recomendaciones para el titular de datos personales. (Si aplica).
- Recuperación de datos.
- En caso de haber realizado recuperación de datos, se debe registrar:
    - Nombre de la persona que realizó la recuperación.
    - Descripción y fecha de los datos restaurados.
    - Descripción de los datos restaurados. (Si aplica).

8. Restricción del uso de equipos de video, fotografía y audio.

   Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en todas aquellas áreas de tratamiento de datos personales salvo autorización expresa de su representante.

   De darse el caso de ser autorizado por el Titular del Banco de Datos Personales se debe realizar el debido registro de su realización, el cual estará a cargo del Responsable de Tratamiento de la Gerencia a la que se le está dando la autorización, el mantenimiento de los registros es responsabilidad del Responsable de Seguridad No Tecnológica quien debe ser notificado.

9. Auditoría Externa de seguridad de datos personales.

   Las auditorías internas y externas de seguridad de datos personales se dan a la par con las respectivas auditorías internas que emprenda la Gerencia de Contraloría.

   Es responsabilidad del Titular del Banco de Datos Personales, realizar una auditoría externa a fin de asegurar imparcialidad en los resultados.

10. Acciones correctivas y mejora continua.

    Es responsabilidad de la Gerencia de Contraloría y Procesos asegurar que la protección de datos personales siga el orden del cumplimiento de la LPDP a nivel de la seguridad de los datos personales por medio del mantenimiento del Sistema de Protección de Datos Personales

dentro del ciclo de mejora continua.

Toda desviación al cumplimiento de la LPDP debe ser corregida mediante acciones correctivas emprendidas por los mismos responsables y Encargados de Tratamiento y con el apoyo de los Responsables de Seguridad y el Responsable Jurídico.

7.6. Disposiciones Complementarias a las Medidas de Seguridad

La empresa, a través del Gerente de Gestión y Desarrollo Humano y con el apoyo de la Gerencia de Contraloría y Procesos debe desarrollar programas dirigidos a titulares de datos personales sobre "consentimiento", "derechos del titular de datos personales" y "finalidad".

Estos programas de difusión en información deben ser realizados dentro del ámbito que le corresponde a la empresa en el rubro automotriz.

La empresa, a través de los Responsables de Seguridad Tecnológica y No Tecnológica, debe asegurar y mantener los mecanismos de auditoría, verificación y toma de decisiones de cumplimiento con el tratamiento de datos personales realizados en bancos de datos de terceros que sean contratados, como lo son las centrales de riesgo, los sistemas de identidad de personas, los sistemas que proveen información de personas sospechosas de lavado de activos y financiamiento del terrorismo entre otros**.**

8. REGISTROS Y ANEXOS

8.1. Anexos:

- Anexo A: Glosario de términos relacionado a la PDP

9. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO A

GLOSARIO DE TÉRMINOS RELACIONADO A LA PDP

a) **Autoridad Nacional de Protección de Datos Personales (APDP)**: Está representada por el Ministerio de Justicia a través de la Dirección Nacional de Protección de Datos Personales y tiene entre sus funciones la de administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales. Otras funciones son:

- Supervisar el cumplimiento de las exigencias previstas en la Ley, para el flujo transfronterizo de datos personales
- Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores
- Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.

b) **Banco de Datos Personales**: Conjunto organizado de datos personales, automatizados o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

c) **Cancelación del Banco de Datos Personales**: Es la solicitud que se realiza ante la APDP, en la que se elimina un banco de datos personales que haya sido inscrito por una persona natural, persona jurídica de derecho privado o entidad pública; toca al titular del banco de datos, eliminar en forma segura de sus instalaciones informáticas y físicas el banco de datos en cuestión.

d) **Datos Personales**: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

e) **Datos Sensibles**: Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

f) **Encargado del Tratamiento**: Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando éste se realice sin la existencia de un banco de datos personales.

g) **Flujo Transfronterizo de Datos Personales**: Es la transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales.

h) **Gestión de riesgos**: Proceso ordenado y continuo para medir y mantener los riesgos por debajo de los umbrales definidos organizacionalmente.

i) **Inscripción de Banco de Datos Personales**: Es el acto registral que el titular del banco de datos personales realiza ante la APDP, para que se tenga debidamente identificado y mantenga el cumplimiento dentro de los alcances de la Ley para efectos de fiscalización y de ejecución de los derechos de las personas a la protección de sus datos personales y al uso de la finalidad de uso consentida.

j) **LPDP**: Ley de Protección de Datos Personales.

k) **Medio informático removible**: Dispositivo de almacenamiento de información. Incluye disquetes, CD's, DVD's, cintas

de respaldo, memorias USB, disco duro externo, entre otros.

l) **Modificación del Banco de Datos Personales**: Es la solicitud de modificación de un banco de datos personales producto de cambios realizados en el banco de datos que haya sido previamente inscrito.

m) **Privacidad**: Ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse.

n) **SPDP**: Sistema de Protección de Datos Personales.

o) **Titular de Datos Personales**: Persona natural a quien corresponde los datos personales.

p) **Titular del Banco de Datos Personales**: Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

q) **Encargado del Banco de Datos Personales**: Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

r) **Responsable de seguridad**: Rol asignado a una persona que coordina y controla la implementación de las medidas de seguridad en un banco de datos personales, en nuestra organización este rol está dividido en dos, un responsable para la seguridad física y otro para la seguridad tecnológica.

s) **Responsable del Tratamiento**: Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

t) **Transferencia de Datos Personales**: Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

u) **Tratamiento de Datos Personales**: Cualquier operación o procedimiento técnico automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

v) **Usuarios de sistemas de información**: Persona natural que tiene acceso a un sistema de información que realiza tratamiento de datos personales. Puede ser el administrador del sistema, administrador de banco de datos, operadores, personal de soporte o titular de los datos personales.

ANEXO 10.3

PROCEDIMIENTO DE ACCESOS AL SISTEMA Y RECURSOS INFORMÁTICOS

1. OBJETIVO

Establecer un procedimiento que permita conocer las actividades que se ejecutan para brindar accesos al sistema y a recursos informáticos.

2. ALCANCE

El proceso abarca desde la solicitud de requerimiento de recursos por parte del área solicitante, hasta la confirmación de acceso al sistema y entrega de recursos informáticos.

3. DEFINICIONES

ERH Empresarial: Plataforma donde se registran las solicitudes relacionadas al sistema.

Módulo: Es una porción del sistema en la cual ejecutan varias tareas que deben realizarse, para que los usuarios puedan cumplir con sus funciones u objetivos.

Usuario: Colaborador que utiliza un sistema informático y recursos informáticos, para el desarrollo de una función o de cualquier prestación de servicio.

Nivel 1 (SIS-GMD): Personal del Outsourcing GMD que, de manera remota, atiende los requerimientos que llegan al SIS tanto por envío de correos a sis@euromotors.com.pe, como por las llamadas al anexo 515.

Nivel 2 (SIS-GMD): Personal del Outsourcing GMD destacado físicamente en las instalaciones de la organización para poder brindar servicio in situ al personal de la empresa.

4. DOCUMENTOS A CONSULTAR

Instructivo para generar requerimientos de recursos para nuevas contrataciones o cambios organizacionales.

5. RESPONSABILIDADES

La **Gerencia de Sistemas** es responsable de asegurar el cumplimiento del presente procedimiento, incluyendo la aprobación e implementación del mismo.

El **Jefe de Administración de Sistemas** es responsable de que el Outsourcing SIS (GMD) cumpla con los requerimientos, procesos y plazos correspondientes a la asignación de cuentas de red, cuentas de correo y asignación de equipo informático, según sean las necesidades solicitadas con el cliente interno.

El **Solicitante** es responsable de ingresar los requerimientos de recursos necesarios para el usuario.

Las **Gerencias de Área, Contabilidad, Gerencia de empresa y Gerencia del grupo** son responsables de aprobar los requerimientos de recursos requeridos por el Solicitante.

La **Coordinadora de Selección** es responsable de notificar a las áreas correspondientes para que puedan asignar los recursos solicitados.

El **Área de Sistemas (SIS)** es responsable de generar los Tickets de Atención en la plataforma de Mesa de Ayuda, además de proporcionar equipos informáticos acorde a las necesidades del área.

El área de **Facility Management** es responsable de proporcionar equipos celulares, además de generar cotizaciones sobre equipos informáticos en caso lo requieran.

El **Analista Funcional** es responsable de realizar altas, bajas y brindar privilegios en el sistema de acuerdo a los requerimientos solicitados por las áreas de negocio.

El **Usuario** es responsable de recepcionar los equipos informáticos y validar sus accesos al sistema.

6. CONDICIONES GENERALES

- El presente documento debe ser revisado cuando cambian los procesos, condiciones de trabajo, por exigencias legales o al menos una vez al año a fin de evaluar si cumplen con los objetivos previstos.

- Todos los equipos computacionales y sistemas de la empresa cuentan con usuarios. La única manera de acceder a ellos es a través de la contraseña, la cual es estrictamente personal. Esta no debe ser escrita en papeles de fácil acceso o archivos sin cifrar.

- En los equipos computacionales el cambio de contraseña exigido por el sistema a los usuarios de red es de 30 días. De no acceder al cambio de password, la cuenta se bloquea.

- En los sistemas de la empresa, el cambio de contraseña exigido por el sistema a los usuarios de red es de 90 días. De no acceder al cambio de password, la cuenta se bloquea.

- Los usuarios de los equipos computacionales tienen la libertad de cambiar la contraseña que tienen asignada cuando se crea conveniente.

- Las contraseñas deben cumplir con los siguientes requisitos: ser complejas, debe contener al menos 8 caracteres, considerando caracteres alfanumérico y caracteres especiales.

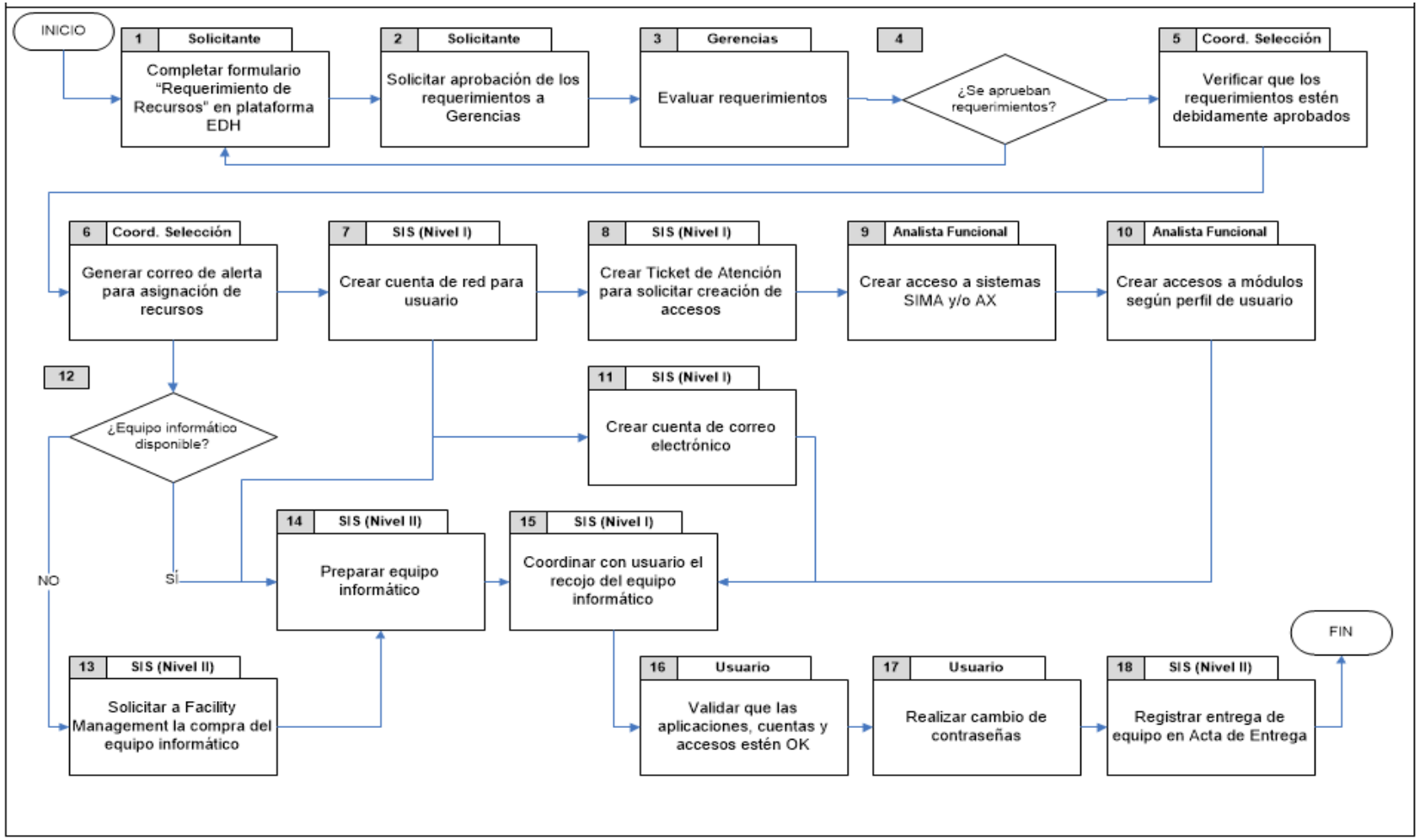
- Las cuentas de acceso para el sistema SIMA se bloquearán luego de tres (03) intentos fallidos de autenticación consecutivos.

- Luego de cierto tiempo de inactividad, la pantalla de los equipos computacionales se bloqueará según el perfil del usuario: personal operativo luego de cuatro (04) minutos, personal administrativo luego de ocho (8) minutos y personal de gerencia luego de doce (12) minutos.

- Los usuarios deben cambiar sus contraseñas si piensan que alguien más la conoce y si ha tratado de dar mal uso de ella. Además, no utilizar de contraseñas números telefónicos, nombres de familia, etc.

- Los usuarios deben cumplir con las políticas de sistemas, las cuales están alineadas al cumplimiento de los aspectos legales que exige el país.

7. DIAGRAMA DE FLUJO



8. DESARROLLO DEL PROCEDIMIENTO

Descripción	Responsable	Documento Asociado
1. Completar formulario y solicitar aprobación El Solicitante debe ingresar al aplicativo web ERH Empresarial (utilizar usuario y clave) y en la opción de Menú: "**Requerimiento de personal**", hacer clic en la opción "**Requerimiento de recursos**". Este formulario debe ser aprobado por Gerencia de Área, Contabilidad, Gerencia General de la empresa, GDH y Gerencia del grupo. Sólo tienen acceso a esta plataforma los empleados que tengan personal a cargo.	Solicitante	http://caerh/ERH/Index.aspx Correo de autorización
2. Verificar documentos del usuario. Luego de Completar formulario y solicitar aprobación, la Coordinadora de Selección verifica que el formulario "**Requerimiento de Recursos**" se encuentre debidamente aprobado y que la documentación del Usuario se encuentre completa para su incorporación. En caso de no haber observaciones, se envía una alerta (correo electrónico) a través de la plataforma ERH Empresarial, dirigido al Gerente de Área, Jefe de Administración de Sistemas, SIS y Facility Management, para la asignación de los recursos necesarios.	Coordinadora de Selección	Correo de alerta
3. Crear cuenta de red y correo electrónico Una vez recibida la alerta (correo electrónico) por parte de la plataforma ERH Empresarial, el SIS Nivel I procede a crear la cuenta de red en el directorio activo. Posterior a ello, procede a crear la cuenta de correo electrónico. Las cuentas estarán conformadas por el usuario de red y su respectiva contraseña. Dichos password serán genéricos y autogenerados, para cuando el usuario ingrese por primera vez realice el cambio.	SIS Nivel I	N/A
4. Preparar equipo solicitado. Paralelamente a Crear cuenta de red y correo electrónico, se prepara el equipo informático por parte del SIS Nivel II. En caso de no contar con el equipo informático, se le solicitará al área de Facility Management una compra tecnológica previamente validada por el Solicitante, Gerente de Área y Jefe de Administración y Sistemas; en forma paralela, el área de Facility Management solicita el celular en caso lo requiera.	SIS Nivel II	N/A

Descripción	Responsable	Documento Asociado
5. <u>Generar acceso en el sistema.</u> El SIS Nivel I genera un Ticket de Atención a través de la plataforma de Mesa de Ayuda solicitando la generación de accesos a los sistemas. Recibido el Ticket de Atención, el Analista Funcional procede con la creación de accesos para el usuario **(creación de cuenta SIMA / AX)**. Las cuentas estarán conformadas por el nombre de usuario del sistema y su respectiva contraseña El password que se le asignará al usuario al momento de la entrega de los recursos será genérico y autogenerado, para cuando el usuario ingrese por primera realice el cambio. Creadas las cuentas en AX/SIMA se procede con brindar los accesos a los módulos solicitados acorde a su puesto. . En caso de demora de notificación o alguna observación respecto al sistema AX/SIMA se canalizará por medio del botón rojo.	Analista Funcional	Ticket de Atención (plataforma Mesa de Ayuda)
6. <u>Validar accesos y recoger equipos informáticos</u> Luego de <u>Preparar el equipo solicitado</u>, el SIS Nivel II se comunica con el Usuario para coordinar el recojo del equipo informático. Durante dicha actividad, se valida con el mismo que se tengan disponibles todas las aplicaciones que serán utilizadas, se entrega los dispositivos requeridos en el formulario y se verifica que el Usuario tenga asignado su respectiva cuenta de red y de sistema. Luego, SIS Nivel II asiste al Usuario para que se realice el cambio de las contraseñas inmediatamente, tanto de acceso a los equipo de cómputo como al sistema. En forma paralela, le indica las políticas que debe tener en cuenta para una gestión de contraseñas responsable. Adicionalmente, capacita al Usuario con respecto a la manera de ejecutar el cambio de contraseña cuando él considere necesario realizarlo. Así también, se indica que en caso de tener dificultades con respecto al ingreso a sus cuentas otorgadas, sean estas por usuario y/o contraseñas, deben comunicarse inmediatamente con el SIS para realizar los cambios en su cuenta de red y/o contraseña o para sistemas con Soporte Funcional. Finalmente, se registra la entrega formal al Usuario y su conformidad.	SIS Nivel II	Acta de Conformidad de Asignación

9. REGISTROS Y ANEXOS

9.1. Registros

Nombre	Acceso	Almacenamiento	Tipo Almace-namiento	Retención	Dispo-sición	Área de Proceso	Responsable del Documento
Acta de Conformidad de Asignación	Físico	Archivador Sistemas	Papel	Indefinido	Backup	Sistemas	SIS Nivel II

9.2. Anexos

CANVIA
nacimos para reinventar

Acta de Conformidad

Euromotors

Conste por el presente documento que yo _____
dejo constancia que en atención al ticket #_____, han realizado la entrega del equipo con el código de activo _____ y con el siguiente detalle:

Codigo de Activo CPU :	S/N CPU :
Codigo de Activo Monitor :	S/N Monitor :
Codigo de Activo NoteBook :	S/N NoteBook :

Asimismo se ha verificado todo lo mencionado en el checklist de Usuario se encuentra instalado y configurado, quedando conforme con la instalación del equipo.

VALIDACIÓN DE ACCESOS	
	Acceso a la red de Euromotors
	Acceso al correo - Google Apps
	Validadción de usuario al link de la Extranet
	Acceso Sistema Oracle E-BUSINESS
	Acceso al Sistema de Talleres
	Envió y recepción de correos.
	Validación Open Office o Microsoft Office
	Prueba de impresión
	Favoritos de Internet

VALIDACIÓN DE ACCESOS	
	Acceso a la red de Euromotors
	Acceso al correo - Google Apps
	Validadción de usuario al link de la Extranet
	Acceso Sistema Oracle E-BUSINESS
	Acceso al Sistema de Talleres
	Envió y recepción de correos.
	Validación Open Office o Microsoft Office
	Prueba de impresión
	Favoritos de Internet

	Accesos y documentos del escritorio.
	Documentos en la unidad D

OBSERVACIONES

_____ Firma del usuario

_____ Firma del Técnico - Soporte SIS
Nombre:

Fecha: _____

10. CONTROL DE CAMBIOS

N° de Revisión	Sección y/o Página	Fecha de Modificación	Motivo	Autorizado por:

ANEXO 10.4

PROCEDIMIENTO DE ASIGNACION DE PRIVILEGIOS DE ACCESO

1. OBJETIVO

Establecer un procedimiento que permita conocer las actividades que se ejecutan, con la finalidad de brindar privilegios de acceso en el sistema.

2. ALCANCE

El proceso abarca desde la solicitud del Usuario hasta la confirmación de privilegios de acceso en el sistema.

3. DEFINICIONES

Mesa de Ayuda: Plataforma donde se registran las solicitudes relacionadas a los accesos del sistema, dicha plataforma esta administrado por el área de sistemas (Soporte Funcional).
Módulo: es una porción del sistema en la cual ejecutan varias tareas que deben realizarse, para que los usuarios puedan cumplir con sus funciones u objetivos.
Privilegio de acceso: Es un acceso, una ventaja exclusiva o especial que goza un usuario por concesión de un superior o por una determinada circunstancia.
Usuario: Colaborador, que tiene personal a cargo que usa el sistema informático y recursos informáticos, para el desarrollo de una función o de cualquier prestación de servicio.
Aplicativo de GDH: es la Plataforma digital por donde las gerencias realizan la solicitud de personal nuevo y donde además se solicitan los accesos a los sistemas del personal contratado.

4. DOCUMENTOS A CONSULTAR

Procedimiento de acceso al sistema y recursos Informáticos.

5. RESPONSABILIDADES

RESPONSABLE	ACCIÓN
Soporte Funcional	Encargado de brindar privilegios de acceso en el sistema de acuerdo a los requerimientos solicitados por las áreas del negocio
Usuario	Encargado de ingresar la solicitud de privilegios de acceso, además de validar su implementación de los permisos en el sistema.
GDH	Encargado de gestionar la solicitud de privilegios de acceso mediante el aplicativo de Solicitud de Requerimiento de Recursos.

6. CONDICIONES GENERALES

- El documento debe ser revisado cuando cambian los procesos, condiciones de trabajo, por exigencias legales o al menos una vez al año a fin de evaluar si cumplen con los objetivos previstos

7. DESARROLLO DEL PROCEDMIENTO

Descripción	Responsable	Documento Asociado
1. <u>Iniciar la solicitud de privilegios de acceso.</u> La Gerencia que solicita un recurso nuevo registra en el aplicativo de GDH, el requerimiento de asignación de privilegios de acceso a los sistemas del usuario contratado	Gerencia	Aplicativo digital de GDH

Descripción	Responsable	Documento Asociado
2. <u>Si el usuario no cuenta con los privilegios necesarios, inicia el requerimiento.</u> Si el usuario no cuenta con los accesos necesarios, ingresa a la plataforma de la Mesa de Ayuda del Soporte Funcional y realiza el requerimiento de los privilegios de acceso a los sistemas, adjunta la conformidad de su gerencia.	Usuario	Aplicativo de la Mesa de Ayuda del Soporte Funcional
3. <u>Asignar de Privilegios de Acceso al Usuario.</u> El Soporte Funcional ingresa en el sistema los privilegios que se requieren de acuerdo a lo aprobado por su Gerencia. Le confirma al usuario mediante el aplicativo de la Mesa de Ayuda.	Soporte Funcional	
4. <u>Comprobación del Usuario.</u> El Usuario verifica en el sistema que se cuente con los privilegios de acceso y brinda su conformidad mediante el aplicativo de la Mesa de ayuda.	Usuario	

8. REGISTROS Y ANEXOS:

Código	Nombre	Acceso	Almacenamiento	Tipo Almacenamiento	Retención	Disposición	Área de Proceso	Responsable del Documento
	REQUERIMIENTO POR EL APLICATIVO DE GDH	http://10.100.30.53/ERH/					GDH	Coordinador de selección
	REQUERIMIENTO POR LA MESA DE AYUDA DEL SOPORTE FUNCIONAL	http://caerh/ERH/Index.aspx					SISTEMAS	Soporte Funcional

REQUERIMIENTO POR EL APLICATIVO DE GDH

Requerimiento de recursos   Recibidos ×   SIS ×

nominas@euromotors.com.pe

para

Requerimiento de recursos 2019-0509

Empresa:

Supervisor:

Puesto Supervisor:

Persona contratada:

DNI:

Lista de Recursos Asignados
01 ACCESOS BASICOS
Cuenta de correos ; sanbartolome.com.pe
02 ACCESO A APLICACIONES
SIMA Recambios ; Asesor de servicios
03 EQUIPOS INFORMATICOS
Computadora ; Desktop (uso general)
04 ANEXO TELEFONICO Y EQUIPO CELULAR
Equipo celular
Salida llamada celular

Este correo fue enviado por el software Empresarial-RH.com

Atentamente,

Gerencia de Gestión y Desarrollo Humano
Euromotors S.A. - Representante Oficial
Av. Domingo Orué 973
Lima 34, Perú

REQUERIMIENTO POR LA MESA DE AYUDA DEL SOPORTE FUNCIONAL

'11/2019 Ticket #499572

Mesa de Ayuda

Bienvenido, | Panel de agente | Mis Preferencias | Salir

Panel de Control | Usuarios | Tickets | Reporte a AIDA | Base de conocimientos | De interés

Abierto (60) | Respondió (40) | Mis Tickets (3) | Vencido (83) | Cerrado (34,348) | Nuevo Ticket

Ticket #499572

Imprimir | Editar | Cambiar Estado | Más

Estado:	Cerrado	**Usuario:**	(13)
Prioridad:	Emergencia	**Correo:**	
Departamento:	Comercial	**Teléfono:**	
Creado en:	08/11/2019 5:22 pm	**Fuente:**	Web (190.116.0.98)

Cerrado por:		**Temas de ayuda:**	Comercial
Plan ANS:	— Ninguno —	**Último mensaje:**	12/11/2019 12:29 pm
Fecha de cierre:	12/11/2019 12:31 pm	**Última respuesta:**	12/11/2019 12:14 pm

Empresa:	
Generacion de la Incidencia:	Configuración de permisos
Solucion Consultora:	No fue necesaria
Tipo de Solucion:	Unicamente procedimiento en el Sistema
Respuesta Nivel 1:	Si

ACCESO

Hilo del Ticket (19)

ANEXO 10.5

PROCEDIMIENTO DE VERIFICACION DE PRIVILEGIOS DE ACCESO

1. OBJETIVO

Establecer un procedimiento que permita conocer las actividades que se ejecutan para verificar los privilegios de acceso en el sistema.

2. ALCANCE

El proceso abarca desde planificación del muestreo de las cuentas, hasta la generación del informe sobre los resultados.

3. DEFINICIONES

Privilegio de acceso: Es un acceso, una ventaja exclusiva o especial que goza un usuario por concesión de un superior o por una determinada circunstancia.

Usuario: Colaborador, que tiene personal a cargo que usa el sistema informático y recursos informáticos, para el desarrollo de una función o de cualquier prestación de servicio.

4. DOCUMENTOS A CONSULTAR

Procedimiento de acceso al sistema y recursos Informáticos.

5. RESPONSABILIDADES

RESPONSABLE	ACCIÓN
Soporte Funcional	Encargado de brindar privilegios de acceso en el sistema de acuerdo a los requerimientos solicitados por las áreas del negocio
Auditor	Encargado de verificar los privilegios de acceso de los usuarios en el sistema, además de generar un informe con los resultados.

6. CONDICIONES GENERALES

- El documento debe ser revisado cuando cambian los procesos, condiciones de trabajo, por exigencias legales o al menos una vez al año a fin de evaluar si cumplen con los objetivos previstos.
- Las auditorias de privilegios de acceso se deben realizar de manera periódica
- El número de auditorías realizadas durante el año debe ser mayores o iguales a dos
- En caso de encontrar diferencias se debe establecer planes de acción para evitar incidentes que pudieran ocurrir.

7. DESARROLLO DEL PROCEDMIENTO

Descripción	Responsable	Documento Asociado
1. <u>Planificar muestreo de cuentas.</u> El Auditor, para realizar la auditoria utiliza una técnica de muestreo aleatoria, teniendo como población el total de cuentas generadas en el sistema, el tamaño de muestra seleccionada para dicha actividad es de 25 cuentas.	Auditor	Registro de cuentas de sistemas sometidas al auditar
2. <u>Contrastar las cuentas de los usuarios versus los perfiles.</u> El auditor verifica que las cuentas seleccionadas tengan los privilegios del perfil según sus puestos, en caso de encontrar diferencias se identifica y se registra	Auditor	

Descripción	Responsable	Documento Asociado
3. <u>Validar diferencias contra el registro de privilegios asignados</u> El auditor verifica las diferencias encontradas de manera conjunta con el Soporte Funcional, sobre toda información relacionada a los privilegios tales como: fecha de habilitación, privilegios asignados y finalmente el responsable que autorizo los privilegios, en caso de no estar sustentada las diferencias se registra las diferencias no sustentadas	Auditor Soporte Funcional	
4. <u>Elaboración del informe.</u> El auditor elabora el informe sobre las cuentas inspeccionada, además informa sobre las diferencias de los privilegios no sustentadas, luego es remitido a la Gerencia de Sistemas para que realice las mejoras y/o correcciones pertinentes.	Auditor	Informe de auditoría de perfiles

8. REGISTROS Y ANEXOS:

N° de Revisión	Sección y/o Página	Fecha de Modificación	Motivo	Autorizado por:
NA			Primera versión.	

ANEXO 10.6

PROCEDIMIENTO DE ACCIONES CORRECTIVAS Y PREVENTIVAS PARA LA PROTECCION DE DATOS PERSONALES

1. OBJETIVO

Controlar de forma eficiente las acciones correctivas y preventivas tomadas para el mantenimiento y/o mejora dentro del marco de la Protección de Datos Personales.

2. ALCANCE

Aplica a todas las áreas y personas que intervengan en la Protección de Datos Personales.

3. DEFINICIONES

- No Observación: Aspectos de un registro que podría mejorarse.**to**
- Corrección: Acción tomada para eliminar una No Observación detectada.
- Acción Correctiva: Acción tomada para eliminar la causa de una No Observación detectada.
- Acción Preventiva: Acción tomada para eliminar la causa de una No Observación potencial.

4. RESPONSABILIDADES

- Analista de Procesos de Calidad : Definir el plan, asignar responsables y dar seguimiento.

5. CONDICIONES GENERALES

Las acciones correctivas pueden surgir de diversas fuentes como:

- Revisión de la Política de PDP
- Auditorías Externas y/o Internas
- Atención de Derecho ARCO
- Cambios en la infraestructura física
- Observaciones de los usuarios

Las acciones se deben tomar cuando

- Se identifiquen inconsistencias en la operación y/o aplicación de la PDP.
- El incumplimiento de los requerimientos de la ley y/o el reglamento es recurrente.
- Incumplimiento o desviación de los requisitos especificados en el checklist de auditoría.

Las acciones preventivas pueden surgir de diversas fuentes como:

- Observaciones y recomendaciones en auditorías internas y externas.
- Análisis de datos y tendencias, obtenidos del seguimiento y control de procesos.
- Resultados de acciones correctivas y preventivas emprendidas.
- Resultados de proyectos de mejora.

La Gerencia o los jefes de cada área son responsables de emprender acciones preventivas eficaces cada vez que:

- Se detecten observaciones y/u oportunidades de mejora en los reportes de auditoría sea interna o externa.
- Se observe que los resultados de las acciones emprendidas no lleguen a colmar las expectativas sobre lo esperado.

6. DESARROLLO

6.1. Análisis de la causa

Antes de programar una acción o medida, es necesario identificar las causas que ocasionan la no Observación y con ello concentrar el plan de acción en eliminar la causa raíz.

6.2. Elaborar plan de Acción para eliminar la Causa Raíz del problema

Identificada la causa raíz, se deberá proponer medidas (acciones correctivas y/o preventivas). En base a esto se debe elegir una o varias acciones, creando de esta forma un plan de trabajo que debe estar vinculado a un responsable y a un plazo de cumplimiento.

El Analista de Procesos de Calidad asignará al responsable, quien deberá velar por el cumplimiento de las actividades definidas.

El plazo de cumplimiento corresponde al periodo en el que se va implementar y asentar la medida, después de este plazo se puede comprobar la efectividad de las acciones tomadas.

6.3. Implementación del Plan de Acción

El responsable de cada medida debe asegurarse que éstas se lleven de acuerdo a lo planificado. En caso las actividades no estén dando los resultados esperados, el plan de acción se debe modificar y comunicar los cambios realizados. El plan se debe cumplir respetando los plazos establecidos, en caso se incumpla con el plazo, se debe indicar el motivo del retraso en las observaciones, señalando además la nueva fecha propuesta.

6.4. Comprobación de la Efectividad de las acciones tomadas

El Analista de Procesos de Calidad o el área de Cumplimiento o Control Interno será el responsable de comprobar la efectividad de las acciones tomadas, para esto definirá un responsable y el plazo para demostrar la efectividad.

Si ante esta prueba la acción no produjo el efecto deseado entonces se deberá tomar otra acción, la cual deberá registrarse tomando en cuenta lo citado anteriormente. Si la acción mostró que es efectiva entonces se dará por cerrada.

6.5. Seguimiento

El Analista de Procesos de Calidad deberá mantener al tanto al Gerente General y el área de Cumplimiento o Control Interno, sobre el seguimiento a las acciones correctivas y/o preventivas.

Así mismo, será responsable de darle seguimiento a las acciones correctivas propuestas por la empresa en las auditorías internas programadas y no programadas.

7. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO 10.7

PROCEDIMIENTO PARA LA GESTIÓN DE CONSENTIMIENTO

1. OBJETIVO

Establecer las estrategias, responsabilidades y actividades a realizar en la Gestión de Consentimientos para el Tratamiento de Datos Personales.

2. ALCANCE

Aplica a todos los formatos de consentimiento que se manejan en los diferentes bancos de datos identificados en la organización.

3. DEFINICIONES

- Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre datos personales, o de cualquier otro tipo concerniente a las personas naturales; que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- Tratamiento: Operación o procedimiento técnico, sea o no automatizado, que permita el recojo, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- Titular de datos personales: Persona natural a quien corresponde los datos personales.

4. RESPONSABILIDADES

- Analista de Procesos de Calidad: Implementar, realizar seguimiento, auditoría y mejoras en lo relacionado a la gestión de consentimientos para el tratamiento de datos personales.
- Gerente General: Dirigir y apoyar en la implementación de la utilización de los consentimientos en todos los canales y todas las sucursales de la organización.

5. CONDICIONES GENERALES

De acuerdo a la Ley 29733 – Ley de Protección de Datos Personales, para cualquier tipo de tratamiento que se realice con datos personales dentro de la organización se debe obtener el consentimiento voluntario, libre, previo, expreso, informado e inequívoco por parte del titular de dichos datos personales, salvo las excepciones establecidas por Ley.

Del mismo modo se debe especificar las finalidades que tendrá el tratamiento de los datos personales, así como el tiempo por el cual se realizará. Adicionalmente se deberá indicar si se realizará algún tipo de transferencia (local o transfronteriza).

6. DESARROLLO

Las diferentes estrategias para aplicar en cada tipo de banco de datos que maneja la empresa se han resumido en el Anexo A: Matriz de Estrategias para la Obtención del Consentimientos.

A continuación, se detalla dichas estrategias y las actividades a realizar según el Banco de Datos.

6.1. Banco de Datos de Video vigilancia

6.1.1. Estrategia

En cada área cerrada donde se haya instalado una cámara de video, se colocará en un lugar de fácil identificación un afiche/cartel que indique que dicha área es una zona video vigilada.

6.1.2. Obtención del Consentimiento

Cuando el titular de los datos personales (cliente, prospecto, trabajador, operador, etc.) ingrese a una zona video vigilada, verá el afiche/cartel y por la acción de quedarse en dicha zona está dando su consentimiento a ser grabado.

6.1.3. Archivamiento e identificación

Los videos son almacenados en un servidor, los cuales son custodiados por el Analista de Seguridad y Salud Ocupacional. Para cualquier revisión se tiene que coordinar previamente con él.

6.2. Banco de Datos de Trabajadores y Banco de Datos de Postulantes

6.2.1. Estrategia

Para ambos Bancos de Datos, la responsabilidad de la gestión de los consentimientos recae bajo el área de Gestión y Desarrollo Humano (GDH

6.2.2. Obtención del consentimiento

a. Para trabajadores nuevos:

Se obtiene la firma del consentimiento cuando el trabajador es contratado. La cláusula del consentimiento está incluida dentro del contrato laboral que firma cada trabajador nuevo.

b. Para trabajadores ya contratados:

Se obtiene la firma del consentimiento con adendas al contrato durante cada renovación de este.

c. Para Postulantes:

Se obtiene la firma del consentimiento durante la etapa de selección. La cláusula del consentimiento está incluida dentro de la Ficha de Datos Personales que completa cada postulante.

6.2.3. Archivamiento e identificación

Los consentimientos son archivados en los legajos de postulantes y trabajadores respectivamente en las oficinas del Área de GDH. Para cualquier revisión se tiene que coordinar previamente con dicha área.

6.3. Banco de Datos de Proveedores

6.3.1. Estrategia

Se utilizará un formato que detalle el consentimiento, que cada proveedor "persona natural" deberá firmar como señal de autorización

6.3.2. Obtención del Consentimiento

a. Proveedores nuevos:

El comprador entregará/enviará el formato al proveedor

Aplica para proveedores de todas las áreas, siendo los responsables:

- *Analista de Compras*: Compra de repuestos.
- *Asesor de Servicios*: Compra de servicios de terceros.
- *Área Corporativa de Logística*: Compras administrativas.

b. Proveedores ya existentes:

El comprador identificará en el sistema si es que el Proveedor tiene registrado un número de consentimiento. En caso aún no lo tenga, en la siguiente operación con el proveedor se le entregará/enviará el formato para la solicitud de la firma del consentimiento.

Aplica para proveedores de todas las áreas. Los responsables son los mismos.

6.3.3. Archivamiento e identificación

El formato firmado deberá ser archivado.

Adicionalmente, para su identificación posterior, el Comprador deberá registrar en la "Ficha del Tercero" del SIMA que dicho proveedor ya cuenta con el consentimiento, detallando el número correlativo asignado.

6.4. Banco de Datos de Prospectos

6.4.1. Estrategia

Se utilizará un texto/glosa que deberá ser incluido en los registros de los diferentes medios/canales donde los prospectos brindan sus datos.

Showroom: Se utilizará un formato de consentimiento predefinido para cuando algún prospecto solicite una cotización.

- *Activaciones*: En la lista donde los asistentes registran sus datos, se agregará un texto/glosa a modo de consentimiento. En el caso que se trabaje con una Tablet, en esta se debe incluir el mismo texto/glosa.
- *Página web*: En todas las pantallas/formularios donde se registren (y envíen) datos personales se incluirá el texto que detalle el consentimiento.
- *Redes sociales*: En los formularios de Facebook se incluirá el texto que detalle el consentimiento. En cuanto a inbox y/o comentarios, se programará una respuesta automática con el texto que detalle el consentimiento.
- *Llamadas*: Al inicio de la comunicación se indicará que la conversación está siendo grabada.
- *Otros medios*: Cualquier otro medio de prospección será canalizado a través de los antes indicados.

6.4.2. Obtención del Consentimiento

a. <u>Showroom:</u>

El Asesor Comercial se encargará de entregar el formato de consentimiento y solicitar la firma del este.

b. <u>Activaciones:</u>

En el momento en que los asistentes registran sus datos en la lista ya están dando su consentimiento. Sería recomendable hacer un comentario breve.

c. <u>Página web:</u>

Cuando se acepten los términos y se envíen los datos se estará dando autorización al tratamiento de los datos.

d. <u>Redes sociales:</u>

Dentro de un formulario de Facebook cuando se acepten los términos o en el caso del a inbox y/o comentarios cuando se continúe con la conversación el prospecto estará autorizando el tratamiento a los datos.

e. <u>Llamadas:</u>

Cuando se continúe con la comunicación luego del mensaje que indique la grabación se estará dando autorización al tratamiento.

6.4.3. Archivamiento e identificación

Todos los medios de prospección generarán Leads que serán dirigidos al CRM.

En el caso de los consentimientos obtenidos en showroom deberán ser archivados.

6.5. Banco de Datos de Clientes

6.5.1. Estrategia

Se utilizará un formato específico que detalle el consentimiento, que cada Cliente "persona natural" deberá firmar como señal de autorización.

6.5.2. Obtención del consentimiento

a. Clientes nuevos – Comercial: Cuando se entregan los documentos para el cierre de la venta, se debe incluir el formato de consentimiento para que sea firmado por el cliente “Persona Natural” o Representante Legal de la empresa.
La firma del documento es indispensable para entregar la unidad.

b. Clientes nuevos – Repuestos: Cuando el Asesor de Repuestos intenta generar el presupuesto y el cliente “Persona Natural” no existe en el sistema se hace entrega del formato de consentimiento y se solicita la firma de este.
Luego se procede con la creación del presupuesto de repuestos.

c. Clientes nuevos – Servicios: Cuando el Asesor de Servicios intenta abrir la orden de trabajo y el cliente “Persona Natural” no existe en el sistema se hace entrega del formato de consentimiento y se solicita la firma de este.
Luego se procede con la apertura de la orden de trabajo.

d. Clientes ya existentes:

Contactar con los clientes para hacer firmar el consentimiento.

Coordinar con el Jefe de Marketing y Analista de Procesos de Calidad

Para intentar realizar una comunicación masiva utilizando los medios/canales disponibles.

6.5.3. Archivamiento e identificación

El formato firmado deberá ser archivado.

Adicionalmente, para su identificación posterior, el Comprador deberá registrar en la “Ficha del Tercero” del SIMA el número correlativo asignado con la siguiente glosa: “Consentimiento LPDP + ##Corr”.

7. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO A

MATRIZ DE ESTRATEGIAS PARA LA OBTENCIÓN DEL CONSENTIMIENTOS

Banco de Datos	Estrategia
Video vigilancia	En cada área cerrada donde se haya instalado una cámara de video, se colocará en un lugar de fácil identificación un afiche/cartel que indique que dicha área es una zona video vigilada.
Trabajadores y Postulantes	Para ambos Bancos de Datos, la responsabilidad de la gestión de los consentimientos recae bajo el área de Gestión y Desarrollo Humano (GDH)
Proveedores	Se utilizará un formato específico que detalle el consentimiento, que cada proveedor "persona natural" deberá firmar como señal de autorización.
Prospectos	Se utilizará un texto/glosa que deberá ser incluido en los registros de los diferentes medios/canales donde los prospectos brindan sus datos. • *Showroom*: Se utilizará un formato de consentimiento predefinido para cuando algún prospecto solicite una cotización. • *Activaciones*: En la lista donde los asistentes registran sus datos, se agregará un texto/glosa a modo de consentimiento. En el caso que se trabaje comuna Tablet, en esta se debe incluir el mismo texto/glosa. • *Página web*: En todas las pantallas/formularios donde se registren (y envíen) datos personales se incluirá el texto que detalle el consentimiento. • *Redes sociales*: En los formularios de Facebook se incluirá el texto que detalle el consentimiento. En cuanto a inbox y/o comentarios, se programará una respuesta automática con el texto que detalle el consentimiento. • *Llamadas*: Al inicio de la comunicación se indicará que la conversación está siendo grabada. • *Otros medios*: Cualquier otro medio de prospección será canalizado a través de los antes indicados.
Clientes	Se utilizará un formato específico que detalle el consentimiento, que cada Cliente "persona natural" deberá firmar como señal de autorización.

ANEXO 10.8

PROCEDIMIENTO PARA LA REPRODUCIÓN O COPIAS DE DATOS PERSONALES

1. OBJETIVO

Definir las actividades que se deben realizar para permitir que el personal pueda hacer uso de dispositivos de reproducción.

2. ALCANCE

Aplica a todo el personal que haga uso de dispositivos de reproducción.

3. DEFINICIONES

- Dispositivos de Reproducción: Son equipos sirven para difundir más fácilmente la información haciendo que la comunicación sea más eficiente.

4. RESPONSABILIDADES

- Gerente / Jefe de Área: Autoriza el uso de los equipos de reproducción.
- Usuario de dispositivos: Quien realiza copias de documentos con datos personales.

5. CONDICIONES GENERALES

Todo el personal debe ser capacitado en temas relacionados a la Protección de Datos Personales.

6. DESARROLLO

6.1. Verificación de puesto y funciones

El Gerente o Jefe del Área determina si el Personal de su área, acorde a su puesto, funciones y responsabilidades tiene o tendrá alguna necesidad de reproducir o copiar documentos que contengan datos personales.

Idealmente se debería realizar cada vez que ingresa personal nuevo al área, caso contrario se debe realizar una revisión periódica.

6.2. Autorización del uso del dispositivo de reproducción

En caso de que se determine la necesidad, el Analista de Procesos de Calidad entrega y explica al Usuario de Dispositivos el Registro de Confidencialidad de Reproducción de Documentos, el cual debe ser firmado.

6.1. Utilización de dispositivos de reproducción

El Usuario de Dispositivos debe cumplir con las políticas de protección de datos personales, así como cumplir con el compromiso de confidencialidad respectivo. El incumplimiento podrá ser sancionado.

7. REGISTROS

7.1. Registros:

Nombre	Ubicación	Tipo	Vigencia	Área	Responsable
Confidencialidad de reproducción de documentos	File de Dispositivo de Reproducción	Físico	Indefinida	Todas	Encargado del Dispositivo

8. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO 10.9

PROCEDIMIENTO PARA PROTECCIÓN DE REPOSITORIOS FÍSICOS

1. OBJETIVO

Definir las actividades para la protección y mantenimiento de repositorios físicos relacionados con los bancos de datos que maneja la empresa.

2. ALCANCE

Aplica a todos los repositorios físicos que contienen información de carácter personal.

3. DEFINICIONES

- Repositorio físico: Es un lugar donde se almacena documentación física como: Ordenes de Taller, Pedidos de Ventas, Ofertas, etc., En cuyo contenido alberga información de carácter personal.

4. RESPONSABILIDADES

- Responsable del Repositorio: Identificar la necesidad de atención en los repositorios.
- Asistente de Compras: Solicitar y coordinar la atención de mantenimiento.

5. CONDICIONES GENERALES

El inicio de este procedimiento se puede dar por diferentes casusas, como: Perdida de llaves de los repositorios físicos de información física, repositorio físico averiado, nuevo repositorio físico de información desprotegido.

Los repositorios físicos dañados o desprotegidos, deben ser atendidos a la brevedad, con la finalidad de evitar un robo de información.

6. DESARROLLO

6.1. Evaluar repositorio físico de Información

Los responsables de los repositorios físicos deben evaluar de manera rutinaria las condiciones de seguridad de los repositorios, las medidas de seguridad de repositorios nuevos, extravió de dispositivos de acceso a los repositorios de Información.

6.2. Comunicar para el resguardo de dichos repositorios

Los responsables de los repositorios físicos, deben comunicar al Asistente de Compras, a través de un correo electrónico con asunto:

"INCONVENIENTES CON LA SEGURIDAD + Identificación del Repositorio"

Que existen problemas con dichos repositorios.

La Información debe consignar la ubicación del repositorio físico, tiempo que se encuentra sin protección, razón por la cual se viene informando.

El Asistente de Compras debe coordinar con el área de logística corporativa la atención inmediata del repositorio de información desprotegido, en el plazo máximo de medio día de haber ingresado el correo electrónico a la bandeja de entrada.

Luego se deberá comunicar al proveedor que realiza actividades de mantenimiento en el local, brindándole la información de la ubicación donde se realizarán los trabajos y la persona de contacto con su respectivo número telefónico.

6.1. Atender requerimiento

El proveedor deberá dirigirse al área en la cual solicito el servicio con un plazo máximo de un día, para la dar la atención respectiva.

El responsable del repositorio físico deberá validar la atención y comunicar vía correo la culminación de los trabajos en los repositorios.

7. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO 10.10

PROCEDIMIENTO PARA LA ATENCIÓN DE INCIDENCIAS

1. OBJETIVO

Definir las actividades que se debe realizar en caso ocurran incidencias con Datos Personales.

2. ALCANCE

Aplica a toda condición potencial que podría afectar la seguridad de Datos Personales.

3. DEFINICIONES

- Problema de seguridad de Datos Personales: Cualquier acción que afecte a la seguridad, integridad y disponibilidad de Datos Personales.

4. RESPONSABILIDADES

- Todos los colaboradores: Identificar y comunicar la incidencia.
- Administrador de incidencias: Revisar, solucionar y comunicar la solución de la incidencia.

5. DESARROLLO

5.1. Identificación de Incidencias

Durante de la ejecución de actividades en la organización, los colaboradores deben informar sobre los problemas que pueden afectar la seguridad de sus datos personales tales como:

- Extravío de documentos con datos personales.
- Presunción de robo de contraseñas.
- Uso indebido de datos personales para finalidades diferentes a las recolectadas.
- Robo de base de datos.
- Uso de datos personales sin consentimiento.
- Daño de documentos con datos personales.
- Falsificación o sustitución de documentos físicos que contienen datos personales
- Daño físico de repositorios de información

Así también se debe informar sobre alguna condición potencial que puede afectar la seguridad de datos personales

5.2. Comunicar incidencia identificada

Enviar un correo a incidenciaslpdp@euromotors.com.pe, con la siguiente estructura:

Asunto	Incidencia LPDP/ (El tipo de incidencia) / (Empresa)
Cuerpo del Correo	Nombre del Colaborador: Tipo de Incidencia: Detalle de la Incidencia: Fecha y hora de la Incidencia: Adjuntar todo el material de sustento.

5.3. Revisar incidencia

El Administrador de Incidencias deberá revisar si la información remitida es suficiente o no para la atención, en caso de requerir más información se solicitará al detalle.

5.4. Tratar incidencia

El Administrador de Incidencias, en base a la información proporcionada, ejecutará las siguientes actividades:

i. Se verificará si el tipo de incidencia cuenta con un procedimiento elaborado. (Consultar Inventario de procedimientos de atención de incidencias)
ii. En caso de tener el Procedimiento de Gestión de Incidencias, deberá ser aplicado.
iii. En caso de no tener elaborado un procedimiento para ese tipo de incidencia, se realizará la Investigación, para determinar responsabilidades y sanciones.
iv. Posterior a la Investigación se deberá elaborar el procedimiento de atención de dicha incidencia.
v. Será aprobado por la Organización de Protección de datos Personales.

5.5. Remitir respuesta

El Administrador de Incidencias, informará al colaborador y a los involucrados sobre las acciones que se ejecutaron o deberán ejecutarse para su respectiva atención.

5.6. Registrar información

Finalmente se registra la información correspondiente a la incidencia, en el formato establecido para dichos fines.

6. REGISTROS

6.1. Registros:

Nombre	Ubicación	Tipo	Vigencia	Área	Responsable
Incidencias de Datos Personales	Área SIS	Físico	Indefinida	Control interno	Administrador de Incidencias

Fecha y hora detectada	Colaborador reportante de la incidencia	Tipo de incidencia	Detalle de la incidencia	Responsable de atención	Tratamiento	Estado

7. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO 10.11

PROCEDIMIENTO DE ELIMINACIÓN DE DATOS PERSONALES

1. OBJETIVO

Definir las actividades que se debe realizar para la eliminación de Datos Personales acorde a la lo que indica la Ley de Protección de Datos Personales.

2. ALCANCE

Aplica desde la identificación de documentos caducados hasta su disposición final.

3. DEFINICIONES

- Repositorio Físico: Lugar donde se almacena documentación física como: Órdenes de Taller, Pedidos de Ventas, Ofertas, etc., cuyo contenido alberga información de carácter personal.

4. RESPONSABILIDADES

- Jefe de Área: Autorizar la salida del almacén, destrucción y disposición final.
- Responsable del Repositorio: Comunicar paquetes de documentos próximos a vencer y registrar movimiento de documentos.
- Responsable de Eliminación de Documentos: Responsable de realizar una destrucción de los documentos, de manera confidencia, además de la disposición física del material destruido.

5. DESARROLLO

El responsable del repositorio de información realiza lo siguiente:

5.1. Identificación de documentos

Una vez identificado, se comunica al Jefe del Área, vía correo electrónico, sobre los documentos cuya fecha de almacenamiento está próxima a caducar, con la finalidad de autorizar su retiro del almacén.

5.2. Registro de la eliminación

Se registra en el Formato de Inventario de Documentos Eliminados, la salida de los documentos y en el campo de observaciones se detalla el Jefe del Área que autorizo la salida de los paquetes.

El responsable de eliminación de documentos realiza lo siguiente:

5.1. Traslado y Eliminación

Se traslada los paquetes a ser eliminados en una zona apropiada, en la que solo tenga acceso dicho responsable.

Para la destrucción se utiliza una trituradora de papeles, con la finalidad de que la información en dichos documentos se encuentre desasociada y no permita ser reconstruida.

5.2. Confirmación y disposición final

Se remite un correo al Jefe del Área informando que se terminó la destrucción de los documentos e indicando la disposición de los documentos destruidos.

6. REGISTROS

6.1. Registros:

Nombre	Ubicación	Tipo	Vigencia	Área	Responsable
Inventario de documentos eliminados	File LPDP	Físico	Indefinida	Todas	Analista de Procesos de Calidad

7. CONTROL DE CAMBIOS

N° Revisión	Fecha	Motivo / Cambios / Detalle

ANEXO 10.12

PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN EN PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVO

Definir un cronograma con las actividades necesarias para la capacitación y sensibilización del personal en relación a Protección de Datos Personales.

2. ALCANCE

La aplicación del presente documento involucra todo el personal de la organización que participe en procesos donde se realicen tratamiento de datos personales.
La validez o vigencia del presente plan no tiene una fecha determinada.

3. DEFINICIONES

- PDP: Abreviatura para el término "Protección de Datos Personales".
- LPDP: Abreviatura para referirnos a la Ley 29733 – Ley de Protección de Datos Personales.

4. RESPONSABILIDADES

- Coordinador de Procesos: Ejecución del plan.
- Gerente General: Control del cumplimiento del plan.

5. CONDICIONES GENERALES

5.1. Temas a tratar

Los tópicos o temas relacionados a la LPDP que deben ser tratados son los siguientes:

- Políticas de protección de datos personales.
- Derechos ARCO.
- Principios de la LPDP.
- Consentimiento.
- Medidas Tecnológicas.
- Medidas Jurídicas

5.2. Técnicas a utilizar

Los medios, técnicas y/o estrategias a utilizar para transmitir al personal estos temas son:

- Charlas presenciales. Se consideran todos los locales a nivel nacional
- Charlas virtuales (E-Learning)
- Mensajes como protector de pantalla en las pc's del personal
- Envío de boletines vía correo corporativo

5.3. Medición y seguimiento

Como indicador general, se debe medir el grado de cumplimiento del plan (%C).
La frecuencia de medición será trimestral (meses de Marzo, Junio, Setiembre y Diciembre).

6. DESARROLLO

En el siguiente cronograma se detalla el tipo de actividades a realizar en cada trimestre del año:

Topicos	1er trim Ene-Mar	2do trim Abr.Jun	3er trim Jul-Set	4to Trim Oct-Dic
Politica de PDP				
✔Charla presencial				
✔Boletines via Correo				
Derechos ARCO				
✔Charla presencial				
✔Charla virtual				
✔Boletines via Correo				
Principios de la LPDP				
✔Boletines via Correo				
✔Protector de pantalla				
Consentimiento				
✔Charla presencial				
✔Charla Virtual				
✔Boletines via Correo				
✔Protector de Pantalla				
Medidas Juridicas				
✔Boletines via Correo				
✔Protector de Pantalla				
Medidas Tegnologicas				
✔Boletines via correo				
✔Protector de Pantalla				

Las celdas sombreadas de verde, indican que en el trimestre correspondiente se realizará al menos una actividad utilizando el medio señalado para abordar el tema indicado.

7. CONTROL DE CAMBIOS

N° de Revisión	Fecha	Motivo

ANEXO 10.13

PROCEDIMIENTO DE AUDITORÍA PARA LA PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVO

Establecer los lineamientos y las actividades que se deben seguir para la Auditoría al Sistema de Protección de Datos Personales con la finalidad de medir su grado de cumplimiento.

2. ALCANCE

La aplicación del presente documento involucra a todas las gerencias, áreas y personal de la organización que participe en procesos donde se realicen tratamiento de datos personales.

3. DEFINICIONES

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el cumplimiento de criterios definidos.
- Auditoría Interna: Auditoría que se realiza por la propia organización para fines internos.
- Auditoría Externa: Auditoría que se realiza por organizaciones y/o instituciones externas con el fin de asegurar la imparcialidad en los resultados.

4. RESPONSABILIDADES

- Analista de Procesos de Calidad: Planificar, comunicar y ejecutar las auditorías, así como realizar el seguimiento del plan de acción luego de la revisión de resultados.
- Gerente General: Revisar los resultados de las auditorías.
- Área de Cumplimiento y Control Interno: Llevar a cabo auditorías externas inopinadas, coordinando con el Resp. Seguridad No Tecnológica cualquier aspecto que sea necesario.

5. DESARROLLO

5.1. Planificación

El Analista de Procesos de Calidad debe realizar las siguientes actividades:

5.1.1. Elaborar el Plan de Auditorías:

El Plan Anual de Auditorías al Sistema de Protección de Datos Personales debe ser revisado y aprobado por el Gerente General antes de finalizar el mes de enero.

5.1.2. Definir el Programa de Auditoría:

El programa debe detallar como mínimo la relación de actividades a realizar durante la auditoría, así como las áreas o personal que estarán involucrados directamente.

Para el caso de las auditorías externas, la elaboración del programa queda bajo la responsabilidad del área Cumplimiento y control interno.

5.2. Comunicación

El Analista de Procesos de Calida debe realizar las siguientes actividades:

5.2.1. Difundir el Plan de Auditorías:

Máximo 1 semana después de la aprobación del Plan, enviar a los Gerentes y Jefes involucrados un correo comunicando y adjuntando el Plan Anual de Auditorías.

5.2.2. Enviar Programa de Auditoría:

Una semana antes de la ejecución enviar el programa a los involucrados directos.

5.2.3. Auditorías no planificadas:

Las auditorías no planificadas se realizan en consecuencia de resultados anteriores, por mejoras/cambios del sistema o por seguimiento de resultados; y no necesariamente deben ser comunicadas dentro de los plazos estipulados en párrafos anteriores; incluso pueden ejecutarse sin previo aviso.

5.3. Ejecución

El Analista de Procesos de Calidad será quien ejecute las auditorías internas en función al programa elaborado y enviado previamente.

La auditoría estará basada en criterios de la Reglamento de la LPDP y la Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales. Para esto se debe de utilizar un Check List con los puntos exactos a revisar.

La obtención de evidencias se realizará a través de una o más de las siguientes acciones:

- Entrevistas o revisión de documentos
- Observación de las instalaciones físicas
- Observación de la ejecución de los procesos realicen tratamiento de datos personales

Para el caso de las Auditorías Externas, estas serán realizadas por el personal asignado por el área de Cumplimiento y control interno, esto con el fin de asegurar la imparcialidad en los resultados. Toda la coordinación previa y/o posterior, será a través del Analista de Procesos de Calidad; y la inspección seguirá la misma metodología que una auditoría Interna.

5.4. Revisión de Resultados

El Analista de Procesos de Calidad debe realizar las siguientes actividades

5.4.1. Elaborar el Informe de Auditoría:

Para formalizar los resultados de las auditorías internas, detallando los diferentes tipos de hallazgo: oportunidades de mejora, observaciones y/o no conformidades.

Para el caso de las no conformidades, se deben contemplar los siguientes elementos:

- Naturaleza: Descripción del requisito que se incumple.
- Hecho: Descripción de lo que se incumple.
- Evidencia: Elemento que demuestra el incumplimiento.

Para el caso de las auditorías externas, la elaboración del Informe de Auditoría queda bajo la responsabilidad del área de Cumplimiento y control interno.

5.4.2. Comunicar los resultados:

Máximo a una semana luego de haber realizado la auditoría se debe enviar y revisar el Informe con el Gerente General.

Dependiendo de los resultados y la revisión, si se considera necesario, se debe convocar a una

reunión con los Gerentes y Jefes involucrados.

Se debe firmar el Control de Auditorías de la Ley de Protección de Datos Personales.

En el caso de las auditorías externas, se realizará una reunión entre el Auditor, el Analista de Procesos de Calidad y Gerente General, la cual será convocada por el Auditor.

5.4.3. Definir un Plan de Acción:

En coordinación con el Gerente General y demás involucrados, establecer un plan que detalle las acciones correctivas y/o preventivas según los hallazgos identificados.

En el Plan de Acción se deben detallar como mínimo las actividades a realizar, los responsables y plazos para su finalización.

5.5. Seguimiento

El Analista de Procesos de Calidad, luego de que se cumplan las fechas definidas en el plan de acción, debe realizar una revisión del cumplimiento a las actividades y también comprobar la efectividad de las acciones tomadas.

6. REGISTROS

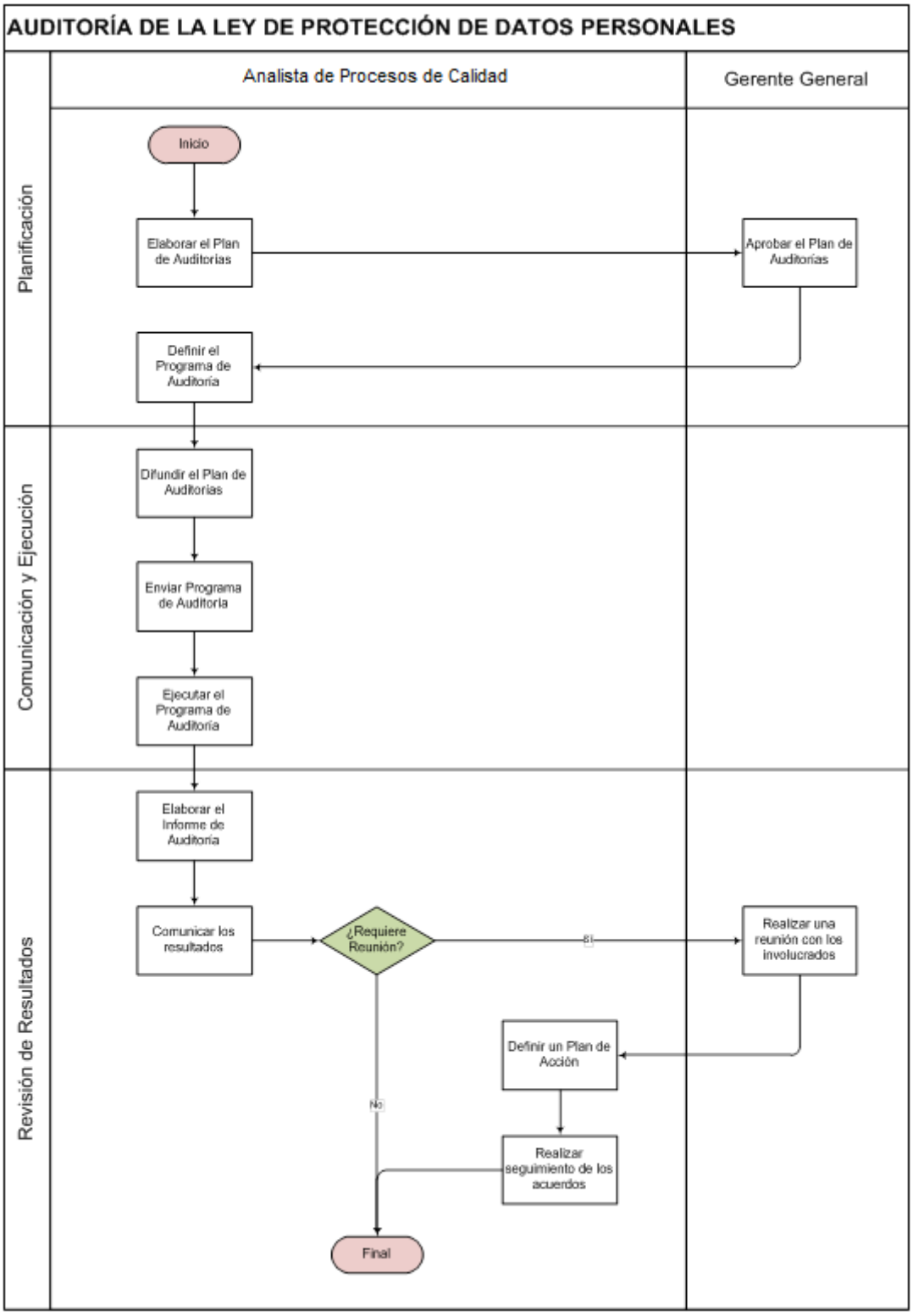
6.1. Registros:

Nombre	Ubicación	Tipo	Vigencia	Área(s)	Responsable
Control de Auditorías de la LPDP	File de LPDP	Físico	Anual	Gerencia General	Analista de Procesos de Calidad

7. CONTROL DE CAMBIOS

N° de Revisión	Motivo
01	Formalización del Procedimiento de Auditoría de la Ley de Protección de Datos Personales

8. DIAGRAMA DE FLUJO



ANEXO 10.14
METODOLOGIA O PLAN DE TRATAMIENTO DE RIESGOS

1. OBJETIVO

Identificar, analizar, evaluar y tratar los riesgos de privacidad de los datos personales, con la finalidad de determinar su tratamiento de acuerdo a los alcances de la ley de protección de protección de datos personales.

2. ALCANCE

Los lineamientos establecidos en esta metodología, son de cumplimiento obligatorio para todas las áreas, procesos de la organización y medios en los que se tratan datos personales.

3. DEFINICIONES

a) **Amenaza:** Toda acción que afecta a un activo de información, aprovechándose de sus vulnerabilidades, generando una serie de consecuencias y que afectan a los objetivos de negocio.

b) **Control Existente:** Medida de seguridad actualmente implementada para proteger los datos personales y/o su medio de tratamiento.

c) **Custodio:** Es la persona encargada de garantizar la seguridad de los datos personales, está representado por los responsables de tratamiento del banco de datos personales.

d) **Impacto:** Cambio adverso en el nivel de objetivos empresariales logrados.

e) **Propietario del riesgo:** Es la persona responsable de rendir cuentas y que tiene la autoridad para gestionar el riesgo, está representado por el responsable de seguridad de protección de datos personales.

f) **Responsable de Seguridad:** Es aquel que vela por el cumplimiento con las medidas de seguridad establecidas para proteger la privacidad de los datos personales en la organización.

g) **Responsable de Tratamiento:** Es aquel que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

h) **Riesgo:** Efecto que crea incertidumbre sobre el cumplimiento de los objetivos de la organización.

i) **Vulnerabilidad:** Es una debilidad del medio de tratamiento o del control que lo protege, la cual es aprovechada por alguna amenaza generando el evento de riesgo.

4. METODOLOGÍA

La metodología de Gestión del Riesgo está dividida en 5 fases:

I. Entendimiento del Contexto

Es comprender el contexto interno y externo en el que se tratan los datos personales para tener un panorama de las interacciones entre los procesos, los actores y el entorno para poder identificar los riesgos a la privacidad de datos personales.

II. Identificación de los riesgos.

Después de identificar el contexto, se identifican los eventos de riesgo con la ayuda del catálogo de eventos de riesgos de privacidad de datos personales **(Anexo A)** y en base al tipo de contexto y a los datos personales que se tratan así como a los bancos de datos en los que se encuentran.

En base a los eventos de riesgo, se realiza en análisis de riesgos.

III. Análisis de los riesgos.

En esta fase se identifican los niveles de probabilidad, impacto y riesgo, tomando en cuenta los elementos de riesgo identificado (evento de riesgo, vulnerabilidad y controles existentes)

Para obtener el Nivel de Riesgo se utiliza el Mapa de Nivel de Criticidad de Riesgo, en el que se busca la intersección de los niveles de impacto y probabilidad.

Niveles de Impacto	
Nivel	**Criterio**
Muy Alto	Multa Muy Grave, con denuncia y afecta la imagen.
Alto	Multa Muy Grave.
Medio	Multa Grave.
Bajo	Multa Leve.
Muy Bajo	Genera una multa leve pero es fácilmente apelable.

Niveles de Probabilidad	
Nivel	**Criterio**
Muy Alta	Frecuente
Alta	Probable
Media	Posible
Baja	Probable
Muy Baja	Muy poco probable

Mapa de Nivel de Criticidad de Riesgo

	Probabilidad	Muy Baja	Baja	Media	Alta	Muy Alta
	Muy Bajo	0	1	2	3	4
	Bajo	1	2	3	4	5
Impacto	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy Alto	4	5	6	7	8

IV. Evaluación de los riesgos.

En base a los criterios de aceptación del riesgo, es que se identifican los riesgos no tolerables y los riesgos tolerables, estos criterios están relacionados a los niveles de criticidad de riesgo identificados.

Criterios de Aceptación del Riesgo

ACEPTABLE
TOLERABLE
INACEPTABLE

V. Tratamiento de los riesgos.

Para aquellos riesgos que son Inaceptables se deben determinar las opciones de tratamiento. Los riesgos que resulten Tolerables pueden tratarse si la organización lo considera.

Las opciones de tratamiento se definen de acuerdo a los siguientes conceptos:

Reducir: Reducir el riesgo de modo que el riesgo residual se pueda re-evaluar como aceptable, minimizando la probabilidad o el impacto.
Retener: Retener el riesgo de acuerdo a la viabilidad de tratamiento o costo-beneficio de tratamiento.
Evitar: Evitar el riesgo cambiando de actividad o proceso.
Compartir: Transferir a otra parte que pueda administrar con mayor eficacia el riesgo.
Remover: Eliminar la fuente de riesgo si está en la posibilidad de la organización.
Incrementar: Incrementar el riegos debido a una oportunidad.

Al definir la opción de tratamiento, se valoran los riesgos residuales que toman sus valores del mapa de criticidad de nivel de riesgo.

Una vez que se tienen valorados los riesgos residuales, se procede a priorizar los riesgos de acuerdo a los siguientes estados:

- No Prioritario.
- Medianamente Prioritario.
- Muy Prioritario.

Para el análisis, evaluación y tratamiento de riesgos se utiliza el formato del **Anexo B**.

VI. Plan de Tratamiento de Riesgos

Luego de priorizados los riesgos, se elabora el Plan de Tratamiento de Riesgos **(Anexo C)** en el que se designan los responsables, se establecen los plazos de ejecución y se nombra a un encargado de seguimiento para garantizar la implementación.

La información necesaria para cada una de las fases puede ser recopilada usando la metodología de Tormenta de ideas, Análisis de Impacto al Negocio, registros de incidentes, registros de las actividades de monitoreo de seguridad u otros métodos que sean convenientes.

5. ROLES Y RESPONSABILIDADES

Responsable	Responsabilidades
Responsable de Seguridad.	▪ Coordinar las actividades de la apreciación del riesgo de acuerdo al contexto establecido.
Propietario del Riesgo.	▪ Responsable de que se gestione y se trate en forma eficaz el riesgo.
Responsables de la operación del control.	▪ Responsable de que el control trabaje eficazmente.
Responsables de la acciones de tratamiento del riesgo.	▪ Responsable de rendir cuenta de las actividades del plan de tratamiento, es el responsable de la ejecución.
Responsable de seguimiento de las acciones de tratamiento.	▪ Responsable de garantizar que las acciones de tratamiento se lleven a cabo mediante el seguimiento de los avances de implementación.

6. ANEXOS

N°	Nombre del Documento	Tipo
1	Catálogo de eventos de riesgo.	Anexo A
2	Formato de identificación, análisis, evaluación y tratamiento de riesgo.	Anexo B
3	Formato de plan de tratamiento del riesgo.	Anexo C

ANEXO A

Catálogo de Eventos de Riesgo

Categoría de Evento de Riesgo	Evento de Riesgo
Acceso ilegítimo a datos personales	Acceso no autorizado a datos personales.
	Abuso de privilegios de acceso.
	Robo de identidad de personal autorizado para tratar datos personales.
	Robo de la base de datos personales.
	Pérdida de información en los flujos de transferencia electrónica.
	Intrusión en las redes de datos en las que se transfieren datos personales.
	Uso y/o divulgación de información sensible.
	Uso y/o divulgación de información de datos personales.
	Difusión de software malicioso en las redes en las que se trata datos personales.
	Uso de datos personales sin consentimiento.
	Consentimiento obtenido sin ser previo, informado, expreso e inequívoco.
	Uso de datos personales sin prueba de consentimiento trazable.
	Uso inadecuado de dispositivos de almacenamiento portátil.
	Robo de dispositivos móviles que almacenan datos personales.
	Recuperación de datos personales a partir de dispositivos de almacenamiento desechados.
	Indiscreción sobre datos personales.
	Uso de influencias para obtención de datos personales.
	Lectura de documentos con datos personales en dispositivos de reproducción desatendidos.
	Intrusión en el traslado de documentos físicos con datos personales.
	Equipos de procesamiento de datos personales desatendidos.
	Uso no autorizado de datos personales por parte de proveedores.
	Recopilación de datos personales de fuentes informales.
Cambio en el procesamiento	Uso no previsto dentro de las finalidades consentidas para los datos personales.
	Manipulación de aplicaciones que procesan datos personales eludiendo la autenticación.
	Alteración del hardware donde se procesan o almacenan datos personales.
	Uso anormal del software de procesamiento de datos personales.
	Compromiso de los canales de comunicación de cómputo.
Cambios no deseados en los	Error en el registro de datos personales.

Categoría de Evento de Riesgo	Evento de Riesgo
datos personales	Corrupción de la información almacenada en el banco de datos personales.
	Eliminación no controlada de datos personales.
	Procesamiento no trazable de datos personales.
	Introducción de falsa información en el banco de datos personales.
	Alteración del software de procesamiento de datos personales.
	Sobrecarga laboral.
	Falsificación de documentos físicos.
	Alteración de documentos físicos con datos personales durante su traslado.
Compromiso del procesamiento	Demora en la atención de derechos ARCO.
	Suplantación de la identidad del usuario autorizado.
	Deficiencias del proceso de atención de derechos ARCO.
	Utilización inadecuada de claves de acceso y niveles de autorización.
	Vulnerabilidades en los sistemas inalámbricos y equipos móviles.
	Vulneración de los sistemas de identificación y seguridad.
	Denegación del servicio del proveedor de datos personales.
	Denegación del servicio del encargado del banco de datos personales.
Desaparición de los datos personales	Extravío de documentos que contienen datos personales.
	Robo de documentos que contienen datos personales.
	Robo y fraude por parte de terceros para uso indebido.
	Borrado de documentos físicos con datos personales.
	Daño a documentos físicos con datos personales.
Indisponibilidad del procesamiento	Sobrecarga de utilización del hardware de procesamiento y/o almacenamiento de datos personales.
	Daños al hardware de procesamiento y/o almacenamiento de datos personales.
	Sobrecarga del software de procesamiento y/o almacenamiento de datos personales.
	Borrado total o parcial de programas para el procesamiento de datos personales.
	Licencia de software de procesamiento de datos personales no renovada.
	Sobrecarga de los canales de comunicación de cómputo.
	Daño a canales de comunicación de cómputo.
	Desaparición de los canales de comunicación de cómputo.
	Daños al personal que procesa y/o almacena datos personales.
	Salida del personal que procesa y/o almacena datos personales.
	Sobrecarga de los canales de transporte de documentos físicos con datos personales.
	Interrupción de los canales de transporte de documentos físicos con datos personales.
	Alteración de los canales de transporte de documentos físicos con datos personales.
	Desaparición de los canales de transporte de documentos físicos con datos personales.

Categoría de Evento de Riesgo	Evento de Riesgo
Modificación del proceso legal	Cambios en el proceso legal que afectan los derechos de acceso de los titulares de datos personales.
	Uso desproporcionado de datos personales para la finalidad consentida.

ANEXO B

Identificación, Análisis, Evaluación y Tratamiento de Riesgos

N°	Evento de Riesgo	Vulnerabilidad	Control Existente	Probabilidad	Impacto	Nivel de Riesgo	Grado de Aceptación	Opción de Tratamiento	Riesgo Residual	Priorización

- **N°:** Se coloca un código correlativo que tiene la forma: R.PRIV.<número>; Ejemplo: R.PRIV.5
- **Evento de Riesgo:** Se coloca la descripción del riesgo a la privacidad de datos personales.
- **Vulnerabilidad:** Es la descripción de la debilidad o falta de control referida a los datos personales.
- **Control Existente:** Es la descripción del control o la medida que se tiene paliar el riesgo.
- **Probabilidad:** Es el nivel que se encuentra definido en el cuadro Nivel de Probabilidad.
- **Impacto:** Es el nivel que se encuentra definido en el cuadro Nivel de Impacto.
- **Nivel de Riesgo:** Es el nivel que resulta de cruzar los valores de probabilidad e impacto en función del Mapa de Criticidad del Nivel de Riesgo.
- **Grado de Aceptación:** Es el grado que se encuentra definido de acuerdo a lo especificado para el uso del cuadro de Criterios de Aceptación de Riesgo.
- **Opción de Tratamiento:** Es la opción definida de acuerdo a las definiciones de Opciones de Tratamiento que se eligen de acuerdo a las decisiones que tome la organización respecto de cada uno de los riesgos.
- **Riesgo Residual:** Es el riesgo resultante luego de la aplicación de la opción de tratamiento, toma los valores Mapa de Criticidad del Nivel de Riesgo.
- **Grado de Aceptación Resultante:** Es el grado de aceptación acorde al nivel de riesgo residual obtenido, se consignan valores de Criterios de Aceptación de Riesgo.
- **Priorización:** Está en función a los valores de priorización del riesgo que se definen de acuerdo a la importancia que la organización le de a cada riesgo en función del cumplimiento del marco de la LPDP.

ANEXO C

Plan de Tratamiento de Riesgos

N°	Evento de Riesgo	Acción de Tratamiento	Responsable	Priorización	Plazo de Ejecución	Fecha Inicio	Fecha Fin	Responsable de Seguimiento

- **N°:** Se coloca el código del riesgo.
- **Evento de Riesgo:** Se coloca la descripción del riesgo a la privacidad de datos personales.
- **Acción de Tratamiento:** Se consigna la acción que permitirá tratar el riesgo.
- **Responsable:** Se coloca el cargo del responsable de la ejecución del riesgo.
- **Priorización:** Se hereda del riesgo, cada una de las acciones de tratamiento asumirán el mismo nivel de prioridad.
- **Plazo de Ejecución:** Puede ser corto, mediano y largo plazo; de acuerdo al nivel de complejidad y prioridad de cada acción.
- **Fecha Inicio:** Es la fecha programada para el inicio de la ejecución de la acción de tratamiento que debe ser acorde al Plazo de Ejecución.
- **Fecha Fin:** Es la fecha programada para la finalización de la acción de tratamiento.
- **Responsable de Seguimiento:** Es el responsable de realizar el seguimiento de la realización de las acciones de tratamiento y de velar que se cumplan los tiempos programados.

Matriz de Riesgos

				Riesgo Inherente			Respuesta al Riesgo	
Sub Proceso	**Codigo del Riesgo**	**Descripción de Riesgo**	**Tipo de Riesgo**	**Probabilidad**	**Impacto**	**Nivel**	**Evitar**	**Reducir**
Obtención de datos personales Post venta /Comercial	CR001	Error en el registro de datos personales en el sistema que soporta el banco de datos de clientes lo que provoca que exista información inexacta y no se cumpla con el principio de calidad de la LPDP.	Riesgo Estrategico	2	2	4		x
Obtención de datos personales Post venta /Comercial /Repuestos	CR002	No cumplir con el procedimiento de bloquear a los clientes en el sistema lo que provoca denuncias y/o multas.	Riesgo Estrategico	3	3	9		x
Obtención de datos personales Post venta /Comercial	CR003	Extravío de file de cliente que contiene documentación de la venta de vehículos, servicios , quedando expuesta toda la informacion del cliente que puede ser aprovechada para finalidades no autorizadas y causar denuncias por parte de los titulares de datos personales.	Riesgo Estrategico	3	3	9		x
Obtención de datos personales Organización	CR004	Error de la información almacenada en el banco de datos personales de clientes (SIMA), lo cual origina problemas para las actividades de marketing.	Riesgo Estrategico	3	3	9		x
Obtención de datos personales MKT	CR005	Uso de datos personales sin consentimiento por parte de los Asesores Comerciales/Taller , puede provocar denuncias por parte de los titulares de datos personales.	Riesgo Estrategico	3	3	9		x
Obtención de datos personales MKT	CR006	Enviar comunicaciones de marketing sin el consentimiento adecuado o envío de promociones no solicitadas por no realizar el proceso de registro de consentimiento de datos correctamente	Riesgo Estrategico	2	2	4		x
Obtención de datos personales	CR007	Pérdida y/ o robo de dispositivos móviles que almacenan datos personales puede provocar que estos sean utilizados en forma ilítica y se generen denuncias en contra de la Organización	Riesgo Estrategico	3	2	6	X	
Accesos y Privilegios Sistemas	CR008	La gestión inadecuada de credenciales de usuario, pueden permitir el acceso no autorizado a cuentas de clientes y a la información sensible almacenada en nuestros sistemas	Operacional	2	2	4		x
Soporte Fisicos Almacenes	CR010	Posible perdida y daños en los documentos de los almacenes de repositorios fisicos que contienen datos personales, esto puede causar el incumplimiento ante alguna auditoria de APDP y ser causantes de multas .	Riesgo Estrategico	2	2	4	X	
Citas de taller	CR011	Recopilación de datos personales via telefonica(citas de taller) donde NO se solicita el consentimiento de proteccion de datos personales esto provocaría el incumplimiento con la LPDP lo que puede ser causante de sanciones y multas por parte de la APDP.	Riesgo Estrategico	3	2	6	X	
Accesos y Privilegios Sistemas	CR012	Accesos y privilegios a colaboradores no autorizados a otras empresas del grupo ,teniendo acceso a informacion de otros clientes lo cual puede causar el mal uso de los datos.	Operacional	3	2	6		X
Soporte Fisicos Almacenes	CR013	Revisión y/o alteración de documentos físicos con datos personales durante su traslado por parte de proveedores de mensajería, puede generar denuncias por parte del titular de datos personales en contra de la empresa.	Operacional	2	2	4	X	
Accesos y Privilegios Sistemas	CR014	Equipos de procesamiento de datos personales desatendidos pueden ser utilizados para realizar operaciones no autorizadas con datos personales.	Riesgo Estrategico	2	2	4	X	
Obtención de datos personales Post venta /Comercial	CR015	Uso de datos personales sin prueba de consentimiento trazable que puede provocar que no se tenga la capacidad de evidenciar cumplimiento ante la APDP.	Riesgo Estrategico	2	2	4		X

ANEXO 10.15
POLITICA DE INTERCAMBIO DE INFORMACION FISICA –DATOS PERSONALES

1. OBJETIVO

Proteger la Información que se intercambia o transfiere dentro de la Organización o con cualquier entidad externa haciendo uso de los recursos de Comunicación.

2. ALCANCE

El siguiente documento involucra a todas las Gerencias, áreas y personal de la Organización que participan en el proceso de traslado o intercambio de Datos Personales, por cualquier medio, dentro de la propia empresa o fuera de esta.

3. RESPONSABILIDADES

Así mismo, el responsable de tratamiento debe mantener un registro trazable del intercambio de información, que se realice por medios o soportes físicos.

4. DESARROLLO

Todo intercambio de información que contenga datos personales, contenidos en soportes físicos hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales, el responsable de tratamiento deberá de llevar un registro considerando los siguientes puntos.

- Origen.
- Motivo del intercambio o traslado de información.
- Responsable.
- Medio empleado
- Medida de seguridad.
- Destino.
- Responsable (Destino)

La información que contenga datos personales debe ser trasladada contemplando mecanismos de seguridad apropiados, entre ellos: sobre lacrados, cajas de seguridad, maletines con clave o candado. En caso de transporte por empresas del rubro debe suscribirse un compromiso de confidencialidad y protección de datos personales, etc.

ANEXO 10.16

POLITICA DE INTERCAMBIO DE INFORMACION POR MEDIOS REMOVIBLES DE ALMACENAMIENTO.

1 .OBJETIVO

Establecer los métodos sobre la protección de la información, cuando esta sea trasladada o intercambiada por medios removibles.

2. **ALCANCE**

El siguiente documento involucra a todas las Gerencias, áreas y personal de la Organización que participan en el proceso de traslado o almacenamiento de Información que contengan Datos Personales, por medio removibles, dentro de la propia empresa o fuera de esta.

3. **RESPONSABILIDADES**

Así mismo, el responsable de tratamiento debe mantener un registro trazable del intercambio de información, que se realice por medios removibles de almacenamiento.

4. DESARROLLO

- El acceso a equipos informáticos se encuentran restringidos.
- Para contar con el acceso, es necesario que el trabajador cuente con un documento de permiso firmado por Gerencia. (Solicitud de Acceso de dispositivos Informáticos).
- En los casos se cuente con el acceso, el responsable deberá de contar con un registro.
- Toda información electrónica que contenga datos personales debe ser almacenadas en forma seguro empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.
- En el caso de los sistemas informáticos, la oficina de TI, deberá de aplicar las medidas de control de acceso y cifrado a la base de datos que contengan datos personales.
- Para el caso de archivos que contengan datos personales, los encargados de tratamiento son responsables de cifrar la información mediante una contraseña.

ANEXO 11

ASIGNACION DE RESPONSABILIDADES PARA EL USO EXCLUSIVO Y ADMINISTRACION DE EQUIPOS Y COMPROMISO PARA LA PROTECCION DE DATOS PERSONALES

Conste por el presente documento la Asignación de Responsabilidades para el Uso Exclusivo y Administración de Equipos y Compromiso para la Protección de Datos Personales que suscribe el señor(a) _____, identificado(a) con D.N.I. N° _____, con domicilio en _____, (en adelante simplemente el colaborador) quien procede en su calidad colaborador de la empresa _____, con R.U.C. N° _____, y con domicilio en _____, con (en adelante simplemente la empresa), ejerciendo el cargo de _____; en los siguientes términos:

Por el presente documento, el colaborador recibe de la empresa el uso exclusivo y la administración de(l)(la) _____, marca _____, modelo _____, Serie N° _____ (en adelante simplemente el equipo), única y exclusivamente para fines del cumplimiento de sus labores y de las tareas propias y requeridas para el impulso y desarrollo de las actividades y necesidades de la empresa. El colaborador será el único autorizado a darle uso al equipo, así como será el responsable de administrar y supervisar su uso por parte de otros trabajadores o colaboradores de la empresa para el cumplimiento de sus funciones, siempre bajo su supervisión directa, cuidando que el equipo no sea utilizado ni aprovechado por ningún tercero ni para fines no autorizados ajenos a los intereses y actividades de la empresa. Para el cumplimiento de las funciones respecto del equipo que le ha sido asignado a su uso y administración, el colaborador deberá cumplir con las siguientes obligaciones:

1.- El colaborador se obliga a mantener confidencialidad sobre toda y cualquier información, planos, diseños, informes, resultados, estrategias, estructuras, programas, equipos, mercadeo, costos, especificaciones técnicas, usos, procedimientos, instalaciones, proyectos, información comercial, estratégica, publicitaria, operativa, financiera, legal, societaria, datos personales y de identificación a los que haya podido tener acceso, nombres, apellidos, huella dactilar, perfil, dirección, números telefónicos, correos electrónicos, imagen, características e información de vehículos, incidencias de servicio, comportamiento y de desempeño de funcionamiento de vehículos y de todo aquello que registren los módulos informáticos o computadoras de a bordo de estos, artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, preferencias e intereses en general, datos económicos, financieros y de seguros, relaciones sociales, entre otros a los que pudiere acceder, y toda otra clase de información que pueda manejar o recibir con relación a los servicios prestados a la empresa o por la empresa, sus clientes, sus potenciales clientes y prospectos, así como el personal, empresas vinculadas, afiliadas, contratistas, y cualquier persona en general, independientemente de la relación o condición que pudieren tener, y toda clase de información que pueda manejar o recibir al hacer uso y/o administrar y/o supervisar la utilización por parte de otros colaboradores, que pudiere haber obtenido mediante los equipos, así como también asegurar que esta confidencialidad sea cumplida por éstos.

2.- El colaborador se encuentra obligado al cumplimiento taxativo e ineludible de la Ley de Protección de Datos Personales, su Reglamento, así como todas las normas concordantes, creadas o por crearse; de igual manera, se obliga al cumplimiento del Código de Conducta para la protección de datos personales que rige en la empresa, que declara conocer. En tal sentido, en caso el colaborador, en cumplimiento de las obligaciones que desempeña y/o en razón del uso y administración del equipo que le ha sido asignado, tuviera acceso total o parcial, directo o indirecto, o bajo cualquier modalidad a la base de datos de la empresa, o tuviera que manejar o tratar cualquier tipo de dato personal, ello será única y exclusivamente de carácter temporal y para el cumplimiento de sus funciones, por lo que está prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en el cualquier tipo de soporte, sea cual fuere su naturaleza.

3.- El colaborador es el único responsable de asegurar que, mediante el uso del equipo, ya sea de manera directa o través de la supervisión en su uso por parte de otros colaboradores, se dé debido cumplimiento y respeto a las normas de protección de datos personales. De esta manera, a excepción de las situaciones propias del tratamiento de datos necesarios para el cumplimiento de sus funciones y labores, el colaborador queda expresamente prohibido de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuviere acceso o conociera, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que conociera en razón del uso y/o administración y/o supervisión en la utilización por parte de otros colaboradores, de los equipos; así como también, asegurar que estas obligaciones sean cumplidas por parte de los otros colaboradores que usen el equipo. Sin embargo, en caso el colaborador tuviera que realizar el tratamiento de cualquier dato personal de la base de datos de la empresa para el cumplimiento de sus funciones y del cargo que ostenta, éste deberá realizarse cumpliendo taxativamente las condiciones contenidas en el consentimiento expreso para tratamiento de datos personales suscrito por la persona cuyos datos se deban tratar, o para las finalidades cuyo tratamiento se encuentre exceptuado por ley de contar con dicho consentimiento, y que el colaborador tiene la obligación de conocer y consultar antes de realizar cualquier tipo de tratamiento.

4.- Finalmente, el colaborador asume el firme compromiso de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndose en una mejora continua. Declarando conocer y obligarse a cumplir nuestra Política de Privacidad publicada en _____, así como nuestro Código de Conducta para la protección de datos personales publicada en www.euromotors.com.pe.

Firmado en la fecha :

Nombre del Colaborador :

Documento de Identidad :

Dirección :

Cargo :

Firma del Colaborador :

ANEXO 12
CLAUSULA DE CONFIDENCIALIDAD DE LOS COLABORADORES
PARA LA PROTECCION DE DATOS PERSONALES

1.- El colaborador se obliga a mantener confidencialidad absoluta sobre la celebración y ejecución de su contrato de trabajo y/o de servicios y sobre toda y cualquier información, planos, diseños, informes, resultados, estrategias, estructuras, programas, equipos, mercadeo, costos, especificaciones técnicas, usos, procedimientos, instalaciones, proyectos, datos personales, y toda otra clase de información que pueda manejar o recibir con relación a los servicios prestados a la empresa o por la empresa, sus clientes, sus potenciales clientes y prospectos, así como el personal, empresas vinculadas, afiliadas, contratistas, y cualquier persona en general, independientemente de la relación o condición que pudieren tener.

2.- Asimismo, el colaborador se obliga a mantener absoluta confidencialidad sobre toda información comercial, estratégica, publicitaria, operativa, financiera, legal, societaria y datos personales y de identificación a los que haya podido tener acceso como consecuencia del desarrollo de su actividades, debiendo proteger y asegurar plena confidencialidad respecto de datos personales como, nombres, apellidos, datos de identificación, huella dactilar, perfil, dirección, números telefónicos, correos electrónicos, imagen, características e información de vehículos, incidencias de servicio, comportamiento y de desempeño de funcionamiento de vehículos y de todo aquello que registren los módulos informáticos o computadoras de a bordo de estos, artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, preferencias e intereses en general, datos económicos, financieros y de seguros, relaciones sociales, entre otros a los que pudiere acceder.

3.- El colaborador se encuentra obligado al cumplimiento taxativo e ineludible de la Ley de Protección de Datos Personales, su Reglamento, así como todas las normas concordantes, creadas o por crearse; de igual manera, se obliga al cumplimiento del Código de Conducta para la protección de datos personales que rige en la empresa, que declara conocer. En tal sentido, en caso el colaborador, en cumplimiento de las obligaciones que desempeña, tuviera acceso total o parcial, directo o indirecto, o bajo cualquier modalidad a la base de datos de la empresa, o tuviera que manejar o tratar cualquier tipo de dato personal, ello será única y exclusivamente de carácter temporal y para el cumplimiento de sus labores, por lo que está prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en el cualquier tipo de soporte, sea cual fuere su naturaleza.

4.- El colaborador únicamente podrá utilizar la información y/o cualquier dato personal proporcionado por la empresa para cumplir con los encargos específicos de sus labores, y nunca para otra finalidad, ni mucho menos en otra oportunidad. De esta manera, el colaborador queda expresamente prohibido de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuviere acceso o conociera durante la vigencia de su relación con la empresa, para fines no autorizados y/o ajenos a sus obligaciones, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que la empresa le haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno; asumiendo plena responsabilidad por las consecuencias y sanciones que se deriven del uso indebido por parte de él o terceras personas relacionadas. En caso el colaborador tuviera que realizar el tratamiento de cualquier dato personal de la base de datos de la empresa, éste deberá realizarse cumpliendo taxativamente las condiciones contenidas en el consentimiento expreso para tratamiento de datos personales suscrito por la persona cuyos datos se deban tratar, o para las finalidades cuyo tratamiento se encuentre exceptuado por ley de contar con dicho consentimiento, y que el colaborador tiene la obligación de conocer y consultar antes de realizar cualquier tipo de tratamiento.

5.- En concordancia con lo anterior, toda información o datos personales que sean proporcionados al colaborador o a la que tenga acceso para el cumplimiento de sus funciones, sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada. Toda la información y datos personales será de carácter confidencial, deberá ser mantenida bajo estricta reserva y no será suministrada a persona alguna excepto a las personas que indispensablemente tengan la necesidad de conocer la misma para la realización de sus labores.

6.- La obligación del colaborador de mantener la confidencialidad, reserva, y protección de la información, datos personales y/o documentación mencionada en este documento se mantendrá vigente y regirá incluso después de la anulación, terminación, rescisión o resolución de la relación contractual que tenga con la empresa, cualquiera fuese su causa, de manera indefinida.

7.- Finalmente, el colaborador asume el firme compromiso de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndose en una mejora continua. Declarando conocer y obligarse a cumplir nuestra Política de Privacidad publicada en _____, así como nuestro Código de Conducta para la protección de datos personales publicada en www.euromotors.com.pe.

8.- Con el objeto de poder cumplir con los objetivos de las relaciones y vínculos que sostiene el colaborador con _____, éste declara conocer y haber sido informado que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte como colaborador, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, en la que está involucrada y forman parte directa el fabricante de los vehículos que comercializa, su importador, y los concesionarios autorizados a comercializar dichos vehículos, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales, es decir, sin necesidad de consentimiento previo, incluyendo encargos de tratamiento y/o transferencias.

Firmado en la fecha :

Nombre del Colaborador :

Documento de Identidad :

Dirección :

Cargo :

Firma del Colaborador :

ANEXO 13

ASIGNACION DE RESPONSABILIDADES PARA LA ADMINISTRACION DE ARCHIVOS FISICOS Y COMPROMISO PARA LA PROTECCION DE DATOS PERSONALES

Conste por el presente documento la Asignación de Responsabilidades para la Administración de Archivos Físicos y Compromiso para la Protección de Datos Personales que suscribe el señor(a) _____, identificado(a) con D.N.I. N° _____, con domicilio en _____, (en adelante simplemente el colaborador) quien procede en su calidad colaborador de la empresa _____, con R.U.C. N° _____, y con domicilio en _____, con (en adelante simplemente la empresa), ejerciendo el cargo de _____; en los siguientes términos:

Por el presente documento, el colaborador recibe de la empresa la administración del archivo físico en el que se almacena el acervo documentario que contiene datos personales recabados por la empresa ubicado en el local _____, (en adelante simplemente el archivo), para fines de su cuidado, gestión, administración, resguardo, protección, seguridad y confidencialidad, recibiendo y haciéndose responsables de las llaves y de su acceso. El colaborador será el único autorizado a acceder y gestionar el uso del archivo, así como será el responsable de administrar y supervisar su uso por parte de otros trabajadores o colaboradores de la empresa para el cumplimiento de sus funciones, siempre bajo su supervisión directa, cuidando que el archivo no sea utilizado, vulnerado ni aprovechado por ningún tercero para fines no autorizados ajenos a los intereses y actividades de la empresa. Para el cumplimiento de las funciones respecto del archivo que le ha sido asignado para su protección y administración, el colaborador deberá cumplir con las siguientes obligaciones:

1.- El colaborador se obliga a mantener confidencialidad sobre toda y cualquier información, planos, diseños, informes, resultados, estrategias, estructuras, programas, equipos, mercadeo, costos, especificaciones técnicas, usos, procedimientos, instalaciones, proyectos, información comercial, estratégica, publicitaria, operativa, financiera, legal, societaria, datos personales y de identificación a los que haya podido tener acceso, nombres, apellidos, huella dactilar, perfil, dirección, números telefónicos, correos electrónicos, imagen, características e información de vehículos, incidencias de servicio, comportamiento y de desempeño de funcionamiento de vehículos y de todo aquello que registren los módulos informáticos o computadoras de a bordo de estos, artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, preferencias e intereses en general, datos económicos, financieros y de seguros, relaciones sociales, entre otros a los que pudiere acceder, y toda otra clase de información que pueda manejar o recibir con relación a los servicios prestados a la empresa o por la empresa, sus clientes, sus potenciales clientes y prospectos, así como el personal, empresas vinculadas, afiliadas, contratistas, y cualquier persona en general, independientemente de la relación o condición que pudieren tener, y toda clase de información que pueda manejar o recibir al hacer uso y/o administrar y/o supervisar la utilización por parte de otros colaboradores, que pudiere haber obtenido mediante el archivo, así como también asegurar que esta confidencialidad sea cumplida por éstos.

2.- El colaborador se encuentra obligado al cumplimiento taxativo e ineludible de la Ley de Protección de Datos Personales, su Reglamento, así como todas las normas concordantes, creadas o por crearse; de igual manera, se obliga al cumplimiento del Código de Conducta para la protección de datos personales que rige en la empresa, que declara conocer. En tal sentido, en caso el colaborador, en cumplimiento de las obligaciones que desempeña y/o en razón del uso y administración del archivo que le ha sido asignado, tuviera acceso total o parcial, directo o indirecto, o bajo cualquier modalidad a la base de datos de la empresa, o tuviera que manejar o tratar cualquier tipo de dato personal, ello será única y exclusivamente de carácter temporal y para el cumplimiento de sus funciones, por lo que está prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en el cualquier tipo de soporte, sea cual fuere su naturaleza.

3.- El colaborador es el único responsable de asegurar que, mediante la protección, gestión y uso del archivo, ya sea de manera directa o través de la supervisión en su uso por parte de otros colaboradores, se dé debido cumplimiento y respeto a las normas de protección de datos personales. De esta manera, a excepción de las situaciones propias del tratamiento de datos necesarios para el cumplimiento de sus funciones y labores, el colaborador queda expresamente prohibido de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuviere acceso o conociera, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que conociera en razón del uso y/o administración y/o supervisión en la utilización por parte de otros colaboradores, del archivo; así como también, asegurar que estas obligaciones sean cumplidas por parte de los otros colaboradores que usen el archivo. Sin embargo, en caso el colaborador tuviera que realizar el tratamiento de cualquier dato personal de la base de datos de la empresa para el cumplimiento de sus funciones y del cargo que ostenta, éste deberá realizarse cumpliendo taxativamente las condiciones contenidas en el consentimiento expreso para tratamiento de datos personales suscrito por la persona cuyos datos se deban tratar, o para las finalidades cuyo tratamiento se encuentre exceptuado por ley de contar con dicho consentimiento, y que el colaborador tiene la obligación de conocer y consultar antes de realizar cualquier tipo de tratamiento.

4.- Finalmente, el colaborador asume el firme compromiso de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndose en una mejora continua. Declarando conocer y obligarse a cumplir nuestra Política de Privacidad publicada en _____, así como nuestro Código de Conducta para la protección de datos personales publicada en www.euromotors.com.pe.

Firmado en la fecha :

Nombre del Colaborador :

Documento de Identidad :

Dirección :

Cargo :

Firma del Colaborador :

ANEXO 14
CLAUSULA DE CONFIDENCIALIDAD PARA PROVEEEDORES Y TERCEROS
PARA LA PROTECCION DE DATOS PERSONALES

1.- Todo proveedor y tercero que tenga alguna relación con _____, se obliga a mantener confidencialidad absoluta sobre la celebración y ejecución de su contrato y/o vinculación, y sobre toda y cualquier información, planos, diseños, informes, resultados, estrategias, estructuras, programas, equipos, mercadeo, costos, especificaciones técnicas, usos, procedimientos, instalaciones, proyectos, datos personales, y toda otra clase de información que pueda manejar o recibir con relación a dicha relación con la empresa, sus clientes, sus potenciales clientes y prospectos, así como el personal, empresas vinculadas, afiliadas, contratistas, y cualquier persona en general, independientemente de la relación o condición que pudieren tener.

2.- Asimismo, el proveedor y tercero se obliga a mantener absoluta confidencialidad sobre toda información comercial, estratégica, publicitaria, operativa, financiera, legal, societaria y datos personales y de identificación a los que haya podido tener acceso como consecuencia de la relación o vinculación que pudiese tener con la empresa, debiendo proteger y asegurar plena confidencialidad respecto de datos personales como, nombres, apellidos, datos de identificación, huella dactilar, perfil, dirección, números telefónicos, correos electrónicos, imagen, características e información de vehículos, incidencias de servicio, comportamiento y de desempeño de funcionamiento de vehículos y de todo aquello que registren los módulos informáticos o computadoras de a bordo de estos, artículos o servicios de interés, victorias y/o participación en promociones comerciales, concursos y/o sorteos, preferencias e intereses en general, datos económicos, financieros y de seguros, relaciones sociales, entre otros a los que pudiere acceder.

3.- El proveedor y tercero se encuentra obligado al cumplimiento taxativo e ineludible de la Ley de Protección de Datos Personales, su Reglamento, así como todas las normas concordantes, creadas o por crearse; de igual manera, se obliga al cumplimiento del Código de Conducta para la protección de datos personales que rige en la empresa, que declara conocer. En tal sentido, en caso el proveedor o tercero, como consecuencia de la relación o vinculación que tenga con la empresa, tuviera acceso total o parcial, directo o indirecto, o bajo cualquier modalidad a la base de datos de la empresa, o tuviera que manejar o tratar cualquier tipo de dato personal, ello será única y exclusivamente de carácter temporal y para el cumplimiento de la obligación o tarea que tuviere que cumplir, por lo que está prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en el cualquier tipo de soporte, sea cual fuere su naturaleza.

4.- El proveedor y tercero únicamente podrá utilizar la información y/o cualquier dato personal proporcionado por la empresa para cumplir con los encargos específicos de la relación o vinculación que lo une, y nunca para otra finalidad, ni mucho menos en otra oportunidad. De esta manera, el proveedor y tercero queda expresamente prohibido de realizar cualquier tipo de tratamiento, parcial o total, bajo cualquier medio o soporte, de cualquier tipo de información y/o datos personales a la que tuviere acceso o conociera durante la vigencia de su relación con la empresa, para fines no autorizados y/o ajenos a sus obligaciones, así como también, está prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir o permitir que terceros puedan tener acceso a los datos personales y a toda y cualquier información que la empresa le haya podido proporcionar, la cual no podrá ser usada por absolutamente nadie ni para ningún fin ajeno; asumiendo plena responsabilidad por las consecuencias y sanciones que se deriven del uso indebido por parte de él o terceras personas relacionadas. En caso el proveedor o tercero tuviera que realizar el tratamiento de cualquier dato personal de la base de datos de la empresa, éste deberá realizarse cumpliendo taxativamente las condiciones contenidas en el consentimiento expreso para tratamiento de datos personales suscrito por la persona cuyos datos se deban tratar, o para las finalidades cuyo tratamiento se encuentre exceptuado por ley de contar con dicho consentimiento, y que el proveedor y tercero tiene la obligación de conocer y consultar antes de realizar cualquier tipo de tratamiento.

5.- En concordancia con lo anterior, toda información o datos personales que sean proporcionados al proveedor y tercero o a la que tenga acceso para el cumplimiento de los objetivos de su relación o vinculación con la empresa, sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada. Toda la información y datos personales será de carácter confidencial, deberá ser mantenida bajo estricta reserva y no será suministrada a persona alguna excepto a las personas que indispensablemente tengan la necesidad de conocer la misma para la realización de sus labores.

6.- La obligación del proveedor y tercero de mantener la confidencialidad, reserva, y protección de la información, datos personales y/o documentación mencionada en este documento se mantendrá vigente y regirá incluso después de la anulación, terminación, rescisión, resolución o terminación de la relación o vinculación que tenga con la empresa, cualquiera fuese su causa, de manera indefinida.

7.- Finalmente, el proveedor y tercero asume el firme compromiso de cumplir, respetar y garantizar la protección de los datos personales de sus titulares, en pleno respeto de los principios de Legalidad, Consentimiento, Finalidad, Proporcionalidad, Calidad, Disposición de Recurso y de Nivel de Protección Adecuado, así como de los requisitos de seguridad aplicables, manteniéndose en una mejora continua. Declarando conocer y obligarse a cumplir nuestra Política de Privacidad publicada en _____, así como nuestro Código de Conducta para la protección de datos personales publicada en www.euromotors.com.pe.

8.- Con el objeto de poder cumplir con los objetivos de las relaciones y vínculos que sostiene el proveedor y tercero con _____, éste declara conocer y haber sido informado que sus datos personales son necesarios e indispensables para la preparación, celebración y ejecución de la relación contractual en la que es parte como proveedor y tercero, por lo que los mismos podrán y serán tratados para el cumplimiento de esa finalidad contractual, conforme a la excepción regulada en el inciso 5) del artículo 14° de la Ley de Protección de Datos Personales, es decir, sin necesidad de consentimiento previo.

Firmado en la fecha :

Nombre del Proveedor o Tercero :

Documento de Identidad :

Dirección :

Cargo :

Firma del Proveedor o Tercero :

Cláusula Contractual - Protección de Datos Personales

1.- Bajo el marco de la Ley de Protección de Datos Personales, _____ y sus respectivos representantes legales que suscriben el presente contrato autorizan expresamente a _____, otorgando consentimiento voluntario, libre, previo, expreso, informado e inequívoco, para incorporar en sus bancos de datos, la información personal contenida en el presente documento, toda aquella derivada de sus relaciones comerciales, tratativas, contractuales, y obligacionales en general, la obtenida por fuente pública y en cualquier otro documento suscrito entre ellas de ser el caso; autorizándola utilizar dichos datos personales para fines administrativos, laborales, contractuales, de locación de servicios, obligacionales, comerciales, de publicidad, de segmentación, estadísticos, de ubicación, de ofrecimiento y/o negociación y/o contratación de productos y servicios, de investigación, seguridad, de asesoría, de contacto, de promociones comerciales, concursos, sorteos, programas de lealtad y/o recompensas, de avisos, encuestas, comunicaciones, individual y/o masiva de productos y servicios, y de ofrecimientos en general, incluyendo las comunicaciones y el tratamiento mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular, o de mensajes electrónicos masivos, y a través de cualquier tipo de comunicación electrónica, telefónica, escrita, virtual, aplicaciones informáticas, o bajo cualquier medio o plataforma, incluyendo redes sociales e interfaces digitales; así como también para dar a conocer sus datos personales, así como su puntualidad o morosidad en sus obligaciones económicas, proporcionando dicha información a las centrales de riesgo, registros administrativos o cualquier registro de historiales crediticios; todo ello, por plazo indefinido.

Los datos personales recogidos serán incorporados y tratados en el Banco de Datos de titularidad _____, declarado ante la Autoridad de Datos Personales, cuya existencia conoce el otorgante, que es automatizado y no automatizado, garantizándose las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos.

El otorgamiento de los datos es de carácter facultativo, y no hay obligación de proporcionarlos, a excepción de aquellos necesarios para la ejecución de las relaciones administrativas, comerciales, contractuales, laborales, de locación de servicios, tratativas, obligacionales en general, o en los supuestos permitidos por ley, para los cuales no se requiere consentimiento.

Los datos serán tratarlos con veracidad, calidad y proporcionalidad; la negativa a otorgarlos impedirá su tratamiento, a excepción de los supuestos permitidos por ley. El otorgante de este documento tiene la facultad de solicitar en cualquier momento y de manera gratuita e irrestricta tener acceso a la información de los datos personales proporcionados por éste, la forma y razones por la que los otorgó, las transferencias realizadas o que se prevén hacer, así como a actualizarlos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos. Para ello, el otorgante podrá ejercer dichos derechos enviando una comunicación escrita simple al domicilio físico precisado al inicio de este documento, haciendo precisión de su pedido, el cual será atendido dentro del plazo de ley.

El responsable de este Banco de Datos es _____, y su destino será el mismo Banco de Datos. En tal sentido, asegura y garantiza que, todo y cualquier dato personal que haya recopilado de manera legítima y con arreglo a ley, será tratado única y exclusivamente para cumplir con la finalidad para lo cual haya sido otorgado, y en los casos permitidos por ley cuyo tratamiento no requiere de consentimiento previo, para cumplir con las finalidades respectivas en ese sentido, tales como, uso de datos de acceso público, uso de datos para la preparación, celebración y ejecución de relaciones contractuales o profesionales necesarias para su desarrollo o cumplimiento, para fines de cumplimiento de las normas contra el lavado de activos y el financiamiento del terrorismo, por mandato legal, por orden de autoridad en ejercicio de sus funciones expresamente establecidas por ley, entre otras que legalmente estén establecidas, conforme a las excepciones reguladas en el artículo 14° de la Ley de Protección de Datos Personales; incluyendo para ello las transferencias de datos, a nivel nacional e internacional que sean necesarias y estén justificadas en las excepciones de Ley.

2.- Por otro lado, se deja expresa constancia que _____es titular del Banco de Datos Personales de administración privada en el cual ha recopilado y continua recopilando información de sus clientes proporcionada de manera consentida e informada para las finalidades y destino autorizados, y bajo las condiciones, restricciones derechos y deberes convenidos con los mismos, que las partes declaran conocer; base de datos que también se nutre sin necesidad de consentimiento, siempre que el mismo está justificado en cualquiera de las excepciones establecidas por ley. Dichos datos personales están incorporados en un Banco de Datos Privados que garantizan las medidas de seguridad técnica, organizativa y legal para el tratamiento, seguridad y confidencialidad de los datos; deber de protección de datos personales que involucra a todas las personas de manera general.

De esta manera, por el presente documento, se deja expresamente establecido que toda transferencia de datos o encargo de tratamiento de estos entre las partes, o cualquier actividad mediante la cual las partes requieran compartir o comunicar datos personales para efectos de la ejecución del presente contrato y de que el mismo pueda cumplir con su finalidad, se deberá realizar manteniendo el más alto grado de seguridad y confidencialidad, tanto a nivel técnico, organizativo como jurídico. Declarando conocer y obligarse la Política de Privacidad publicada en _____, así como el Código de Conducta para la protección de datos personales publicada en www.euromotors.com.pe.

El receptor de los datos, ya sea por transferencia o simple encargo de tratamiento, se obliga a respetar y cumplir de manera irrestricta absolutamente todas las condiciones para la protección y tratamiento de los datos personales que le son transferidos o encargados para tratamiento, conforme a las estipulaciones y finalidades necesarias, y únicamente para el cumplimiento de la finalidad de este contrato. En caso de encargo, éste será para un tratamiento específico y temporal, y siempre para el debido cumplimiento de la finalidad de este contrato. En tal sentido, el receptor deberá asegurar que los datos personales que recibe sean tratados con seguridad y confidencialidad, y únicamente para el cumplimiento de la finalidad de este contrato.

El receptor de los datos deberá cumplir de manera inmediata con proporcionar acceso a la información de los datos personales proporcionados a sus titulares, la forma y razones por la

que los otorgaron, las transferencias realizadas, así como asegurar a los titulares el derecho a actualizar sus datos, hacer inclusiones o agregados, rectificar los mismos, hacer supresiones, cancelarlos, plantear oposiciones, revocarlos o denegarlos total o parcialmente, así como plantear los reclamos y solicitudes respecto de los mismos.

El receptor será responsable directo por la vulneración de los derechos de los titulares de los datos personales que le sean transferidos o entregados para encargo de tratamiento.

Concluido el presente contrato, toda transferencia de datos o encargo de tratamiento de datos se tendrá igualmente por concluida de manera definitiva. Para el caso del encargo de tratamiento, concluido el presente contrato, sea por la causa que fuera, el receptor de los datos deberá cumplir con devolver y restituir toda la información, documentación y datos personales que haya recibido, así como con eliminar y cancelar por completo todas las copias o respaldos que se hubiera podido crear, sin dejar rastro alguno de los mismos, estando prohibido de conservar cualquier tipo de documentación y/o información y/o datos, esté contenida en documentos escritos, de audio, video, magnético, informático, digital y/o en cualquier tipo de soporte, sea cual fuere su naturaleza, así como también, estando prohibido de recopilar, registrar, organizar, almacenar, modificar, extraer, consultar, utilizar, bloquear, difundir, compartir, transferir, divulgar, comunicar, copiar, reproducir, trasmitir, así como de realizar cualquier tratamiento respecto de los mismos, debiendo asumir las consecuencias legales por su incumplimiento. Debiendo, asimismo, recuperar, devolver, cancelar y/o eliminar de manera inmediata y definitiva, conforme a lo antes indicado, toda información de datos personales que hubiera podido compartir y/o encargar y/o transferir.

El receptor únicamente podrá utilizar la información y/o cualquier dato personal para cumplir con el objetivo de este contrato; nunca para otra finalidad. En tal sentido, el receptor queda expresamente prohibido de transferir los datos personales que haya recibido a terceros, a excepción de aquellos expresamente autorizados, y de aquellos que se puedan tratar sin consentimiento bajo las excepciones establecidas por ley. De esta manera, el receptor deberá contar con las medidas de seguridad y protección técnica, organizativa y legal para el tratamiento, seguridad, protección y confidencialidad de los datos personales e información que le son confiados. Toda información o datos personales que sean proporcionados al receptor sea cualquiera la modalidad o soporte, y sea cual fuera su naturaleza, tendrá el carácter de estrictamente confidencial, exclusiva y reservada.

1. OBJETIVO

Establecer el procedimiento para asegurar los controles de la seguridad en lo que respecta a sistemas (software y hardware).

2. ALCANCE

Se aplica a todos los sistemas informáticos de las empresas del Grupo Euromotors.

3. DEFINICIONES

3.1. Backup: Copia de respaldo o seguridad. Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.
3.2. Computadora: Dispositivo electrónico capaz de procesar información y ejecutar instrucciones de los programas. Una computadora es capaz de interpretar y ejecutar comandos programados para entrada, salida, cómputo y operaciones lógicas.
3.3. Firewall: Programa/Sistema que protege a una red de otra red.
3.4. Hardware: Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).
3.5. Internet: Red informática descentralizada de alcance global.
3.6. Malware: Es una forma abreviada del término inglés "malicious software" (software malicioso) y hace referencia a virus, spyware, gusanos, etc.
3.7. Password: Clave secreta de uso universal.
3.8. Ransomware: Lo que hace es secuestrar los datos de un ordenador y pedir un rescate económico a cambio de liberarlo.
3.9. SIS: Soporte Integral de Sistemas, es la mesa de ayuda que brinda soporte especializado de Sistemas a los usuarios finales.
3.10. Software: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.
3.11. Spyware: Es un tipo de programa que se instala con o sin su permiso en los ordenadores para recopilar información acerca de los usuarios, sus equipos o los hábitos de navegación, supervisar todas sus actividades sin su conocimiento y envíar estos datos a un usuario remoto.
3.12. Troyano: No es un virus, sino un programa destructivo que se hace pasar por una aplicación auténtica.los troyanos abren una puerta trasera en el equipo que facilita a usuarios y programas maliciosos el acceso al sistema para robar información personal y confidencial.
3.13. USB (Universal Serial Bus): Conector de dispositivos externos que hace de vía de ampliación de los nuevos ordenadores.
3.14. Virus: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

4. DOCUMENTOS A CONSULTAR

4.1. Procedimiento General “Certificación del Operador Económico Autorizado” – DESPA – PG.29 Versión 3 – Anexo 1, A.4.

5. RESPONSABILIDADES

5.1. Gerente General: Responsable de la aprobación del presente procedimiento.
5.2. Jefe de Administración de Sistemas: Responsable de la ejecución y seguimiento para la correcta aplicación del presente procedimiento.

6. DESARROLLO DEL PROCEDIMIENTO

Descripción	Responsable	Documento Asociado
6.1. Descripción 6.1.1. Inventario y Adquisiciones ▪ Con el propósito de identificar la infraestructura informática instalada en la empresa, el área de Sistemas en colaboración con la mesa de ayuda realiza inventario informático periódicamente. ▪ Si se trata de equipos a dar de alta o adquirir estos serán configurados y entregados con cargo a los usuarios respectivos, registrándose en el formato Acta de Conformidad, realizando la ficha técnica según el Formato de Inventario y la codificación del equipo que lo realizan pegando un sticker. 6.1.2. Asignación e Instalación ▪ Únicamente el área de sistemas está autorizada para realizar la instalación de cualquier tipo de software en los equipos propiedad de la empresa. ▪ Queda estrictamente prohibido a los usuarios instalar o hacer uso de cualquier software no autorizado. ▪ Sistemas controla qué software debe instalarse en los equipos de la empresa, una vulneración de este control amerita ser reportado al área de personal, para que se realicen la amonestación correspondiente.	Jefe de Administración de Sistemas SIS	Acta de Conformidad Formato de Inventario Procedimiento de Accesos al Sistema y Recursos Informáticos (PR-C-SIS-002)
6.2. Autorización de medios ▪ Los medios de cómputo que se definen son: Lector RW de CD/DVD y Puertos USB. ▪ El Jefe del área de Sistemas tiene automatizado el control de los medios mediante herramientas del directorio activo. ▪ Todos los usuarios por defecto no tienen acceso a estos medios, se otorgará un acceso temporal y luego regresará a su estado inactivo.	Jefe de Administración de Sistemas	Solicitud de Acceso de Dispositivos Informáticos

6.3. Acceso a la red de cómputo y aplicaciones ▪ Para que los trabajadores puedan acceder a la red, cuentan con un usuario y password creado por el Área de Sistemas. ▪ Mientras el usuario no se autentique con un usuario y password válido el equipo no permitirá la utilización del mismo. ▪ Las aplicaciones son accedidas también con un usuario y password, la cual es registrada y administrada por el aplicativo. ▪ El password es definido por el usuario. ▪ El password debe contener números y caracteres. ▪ El password tiene una duración de 3 meses como mínimo. Luego de este tiempo el sistema le pedirá que el password sea cambiado.	Jefe de Administración de Sistemas	Procedimiento de Accesos al Sistema y Recursos Informáticos (PR-C-SIS-002)
6.4. Programa de Antivirus ▪ Todas las computadoras cuentan con un programa antivirus instalado. ▪ Los equipos que resultan infectados con virus, son inmediatamente reinstalados para evitar mayores infecciones o pérdida de información.	Jefe de Administración de Sistemas SIS	n/a
6.5. Ejecución y control de Backups ▪ Es responsabilidad del usuario guardar (almacenar) la información que maneja en sus actividades diarias en el “Servidor de Archivos” que contiene carpetas individuales para que cada uno de los usuarios graben su información. ▪ ▪ El área de Sistemas realiza un backup diario centralizado al servidor de archivos. ▪ ▪ El área de Sistemas realiza pruebas de levantamiento de información de los backups realizados.	Jefe de Administración de Sistemas SIS	Política de Tecnologías de Información (PO-C-SIS-001)
6.6. Soporte técnico ▪ El Área de Soporte Integral de Sistemas (SIS) es el encargado de realizar el soporte técnico a los usuarios de la empresa. ▪ El Usuario llama vía teléfono al SIS y explica su requerimiento. ▪ El SIS registra la ocurrencia en su sistemas de gestión de Help Desk.	Jefe de Administración de Sistemas SIS	Política de Tecnologías de Información (PO-C-SIS-001)

6.7. Control de correos electrónicos ▪ Las cuentas de correo son solicitadas por la gerencia o Jefatura de cada área mediante el formato de creación de usuarios. ▪ El SIS tiene hasta 48 horas para crear la cuenta de correos, luego de la conformidad del área de personal. ▪ El SIS informará al usuario final las credenciales de uso de su nueva cuenta de correo.	Jefe de Administración de Sistemas SIS	n/a
6.8. Control de acceso al sistema SIMA ▪ SIMA: Programa que la organización utiliza para gestionar la información de sus operaciones logísticas. ▪ Las cuentas de acceso son solicitadas por la gerencia de cada área mediante la plataforma ERH Empresarial de GDH. ▪ El acceso es indicado por perfiles de usuarios.	Jefe de Administración de Sistemas SIS	Política de Tecnologías de Información (PO-C-SIS-001)
6.9. Acceso y uso de Internet ▪ Todos los usuarios autenticados de la red cuentan con el acceso a Internet, el cual es asignado de acuerdo al perfil que le corresponda de acuerdo a sus funciones en la empresa.	Jefe de Administración de Sistemas SIS	Política de Tecnologías de Información (PO-C-SIS-001)
6.10. Licencias de software ▪ Es responsabilidad del área de Sistema el control de las licencias de software, la documentación que acredite a la empresa como usuario legal del software, así como asegurarse de contar con el número de licencias requeridas. Además de evitar y prohibir el uso de programas sin licencia por parte del propietario mismo. ▪ ▪ Tanto los medios de distribución del software original quedarán bajo custodia del área de Sistemas.	Jefe de Administración de Sistemas	Política de Tecnologías de Información (PO-C-SIS-001)

6.11. ¿Cómo actuar ante un evento de explotación de una vulnerabilidad? 6.11.1. Seguridad de datos: El área de Sistemas es la única autorizada para proveer y cambiar las claves según sea necesario. 6.11.2. Daño físico o robo: En caso de daño físico o pérdida por robo, el responsable del equipo debe reportarlo inmediatamente a su Jefe inmediato y al SIS para seguir con los procedimientos correspondientes. 6.11.3. Para prevenir la infección de virus: No utilizar software ilegal ni visitar páginas web de dudosa reputación en los equipos. Verificar los archivos con el software antivirus instalado para tal fin, recordando que éstos pueden ser más nuevos que el antivirus y pasar desapercibidos. 6.11.5. Responsabilidades: ▪ Es responsabilidad del usuario guardar la información que maneja en sus actividades diarias en el espacio particular otorgado en el servidor de archivos. ▪ No es responsabilidad del área de Sistemas el contar con respaldos de información personal de los usuarios.	Jefe de Administración de Sistemas	Plan de Contingencia Informático (PL-C-SIS-001)
6.12. Retiro o cese de un trabajador o usuario ▪ El cese del personal es informado por el área de Personal al SIS. ▪ Cuando un trabajador o usuario se separa de la empresa, el área de Sistemas realiza unos días después lo siguiente: ○ Realiza el backup de su correo electrónico. ○ Elimina sus accesos a la red. ○ Elimina sus accesos a los aplicativos. ▪ La retención de la información es por un año.	Jefe de Administración de Sistemas	n/a

6.13. Incidencias ▪ Toda incidencia que detecte el área de Sistemas que lo haya cometido el usuario o trabajador lo reporta mediante email a su jefatura inmediata y al área de personal para que tomen las medidas correctivas como sanciones mediante memorándum de llamada de atención hasta con suspensión de labores. ▪ Las incidencias que se pueden encontrar que comete el usuario son: o Robo, extracción o exposición de información fuera de los sistemas de Euromotors. o Abuso de un perfil de usuario asignado que no le corresponde. o El usuario infractor es el dueño de la cuenta que compartió su contraseña. o Alterar o borrar información. o Vandalismo premeditado sobre los equipos, software y programas o módulos operativos de la empresa. o Abuso del servicio de Internet, software o páginas pornográficas. o No reportar que tiene dificultades con su equipo de cómputo. o Intrusión de los equipos de cómputo, como una la PC/laptop, para incorporar un medio de cómputo o para sustraerlo o cambiar. o Revelar o difundir los datos contenidos en un sistema de información. o El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento. o Falsificación de documentos vía computarizada. o Intrusión o incorporación de instrucciones que provocan interrupciones en la lógica interna de los programas.	Jefe de Administración de Sistemas	Plan de Contingencia Informático (PL-C-SIS-001)
6.14. Capacitaciones ▪ Según requerimiento y disponibilidad el área de sistemas realiza inducción al usuario sobre el manejo de los controles de seguridad que tiene el área de sistemas para proteger la información como también del manejo de algún programa o módulo.	Jefe de Administración de Sistemas	Procedimiento de Accesos al Sistema y Recursos Informáticos (PR-C-SIS-002)

6.15. Cumplimiento de los controles de seguridad en sistemas ▪ La Jefatura de Sistemas realiza mensualmente una revisión aleatoriamente de los controles que realiza su personal de acuerdo al formato Checklist de Seguridad en Sistemas.	Jefe de Administración de Sistemas	Checklist de Seguridad en Sistemas (F-C-SIS-007)
6.16. Protección para el Teletrabajo Sobre las medidas de protección adoptadas por el área de Sistemas: ▪ Para todos los dispositivos que se encuentren fuera de las instalaciones de la organización y accedan de manera remota a los sistemas que esta posee, deberán contar con mecanismos de seguridad para salvaguardar los activos. Estos mecanismos son: o Políticas de aseguramiento (GPO) por intermedio del Microsoft Active Directory. o Sistemas de Protección: - Antivirus / Malware - Data Loss Prevention - Web Control - Firewall de protección o Software de conexión VPN. o Actualizaciones de seguridad del Sistema Operativo. ▪ Los usuarios hacen uso del acceso remoto vía el software de VPN, este es del tipo restringido o de accesos puntuales y de acuerdo con los servicios que el usuario necesite para realizar su trabajo. Para ello se crearán plantillas por función para asignar según sea el caso. ▪ Los usuarios deben de respaldar su información periódica o permanentemente en la unidad compartida “U:”. ▪ No se admite el uso de un dispositivo BYOD en la organización.	Jefe de Administración de Sistemas	

7. REGISTROS Y ANEXOS

Nombre	Acceso	Almacenamiento	Tipo de Almacenamiento	Retención	Disposición	Área de Proceso	Responsable del Documento
Acta de Conformidad	Físico en cada área	Archivo del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Formato de Inventario	Físico en cada área	Archivo del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Procedimiento de Accesos al Sistema y Recursos Informáticos (PR-C-SIS-002)	Digital	Carpeta del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Solicitud de Acceso de Dispositivos Informáticos	Físico en cada área	Archivo del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Política de Tecnologías de Información (PO-C-SIS-001)	Digital	Carpeta del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Plan de Contingencia Informático (PL-C-SIS-001)	Digital	Carpeta del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas
Checklist de Seguridad en Sistemas (F-C-SIS-007)	Físico en cada área	Archivo del área de Sistemas	Electrónico	1 año	Eliminar	Sistemas	Jefe de Administración de Sistemas

8. CONTROL DE CAMBIOS

N° de Revisión	Sección y/o Página	Fecha de Modificación	Motivo	Autorizado por:
00	Todo el documento	21/03/2012	Creación del documento.	Jefe de Administración de Sistemas
01	Todo el documento	16/05/2022	Actualización del procedimiento.	Jefe de Administración de Sistemas

ELABORADOR	REVISOR	APROBADOR
Marco Miranda Jefe de Administración de Sistemas	Yliana Molina Coordinadora de Procesos de Calidad	Fernando Melly Gerente de Sistemas

ANEXO 1

EMPRESAS QUE CONFORMAN EL GRUPO EUROMOTORS

1.- EURO MOTORS S.A. – R.U.C. N° 20168544252 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 00233196 del Registro de Personas Jurídicas de Lima.

2.- ALTOS ANDES S.A.C. – R.U.C. N° 20296136728 – Av. Tomás Marsano 402-Surquillo-Lima – Partida N° 03007041 del Registro de Personas Jurídicas de Lima.

3.- RENTING S.A.C. – R.U.C. N° 20509031500 – Jr. Domingo Martínez Lujan 1202 - Surquillo-Lima – Partida N° 11667075 del Registro de Personas Jurídicas de Lima.

4.- EUROSHOP S.A., R.U.C. N° 20349065488 – Av. Domingo Orué 989-Surquillo-Lima – Partida N° 03020437 del Registro de Personas Jurídicas de Lima.

5.- SAN BARTOLOME S.A., R.U.C. N° 20125327509 – Av. 1ero. de Mayo 559-Urb. El Puente-El Agustino-Lima – Partida N° 00364037 del Registro de Personas Jurídicas de Lima.

6.- EURO CAMIONES S.A., R.U.C. N° 20550808791 – Av. Los Cipreses 420-Urb. Los Ficus-Santa Anita-Lima – Partida N° 12947841 del Registro de Personas Jurídicas de Lima.

7.- EUROLIFT S.A., R.U.C. N° 20536982559 – Av. República de Argentina 2165-Lima-Lima – Partida N° 12540250 del Registro de Personas Jurídicas de Lima.

8.- EUROINMUEBLES S.A.C., R.U.C. N° 20549632204 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 12907303 del Registro de Personas Jurídicas de Lima.

9.- 1 ONE S.A.C., R.U.C. N° 20520549740 – Av. Tomás Marsano 432-Surquillo-Lima – Partida N° 12225562 del Registro de Personas Jurídicas de Lima.

10.- EUROCONNECT S.A.C., R.U.C. N° 20605166793 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 14348700 del Registro de Personas Jurídicas de Lima.

11.- INTERNATIONAL CAMIONES DEL PERU S.A., R.U.C. N° 20600045521 – Av. Domingo Orué 973-Surquillo-Lima – Partida N° 13209869 del Registro de Personas Jurídicas de Lima.

12.- REVO MOTORS S.A., R.U.C. N° 20600137272 – Av. Tomás Marsano 402-Surquillo-Lima – Partida N° 13366991 del Registro de Personas Jurídicas de Lima.

13.- T1 S.A.C., con R.U.C. N° 20612019470 – Jr. Catalino Miranda 278 – Barranco – Lima – Partida N° 15509068 del Registro de Personas Jurídicas de Lima.