Riesgos legales y definición de la política de la empresa

# Indice

[Indice 1](#_Toc292570722)

[Ley Habeas Data (25.326) 2](#_Toc292570723)

[Seguridad 2](#_Toc292570724)

[Confidencialidad 2](#_Toc292570725)

[Derechos de las personas 2](#_Toc292570726)

[Registro de bases de datos y archivos 3](#_Toc292570727)

[Requisitos de la Base de Datos 4](#_Toc292570728)

[Sanciones 5](#_Toc292570729)

[Infracciones 5](#_Toc292570730)

[Infracciones leves 6](#_Toc292570731)

[Infracciones graves 6](#_Toc292570732)

[Infracciones muy graves 7](#_Toc292570733)

[Jurisprudencia 7](#_Toc292570734)

[Aplicaciones a [Scoring Vehicular Estadístico / GPICA] 9](#_Toc292570735)

[Privacidad, pertinencia y calidad de los Datos 9](#_Toc292570736)

[Buen Uso de la Información 9](#_Toc292570737)

[Confidencialidad, Actualización y Seguridad de los Datos 9](#_Toc292570738)

[Derecho de Acceso, pedido de modificación y supresión de datos 10](#_Toc292570739)

# Ley Habeas Data (25.326)

## Seguridad

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

## Confidencialidad

El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

## Derechos de las personas

* **ACCESO:** Derecho a obtener información acerca de la siguientes circunstancias: existencia de datos referidos a su persona en todo archivo, registro, banco o base de datos que contenga información personal; fuentes y medios a través de los cuales se obtuvieron sus datos; finalidad para la cual fueron recabados sus datos; y destino previsto para sus datos.
* **RECTIFICACION:** Derecho  a exigir que los datos personales incluidos en un archivo, registro, banco o base de datos que sean inexactos o incompletos, sean rectificados o actualizados.
* **SUPRESION:** Derecho a exigir que se eliminen los datos personales que, por diversas circunstancias, no deban figurar en un archivo, registro, banco o base de datos, o que se supriman o sometan a confidencialidad los datos personales que sean inexactos o incompletos.
* **TUTELA:** Derecho a iniciar acciones judiciales tendientes a tomar conocimiento de los datos personales almacenados en archivos, registros, bancos o bases de datos públicos o privados destinados a proporcionar informes y, cuando corresponda, a exigir su rectificación, supresión, confidencialidad o actualización, así como a reclamar los daños y perjuicios que pudiera haber sufrido como consecuencia de la inobservancia de la ley.
* **IMPUGNACION:** Derecho a impugnar todo acto administrativo o decisión privada que implique una apreciación o valoración del comportamiento de un ciudadano fundado únicamente en el tratamiento de datos de carácter personal que permita obtener un determinado perfil de su personalidad.
* **CONSULTA:** Derecho a solicitar a la Dirección Nacional de Protección de Datos Personales o al Centro de Protección de Datos Personales de la Ciudad de Buenos Aires, información relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data.

El derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

## Registro de bases de datos y archivos

Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

El registro de archivos de datos debe comprender como mínimo la siguiente información:

* Nombre y domicilio del responsable;
* Características y finalidad del archivo;
* Naturaleza de los datos personales contenidos en cada archivo;
* Forma de recolección y actualización de datos;
* Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
* Modo de interrelacionar la información registrada;
* Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
* Tiempo de conservación de los datos;
* Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

La inscripción se realiza a través del web site de la Dirección Nacional de Protección de Datos Personales. El costo del trámite depende del tipo de bases de datos que se registren y de la cantidad de datos personales tratados. El valor del arancel más alto es de $ 3.000.- y es gratuito para aquellas bases de datos que contengan información referida a menos de 5.000 personas.

Los archivos, registros, bases o bancos de datos que se creen con posterioridad a la fecha de apertura del Registro Nacional de Bases de Datos Privadas deberán inscribirse antes de su creación.

La inscripción en el Registro Nacional de Bases de Datos Privadas es obligatoria y debe renovarse anualmente. La legislación vigente establece sanciones de $ 1.000.- a $ 50.000.- para quienes incumplan el deber registral.



Isogotipo de responsables registrados

### Requisitos de la Base de Datos

Los requisitos generales que deben cumplir los titulares de archivos, registros, bancos o bases de datos que contengan información relativa a personas para garantizar la veracidad de la información contenida, la congruencia y la racionalidad de la utilización de los mismos, pueden resumirse enumerando los siguientes principios rectores:

* Pertinencia: Los datos que se recaben y almacenen deben ser pertinentes y adecuados, es decir, estar relacionados con el fin perseguido en el momento de creación de la base de datos.  En ningún caso se puedan utilizar los datos obtenidos para finalidades distintas de aquéllas para las que se hubieran recogido.
* Finalidad:Los datos deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma e informarse en el momento en el que la información personal es recolectada. Los datos que se obtengan deben tratarse de manera leal y lícita, y su almacenamiento debe perseguir fines concretos y legítimos.
* Utilización no abusiva: Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.
* Exactitud: Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Si fueren inexactos o incompletos, deben ser suprimidos y sustituidos, o en su caso completados.
* Limitación en el tiempo: Los datos deben ser eliminados una vez que se haya cumplido la finalidad para la que fueron recabados.
* Legalidad: El procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal, no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.
* Publicidad: Los archivos, registro, base o banco de datos alcanzados por las disposiciones legales deben inscribirse en el Registro que al efecto habilite la Dirección Nacional de Protección de Datos Personales para permitir que, a través de su consulta, los ciudadanos pueden tomar conocimiento de los archivos en los cuales pueden existir datos referidos a su persona y de la identidad de los responsables de su tratamiento, para poder ejercer una defensa adecuada de sus derechos.
* Seguridad: La información personal referida a los ciudadanos debe almacenarse en archivos, registros, bancos o bases de datos que reúnan condiciones técnicas de integridad y seguridad.
* Consentimiento: Como regla general, el tratamiento de datos de carácter personal requiere el consentimiento libre, expreso e informado del titular de los datos. Ello, para permitir que cada persona pueda elegir qué datos referidos a su persona pueden ser sujetos a tratamiento. En principio, el consentimiento debe constar por escrito o por medio equiparable que deberá ser establecido por la DNPDP. El requisito del consentimiento previo cuenta con las siguientes excepciones:
  + Cuando los datos se obtienen de fuentes de acceso público irrestricto;
  + Cuando lo datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
  + Cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
  + Cuando deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
  + Cuando se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la ley 21.526.

## Sanciones

El organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

En caso de demanda y habiendo sido producida la prueba, el juez dictará sentencia. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

Para quien inserte o hiciere insertar, a sabiendas, datos falsos en un archivo, registro, banco o base de datos personales, se establece una pena de prisión de 1 mes a 2 años. Para quien proporcione a un tercero, a sabiendas, información falsa contenida en un archivo, registro, banco o base de datos personales, se establece una pena de prisión de entre 6 meses a 3 años. Si de alguno de estos delitos se derivara un perjuicio a alguna persona, la escala podrá aumentarse en la mitad del mínimo y del máximo, y si el autor o responsable del ilíctio es un funcionario público en ejercicio de sus funciones, podrá aplicársele la accesoria de inhabilitación para el desempeño de cargos públicos por el doble de tiempo de la condena.

Para quien, a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un archivo, registro, banco o base de datos personales, se establece un pena de 1 mes a 2 años de prisión. La misma pena se establece para quien revelare a otro información registrada en un archivo, registro, banco o base de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley, y si se trata de un funcionario público, podrá aplicársele, además, pena de inhabilitación especial de 1 a 4 años.

## Infracciones

Las infracciones se clasifican en las siguientes categorías: "Leves", "Graves" y "Muy Graves".

Se aplican las siguientes multas de acuerdo a la categoría:

* Infracciones leves: De Pesos Un Mil ($ 1.000.-) a Pesos Tres Mil ($ 3.000.-).
* Infracciones graves: De Pesos Tres Mil ($ 3.000.-) a Pesos Cincuenta Mil ($ 50.000.-).
* Infracciones muy graves: De Pesos Cincuenta Mil ($ 50.000.-) a Pesos Cien Mil ($ 100.000.-).

### Infracciones leves

* No atender, por motivos formales, la solicitud del interesado de acceso, rectificación, confidencialidad o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
* No proporcionar la información que solicite la Dirección Nacional de Protección de Datos Personales en el ejercicio de las competencias que tiene atribuidas, en relación con aspectos no sustantivos de la protección de datos.
* No solicitar la inscripción de una base de datos personales pública o privada que exceda el uso personal.
* Recoger datos de carácter personal de los propios titulares sin proporcionarles la información que señala el artículo 6° de Ley N° 25.326. e) Incumplir el deber de secreto establecido en el artículo 10 de la Ley N° 25.326, salvo que constituya infracción grave.

### Infracciones graves

* Proceder a la creación de bases de datos de titularidad pública o recoger datos de carácter personal para las mismas, sin autorización de disposición general, publicada en el "Boletín Oficial" o diario oficial correspondiente y cumpliendo los requisitos del artículo 22 de la Ley N° 25.326.
* Proceder al tratamiento de datos de carácter personal que no reúnan las calidades de ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
* Recoger datos de carácter personal sin recabar el consentimiento libre, expreso e informado de su titular, en los casos en que éste sea exigible.
* Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en Ley N° 25.326 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
* El impedimento o la obstaculización del ejercicio de los derechos de acceso y la negativa a facilitar la información que sea solicitada.
* Mantener datos de carácter personal inexactos o no efectuar las rectificaciones, actualizaciones o supresiones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la Ley N° 25.326 ampara.
* La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a bases de datos que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros bases de datos que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
* Mantener las bases de datos, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
* No proporcionar en plazo a la Dirección Nacional de Protección de Datos Personales cuantos documentos e informaciones sean requeridos, conforme las previsiones de la Ley 25.326 o sus disposiciones reglamentarias.
* La obstrucción al ejercicio de la función de inspección y fiscalización a cargo de la Dirección Nacional de Protección de Datos Personales.
* No inscribir la base de datos de carácter personal en el Registro Nacional de Protección de Datos Personales, cuando haya sido requerido para ello por la Dirección Nacional de Protección de Datos Personales.
* Incumplir el deber de información que se establece en los artículos 6 y 26 de la Ley N° 25.326, cuando los datos hayan sido recabados de persona distinta del afectado.

### Infracciones muy graves

* Recoger datos de carácter personal en forma engañosa y fraudulenta.
* La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
* Recolectar y tratar los datos sensibles vulnerando los principios y garantías de la Ley N° 25.326.
* No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por la Dirección Nacional de Protección de Datos Personales o por las personas titulares del derecho de acceso.
* Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
* La vulneración del deber de guardar secreto sobre los datos sensibles, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
* No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, actualización, supresión o bloqueo.
* No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en una base de datos, de conformidad con los artículos 5° y 6° de la Ley N° 25.326.

# Jurisprudencia

En esta sección se mencionan sentencias favorables y no favorables a las empresas de suministro de datos relacionadas con la protección de información.

* Si bien es cierto que el responsable del tratamiento de datos -esto es, la persona física o de existencia ideal que es titular de un archivo o registro, base o banco de datos- tiene una obligación personal o directa de preservar la calidad de los que almacena y por tal razón debe realizar las diligencias apropiadas y exigibles -v. gr. verificar la exactitud y actualidad de la información-, carece de facultades para modificar, revisar o alterar la información que le fue suministrada por fuentes oficiales o por un tercero. Menos aún las tiene para dirimir las controversias que deben ventilarse y dirimirse en el Poder Judicial ante los tribunales competentes y por la vía pertinente (CNCiv.,  Sala G, "Montini, Roberto R.L. c/ Diners Club Argentina SACT. s/ Hábeas Data", 14/05/03).
* Corresponde confirmar la sentencia apelada por la cual se condenó a la empresa Veraz S.A. por suministrar información no fidedigna pues a pesar de lo argumentado por la demandada respecto a que la información incluida por la misma en su base de datos proviene de fuentes judiciales, públicas y bancarias, debidamente chequeadas y verificadas, el informe respecto de la situación crediticia de la actora fue confeccionado con liviandad, sin el necesario y reconocido chequeo y/o verificación que efectuaban diariamente a fin de extremar los medios de seguridad en el flujo de la información. (en el sub lite, la actora había cancelado su deuda en octubre de 1998, sin embargo en el mes de abil de 1999 continuaba situada en el nivel 4 -alto grado de insolvencia- dentro del informe producido por la Organización Veraz S.A.). ("P., S. c/ Organización Veraz y otros". CNCiv., Sala A, agosto 07/2001. ED, 194-346).
* Corresponde admitir la indemnización por daño moral solicitada por los gerentes de una empresa contra la entidad bancaria con la que ésta operaba, por cierre de una cuenta corriente que provocó que el Banco Central dispusiera la inclusión de sus datos -tanto de la empresa como de los gerentes- en un boletín periódico de personas inhabilitadas para operar como cuentacorrentistas dirigido a bancos. ("Coccia, Carlos Antonio c/ Veritas DGC Land Inc. Sucursal y otro s/ Daños y Perjuicios" - CNCiv., Sala C - 26-09-00. Revista El Derecho, 16/03/2001).
* Un dato falso o inexacto registrado en el Banco de Datos "Organización Veraz S.A." con respecto al actor y como consecuencia de una errónea información suministrada por el B.C.R.A. por el Banco codemandado pudo y debió causar al actor una profunda lesión en su persona porque toca a su prestigio profesional y a su innegable derecho a requerir la protección de su intimidad (arts. 19, Constitución Nacional y 1.071 bis, Código Cvil en su redacción posterior a la ley 17.711) ("Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro". CNCiv., Sala K, 22/10/02).
* La existencia y publicidad de datos desactualizados y erróneos relacionados con el actor deben haber repercutido en su espíritu, sentimientos o afecciones más íntimas, ya que implicaron un ataque a su honor, a su imagen y reputación; máxime si se tiene en cuenta la extensa labor profesional y académica del actor. Tales circunstancias, justifican sin hesitación la procedencia del daño moral. ("Ravina, Arturo Octavio c/ Organización Veraz S.A.". CNCiv., Sala F, 06/02/02 - ED, 197-265).
* El Banco que por error comunicó al Banco Central la inhabilitación de una persona creyéndola cliente de la institución, se halla incurso en responsabilidad aquiliana, ya que no la une ninguna relación contractual con la damnificada y, en consecuencia, deberá reparar el daño causado por el ilícito (art. 1067 Cód. Civil). Esto es, haber quedado sindicado en el Banco Central y en las empresas que brindan informes como “deudor irrecuperable”. Debe responder el responsable por el agravio moral causado en razón del descrédito en la solvencia moral y económica que a raíz de ello se sufrió (CNCom., Sala B, 12/03. "Pereyra, Héctor Alberto c/ Citibank NA s/ Sumario").
* A criterio de la preopinante, el daño se configuró. Su prueba es que el actor fue incluido injustamente en los registros de "Organización Veraz" por una comunicación falsa del demandado. Es de público y notorio, los efectos nocivos que produce para los afectados la aparición en tales registros. En el plano del "daño moral" tal situación configura una lesión per se; es innecesario probar más daño que el haber estado erróneamente incluido en estos registros durante mas de tres años injustamente. Estamos ante una prueba in re ipsa. ("Derderian, Carlos c/ Citibank N.A. s/ sumario". CNCom. Sala B, 12/09/02. Causa 30247/00).
* La entidad financiera que identificó ante el B.C.R.A. a una persona como deudora, persona que ni siquiera es su cliente, queda incurso en responsabilidad aquiliana, y en consecuencia deberá reparar el daño específicamente contemplado en el art. 1078 C.C. El Banco causó un descrédito en la solvencia moral y económica del actor injusta e injustificable, ello tiene una innegable proyección en el plano individual. El daño a que me refiero no queda reducido al clásico “Pretium doloris” sino que además involucra toda lesión a intereses jurídicos del espíritu, alteraciones desfavorables para la víctima. Toda persona tiene el derecho perfecto de ser protegido en su reputación, honor, estima de que goza en un determinado ámbito social, etc., no pudiendo ser privado sin causa legítima de esos derechos; por tanto si el actor sufrió una violación en su ejercicio, indudablemente por el art. 1078 corresponde sea indemnizado. Adicionalmente, el daño moral no se mide sólo ni fundamentalmente por las repercusiones que contiene, sino por el menosprecio que la dañosa en si misma denotó a la persona y se estima en razón del bien no patrimonial lesionado. (CNCom., Sala B, causa 44.356/01. "Lupi, Luis Fernando y otro c/ Lloyds Bank S.A. s/ Ordinario").
* El Banco que suministró erróneamente información sobre un cuentacorrentista, lo que motivó su inhabilitación por el Banco Central, debe responder aunque el perjuicio provenga de la inclusión de la información equivocada en otras bases de datos o servicios de información crediticia, puesto que es el autor de la errónea información original ("Gualtieri Orlando A. c/ Citibank NA" - C.N.Civ., 10/04/2001- JA, 2001-IV-504).
* La errónea inclusión del actor en el registro de deudores a partir del equívoco producido por una situación de homonimia en la persona contra quien se debía dirigir la ejecución, demuestra que la entidad demandada no empleó el debido cuidado, atención y diligencia para prevenir su producción, ni en hacerlo cesar en cuanto fue advertida del error. Tales circunstancias constituyen la "torpeza calificada" a la luz del Art. 902 del Código Civil y justifica por si sola la condena impuesta. La ilicitud objetiva surge de la confrontación de la conducta obrada con la Ley en sentido material (o lato o amplio) mediante la confrontación total del ordenamiento jurídico (Art. 1066, 1071, 1113 y concordantes del Código Civil). (Serafino, Gustavo Adrián c/ Banco de la Provincia de Buenos Aires s/ Ordinario. CNCom., Sala A, 06/02/04).
* No vulnera principios de intimidad el informe dado por una organización que proporcioa información a las entidades que lo requieran sobre posibles clientes, en tanto éstos se limitan a datos personales y juicios pendientes, no siendo ellos datos secretos ni confidenciales. ("Depaolini, Angela M. c/ Organización Veraz". CCivil y Com. San Isidro, Sala I, 21/6/96. LL Buenos Aires, 1996-1082 begin\_of\_the\_skype\_highlighting            1996-1082      end\_of\_the\_skype\_highlighting).
* Es deber de la empresa que lucra con la emisión de informes de los que surge la eventual solvencia comercial de las personas, el instrumentar las medidas necesarias para que la información suministrada se ajuste a la realidad o soportar sus consecuencias, sin que sean los propios sujetos pasivos de la información los que deban aportar los datos pertinentes. (CNCiv, Sala K, Sentencia Interlocutoria K070307. "Lucato, Omar Norman c/ Organización Veraz. S.A. s/ Hábeas Data").
* La acción de hábeas data es improcedente si no se demuestra el motivo descalificante del dato en cuestión, ni que su origen sea la anotación en registros o bases de datos propios o de terceros, ya sean públicos o privados, destinados a suministrar información (CFed. Bahía Blanca, Sala I, 18/1/95, "Gutierrez, Héctor c/ Casino Militar del Personal Superior de la Base Naval de Puerto Belgrano", LL. 2/2/96).
* No corresponde hacer lugar a la demanda tendiente a que el banco de datos demandado elimine de sus registros ciertos datos relativos a la situación financiera de la actora, pues esta no ha probado el error, falsedad, inexactitud o desactualización de tal información, ni tampoco que se hubiera exorbitado el ámbito propio en que la misma pueda ser proporcionada. (CNCom., Sala C, "F., L. c/ Organización Veraz S.A. s/ amparo", 11/10/2002).

# Aplicaciones a [Scoring Vehicular Estadístico / GPICA]

## Privacidad, pertinencia y calidad de los Datos

En cumplimiento con lo dispuesto por la Ley 25.326 en ningún caso se accede a datos sensibles de las personas, como ser el honor, culto, raza, color de piel, ideología política y filosófica, cuyo tratamiento puede ser fundamento de actos de discriminación.

Solo se colecta información disponible en tanto resulte pertinente, útil o necesaria para facilitar la toma de decisiones a empresas aseguradoras y prescinde de toda otra información que excede a las previsiones del marco regulatorio establecido por la Ley 25.326 (Habeas Data). Estos procesos se desarrollan respetando estrictos controles de validación en donde se descartan aquellos datos en los que se advierten incongruencias.

## Buen Uso de la Información

Se exige a los clientes que cada informe solicitado sea destinado exclusivamente para la evaluación de conductores. Los clientes quedan obligados contractualmente con dicho principio y son responsables por su mal uso.

## Confidencialidad, Actualización y Seguridad de los Datos

La empresa guarda estricta confidencialidad de los datos frente a terceros, accediendo a los mismos tan sólo quienes estén debidamente identificados. Continuamente se implementan medidas técnicas y organizativas para proteger la autenticidad y confidencialidad de los datos almacenados, a fin de evitar la alteración y sustracción por parte de terceros ajenos[[1]](#endnote-2).

Se implementan procedimientos que permiten actualización, rectificación y supresión de datos en conformidad con la Ley 25.326 (Habeas Data). Los actualizaciones de los datos colectados por la empresa se encuentran adecuadamente respaldadas, pudiendose consultar las fuentes oficiales que lo originan.

Con respecto al manejo de datos entregados por medio del sitio web:

* Se asegurará que solo usuarios identificados y debidamente autorizados puedan solicitar o tener acceso a los datos;
* Se adoptarán las medidas que sean necesarias para impedir la solicitud o acceso a los datos por cualquier persona que este autorizada. Se utilizan para ello códigos de seguridad y autenticación de usuarios.
* Solo se utilizarán para el almacenamiento de datos dispositivos que sean de propiedad de la sociedad, tales como discos, CD y DVD).
* La información deberá ser codificada (usando como normas mínimas AES, Triple DES, MD5) cuando no esté siendo utilizada y la la información impresa deberá destruirse por completo una vez que ya no se necesite, por medio de máquinas trituradoras de manera que los resultados no sean legibles ni utilizables para ningún objeto;
* El almacenamiento de datos en el servidor es asegurado a través firewalls, múltiples capas de seguridad de red y dispositivos para detección/prevención de intrusos (IDS/IPS).

## Derecho de Acceso, pedido de modificación y supresión de datos

Se facilita a cada persona debidamente identificada el acceso gratuito a la totalidad de los datos existentes en la base de datos, a través de [ sección del sitio web que va a servir para esto]. Quedan reconocidos, respecto a los datos informados por la empresa, los derechos de acceso, cancelación y rectificación de datos, los cuales podrá ejercitar plenamente, contactandose con la misma.

La solicitud o correción de datos puede hacerse a través de los siguientes medios:

1. Personalmente en el domicilio de [Nuevos Rumbos] sito en Av. XXXXXXX #### de la Ciudad Autónoma de Buenos Aires, de lunes a viernes en el horario de Y Hs. a Z Hs., previa acreditación de identidad.
2. Sitio web: [http://www.nuevosrumbos.com/formulario\_datos.jsp]

1. Ver documento Seguridad y Actualizacion.docx [↑](#endnote-ref-2)