URIBE · YÁÑEZ

Asesores Legales

DATOS PERSONALES

URIBE · YÁÑEZ


The Data Dollar Store - A Data Shopping Social Experi...
Copy link
"¿Qué me darías por un grabado
Watch on YouTube

Tap Here

URIBE · YÁÑEZ

DEFINICIONES GENERALES

1 — ¿Qué es un Dato Personal?

DEFINICIONES GENERALES

1

Régimen general

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

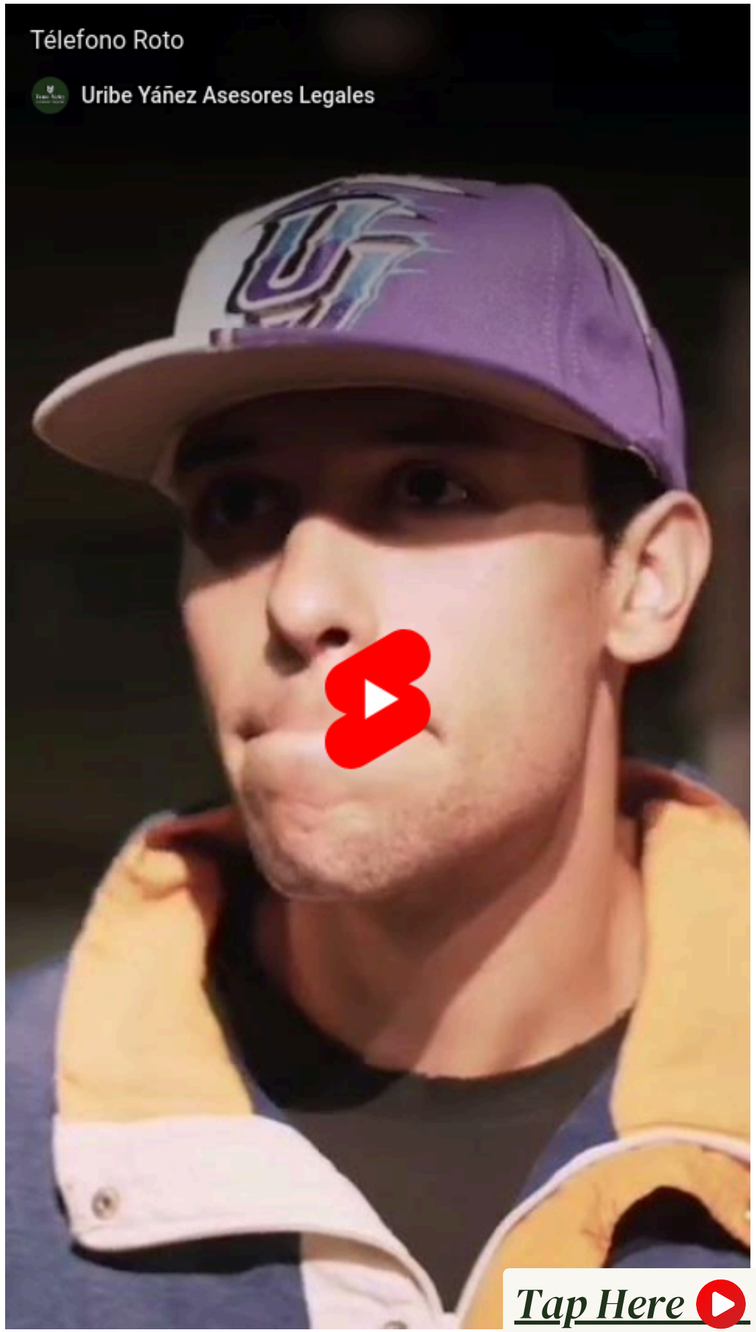
URIBE · YÁÑEZ

DEFINICIONES GENERALES

1

Habeas data financiero

Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica.


Télefono Roto
Uribe Yáñez Asesores Legales
Tap Here

URIBE · YÁÑEZ

DEFINICIONES GENERALES

2

¿Qué se entiende por Responsable del Tratamiento?

URIBE · YÁÑEZ

DEFINICIONES GENERALES

2

¿Qué se entiende por Responsable del Tratamiento?

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

DEFINICIONES GENERALES

3

¿Qué se entiende por Encargado del Tratamiento?

URIBE · YÁÑEZ

DEFINICIONES GENERALES

3

¿Qué se entiende por Encargado del Tratamiento?

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

DEFINICIONES GENERALES

3

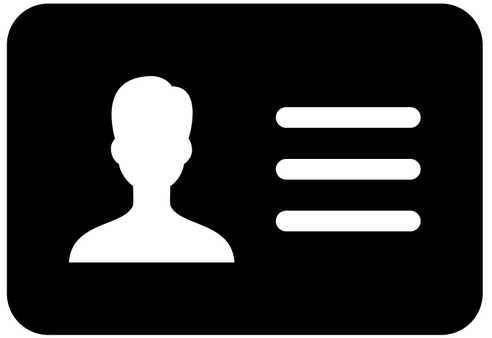
¿Qué se entiende por Encargado del Tratamiento?

Tercero, proveedor o contratista que tiene un encargo a favor del Responsable.

DEFINICIONES GENERALES

4

¿Quién es el Titular del dato personal?

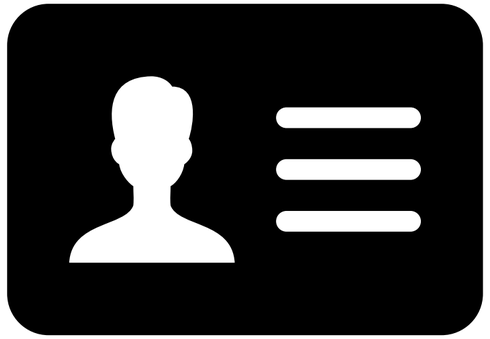


DEFINICIONES GENERALES

4

Régimen general

Persona natural cuyos datos personales sean objeto de Tratamiento.

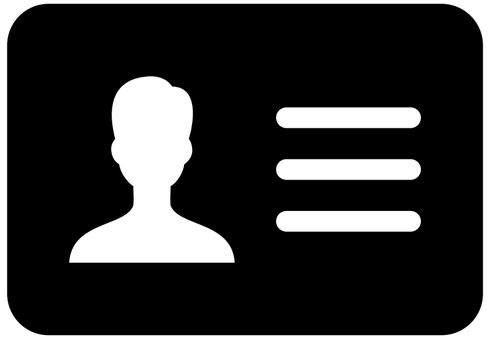


DEFINICIONES GENERALES

4

Habeas data financiero

Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos.



URIBE · YÁÑEZ

DEFINICIONES GENERALES

5

¿Qué significa el Tratamiento de Datos Personales? ¿Qué acciones comprende el Tratamiento?

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

URIBE · YÁÑEZ

DEFINICIONES GENERALES

6

¿Qué es una Base de datos?

Conjunto organizado de datos personales que sea objeto de Tratamiento.

URIBE · YÁÑEZ

DEFINICIONES GENERALES

7

¿Qué cantidad de datos debe manejar una persona para ser considerado Responsable del tratamiento?

A partir del Tratamiento de uno (1) o más Datos Personales. La importancia radica en la realización de operaciones sobre la información personal (tratamiento) y no en la cantidad de datos que trate el Responsable.

DEFINICIONES GENERALES

8

¿El Encargado debe ser autorizado por el Titular del Datos para tratar su información personal?

Al momento de solicitar autorización del Titular, el Responsable deberá mostrar su Política de privacidad donde debe constar toda la información y quién será encargado de esta.

DEFINICIONES GENERALES

9

¿Cuál es la normativa de Habeas Data en Colombia?

Art. 15 de la Constitución Política de Colombia; Ley 1581 de 2012; Ley 1266 de 2008 (Habeas Data financiero); Decreto 1074 de 2015; Circular Única de la SIC, Título V.

URIBE · YÁÑEZ

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

10

¿Cuáles son los principios rectores para el Tratamiento de datos personales?

- Principio de legalidad;
- Principio de finalidad;
- Principio de libertad;
- Principio de veracidad o calidad;
- Principio de transparencia;
- Principio de acceso y circulación restringida;
- Principio de seguridad;
- Principio de confidencialidad

URIBE · YÁÑEZ

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

11

¿Quiénes deben cumplir con los principios del Tratamiento de Datos Personales?

Los Responsables y Encargados del Tratamiento de los Datos. Estos a su vez, deben verificar que sus empleados cumplan con dichos principios.

URIBE · YÁÑEZ

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

12

¿Qué busca el principio de seguridad y el principio de confidencialidad?

Que los Responsables y Encargados del Tratamiento tomen medidas técnicas, humanas y administrativas para evitar la adulteración, pérdida, uso o acceso no autorizado o fraudulento a los Datos Personales.

URIBE · YÁÑEZ

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

13

¿Qué es el principio de acceso y circulación restringida? ¿Cómo hacerlo efectivo?

El principio de acceso y circulación restringida establece que el Tratamiento de los Datos Personales podrá realizarse por las personas autorizadas por el Titular y/o por aquellas bases de datos que estén exentas del ámbito de aplicación de la Ley.

AUTORIDAD DE PROTECCIÓN DE DATOS EN COLOMBIA

14

¿Quién es la Autoridad de Protección de Datos en Colombia?

La SIC tiene facultad para investigar y sancionar a las entidades del orden privado y solo podrá investigar a los organismos del orden público. En vista de ello, la entidad administrativa facultada para sancionar a las autoridades públicas será la Procuraduría General de la Nación.

Industria y Comercio
SUPERINTENDENCIA

AUTORIDAD DE PROTECCIÓN DE DATOS EN COLOMBIA

15

¿Cuáles son las funciones de la SIC?

La Superintendencia de Industria y Comercio tiene funciones que incluyen garantizar la protección de datos, investigar y tomar medidas, bloquear datos en casos de riesgo, promover derechos mediante campañas, dar instrucciones de adecuación, solicitar información, emitir declaraciones, administrar un registro, sugerir ajustes normativos, y colaborar internacionalmente según la ley.

URIBE · YÁÑEZ

ÁMBITO DE APLICACIÓN RÉGIMEN GENERAL

16

¿A quién le aplica el Régimen General de Protección de Datos?

A todas aquellas personas naturales o jurídicas que tengan Datos Personales en sus bases de datos. La Superintendencia de Industria y Comercio ha expuesto que: "El régimen general de protección de datos personales es aplicable a todas las sociedades y entidades en Colombia sin excepción."1

1 SIC, (s.f.). Enlace aquí.

ÁMBITO DE APLICACIÓN RÉGIMEN GENERAL

17

¿Una entidad u organismo de carácter público está sometido al Régimen General de Protección de Datos?

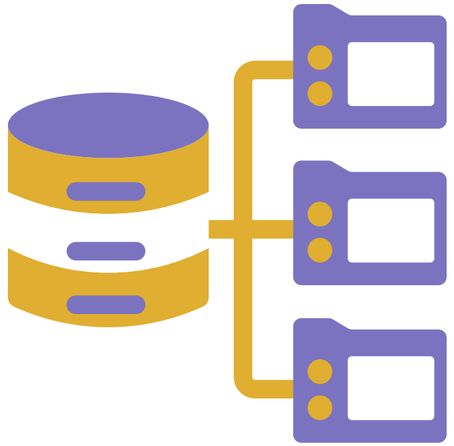
El Régimen aplica tanto a entidades de naturaleza privada como pública. Sin embargo, existen excepciones muy puntuales como las bases de datos de defensa nacional, inteligencia y contrainteligencia, entre otras, contenidas en el art. 2 de la Ley 1581 de 2012.

ÁMBITO DE APLICACIÓN RÉGIMEN GENERAL

18

¿Cuándo NO aplica el régimen general de tratamiento de datos?

a. A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico;
b. A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
c. A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.
d. A las bases de datos y archivos de información periodística y otros contenidos editoriales, y
e. A las bases de datos y archivos regulados por la Ley 1266 de 2008 y la Ley 79 de 1993.



ÁMBITO DE APLICACIÓN RÉGIMEN GENERAL

19

¿Las empresas extranjeras deben cumplir con el régimen General de Protección de Datos?

Las empresas extranjeras deberán cumplir con el Régimen de Datos en dos casos:

I. Cuando la sociedad extranjera posea una filial, subsidiaria o empresa en Colombia y esta última realice el Tratamiento de Datos Personales de los residentes en Colombia;
II. Cuando la empresa extranjera no radicada en Colombia realice actividades de Tratamiento en nuestro territorio y deba acobijarse a la normatividad del país.

DERECHOS DEL TITULAR DEL DATO

20

¿Cuáles son los derechos de los Titulares sobre sus datos personales?

Conocer, actualizar y rectificar sus Datos Personales, revocar la autorización para el tratamiento, solicitar la supresión de sus datos, quejarse ante la SIC, solicitar prueba de la autorización.

URIBE · YÁÑEZ

DERECHOS DEL TITULAR DEL DATO

Tap Here

DERECHOS DEL TITULAR DEL DATO

21

¿El Titular puede solicitar prueba de la autorización para el Tratamiento las veces que desee y de manera gratuita?

El derecho de acceso a los Datos Personales implica que el Titular conozca sobre la información que ha recolectado el Responsable de él, de manera que pueda ejercer sus derechos de actualización, rectificación y supresión de estos.

DERECHOS DEL TITULAR DEL DATO

22

Además del Titular, ¿Quiénes pueden solicitar acceso a la información del Titular?

Sus causahabientes o representantes legales, entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial, así como cualquier tercero autorizado por el Titular o por la ley (Ley 1581 de 2012, Art. 13).

DERECHOS DEL TITULAR DEL DATO

23

¿El Titular puede obligar al Responsable a que este trate sus Datos de acuerdo con las finalidades que escoja o se debe realizar el tratamiento con la totalidad de las finalidades dispuestas?

Según el Decreto 1074 de 2015, al solicitar permiso para usar datos personales, se deben especificar todas las razones para su uso. Si se requiere información, el responsable debe usar esos datos solo para el propósito indicado y no para publicidad u otros fines sin autorización.

DERECHOS DEL TITULAR DEL DATO

24

¿El titular puede requerir al Responsable y/o al Encargado mediante una consulta o reclamo? ¿Están solidariamente obligados a responder al Titular?

Al amparo del art. 8 de la Ley 1581 de 2012, se establece que el titular tendrá como derecho:

a) "Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado."

DERECHOS DEL TITULAR DEL DATO

25

Para presentar una queja ante la Superintendencia de Industria y Comercio (SIC), ¿Qué trámite debe haber agotado el Titular como requisito de procedibilidad?

En primer lugar, se debe presentar una consulta o reclamo al Responsable o Encargado del Tratamiento. En caso de no ser resuelto, podrá elevar la queja ante la SIC (art. 16, Ley 1581 de 2012).

DERECHOS DEL TITULAR DEL DATO

26

¿El habeas data es un derecho constitucional? ¿El titular podría proteger la vulneración de sus datos personales a través de una tutela?

El derecho de habeas data está consagrado como un derecho fundamental en el art. 15 de la Constitución Política de Colombia.

En ese sentido, el art. 86 de la carta establece que "toda persona tendrá acción de tutela para reclamar ante los jueces, (…) la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados".

DERECHOS DEL TITULAR DEL DATO

27

Si una empresa contacta por vía telefónica al Titular para ofrecerle un servicio y este no le ha otorgado la autorización para el Tratamiento de sus Datos, ¿puede quejarse del hecho ante la Autoridad de Datos?

Para realizar el Tratamiento de Datos Personales, el Responsable o Encargado debe contar la autorización del Titular.

Sin embargo, antes de presentar la queja a la SIC, debe presentar la queja ante la empresa que lo contactó.

AUTORIZACIÓN DEL TITULAR

28

¿Qué es la autorización para el Tratamiento de datos y quién la otorga?

La autorización es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales (Ley 1581 de 2012, Art. 3).

AUTORIZACIÓN DEL TITULAR

29

¿Cuáles son los tres mecanismos o formas por las cuales se puede obtener la autorización del Titular?

De forma escrita, verbal o de forma inequívoca.

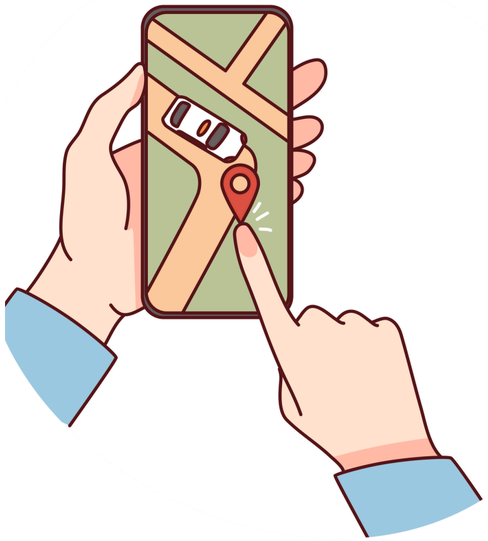
AUTORIZACIÓN DEL TITULAR

30

¿Es legítimo obtener la autorización del Titular por cualquier medio? (i.e. vía telefónica, chat de WhatsApp, correo electrónico, etc.)

De acuerdo con la legislación, la autorización "deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior" (Ley 1581 de 2012, Art. 9).

En tal sentido, cualquier medio físico o electrónico que permita almacenar la autorización para que posteriormente pueda ser consultada por el Titular o solicitada por la SIC será válido.



AUTORIZACIÓN DEL TITULAR

31

En caso de que el Titular desee, ¿puede revocar su autorización en cualquier circunstancia o momento?

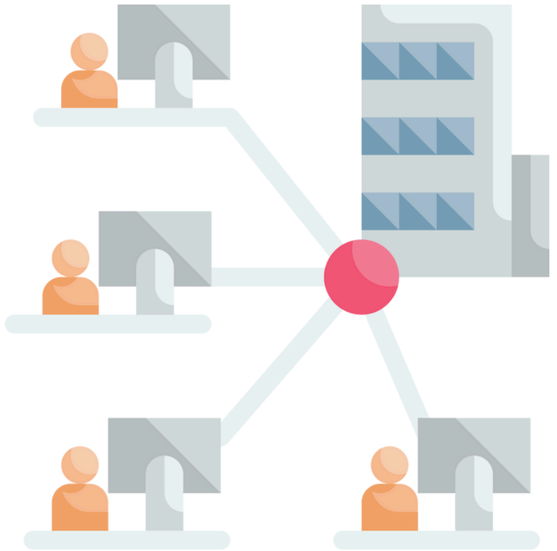
En el único caso donde no procederá la revocatoria de la autorización será cuando el Titular posea una obligación legal o contractual que implique la permanencia de su información en la base de datos del Responsable (art. 2.2.2.25.2.6., Decreto 1074 de 2015).

AUTORIZACIÓN DEL TITULAR

32

Si al momento de solicitar un préstamo el titular autorizó a una entidad financiera para que tratar sus datos, ¿puede revocar dicha autorización cuando lo llamen para cobrar?

No procederá la revocatoria ya que el Titular detenta una obligación legal o contractual que implica que sus Datos Personales reposen en las bases de datos del Responsable/Encargado (art. 2.2.2.25.2.6., Decreto 1074 de 2015).



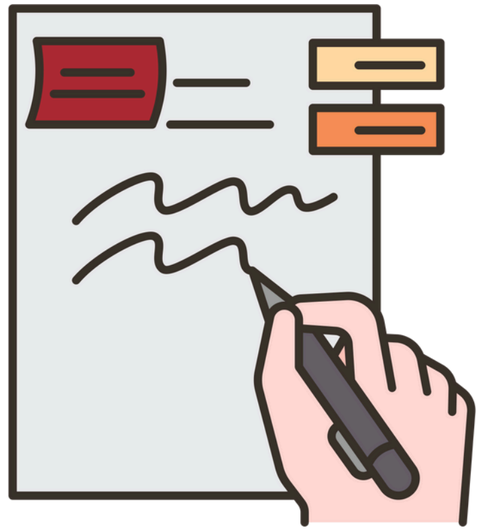
AUTORIZACIÓN DEL TITULAR

33

¿En qué casos no es necesaria la autorización del Titular para tratar su información?

De acuerdo con el art. 10 de la Ley 1581 de 2012, no será necesaria la autorización del Titular en los siguientes casos:

A. Cuando la información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
B. Datos de naturaleza pública;
C. Casos de urgencia médica o sanitaria;
D. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
E. Datos relacionados con el Registro Civil de las Personas.

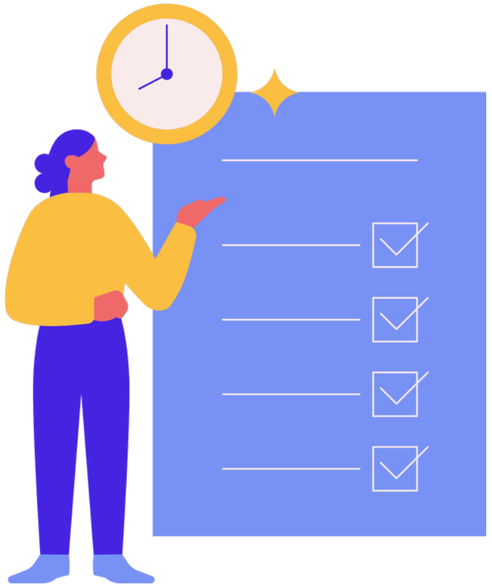


AUTORIZACIÓN DEL TITULAR

34

¿Durante qué período debe el responsable almacenar autorización para el Tratamiento otorgada por el Titular?

No está expresamente establecido en la ley un período entre el cual el Responsable/Encargado deban almacenar la copia de la autorización del Titular. Sin embargo, sí se fija que el Titular deberá poder solicitar copia de su autorización, por lo que se entiende que, como mínimo, el Responsable y/o Encargado del Tratamiento deberán almacenar la autorización por el período que traten los Datos Personales del Titular.



AUTORIZACIÓN DEL TITULAR

35

¿Qué información debe indicar el Responsable o Encargado del Tratamiento cuando esté recolectando información del Titular?

De acuerdo con el art. 12 de la Ley 1581 de 2012, el Responsable deberá informar de manera clara y expresa lo siguiente:

A. El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
B. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
C. Los derechos que le asisten como Titular;
D. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Aunque no está expresamente establecido que el Encargado deba informar al Titular estos apartados, ya que puede solicitar directamente la autorización al Titular, se recomienda hacerlo.

URIBE · YÁÑEZ

AUTORIZACIÓN DEL TITULAR

36

Si no se informa al Titular sobre las finalidades del Tratamiento en el momento que se obtiene su autorización, ¿dicha autorización es válida?

No será válida, de acuerdo con el Art. 12 de la Ley 1581de 2012.

AUTORIZACIÓN DEL TITULAR

37

Si el Titular suministra sus Datos al Responsable, pero este último no le solicitó la autorización, ¿se entiende intrínsecamente que el Titular desee que le traten sus Datos Personales? ¿Es válido como una autorización?

Podría ser una conducta inequívoca, sin embargo, posiblemente no habría prueba de dicha autorización y posiblemente no sería clara la finalidad autorizada.

También es problemático porque no cumple cabalmente con el principio de finalidad.

AUTORIZACIÓN DEL TITULAR

38

¿El silencio es un tipo de autorización?

El silencio de la persona no podrá ser entendido como autorización y siempre se requerirá, por lo menos, una conducta inequívoca del mismo o en su defecto la autorización expresa de manera verbal o escrita.

DATOS PERSONALES A MENORES DE EDAD

39

¿Está prohibido el Tratamiento de Datos Personales de menores de edad?

Aunque el art. 7 de la Ley 1581de 2012 lo proscribe y solo permite el Tratamiento de datos de carácter público, la Corte Constitucional ha establecido que se puede realizar el Tratamiento de datos de menores, pero con niveles de seguridad y tecnológicos más altos en comparación con la información personal de mayores de edad.

La Corte Constitucional declara como inexequible la expresión "salvo aquellos que sean de naturaleza pública" en una ley específica. Esta medida busca proteger la falta de consentimiento legal en menores, asegurando que el consentimiento otorgado por su tutor sea efectivo y evitando la divulgación indiscriminada de información en medios públicos, con el fin de proteger los derechos de los menores.

3 “Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.”

DATOS PERSONALES A MENORES DE EDAD

40

¿Cuáles son los requisitos para tratar los Datos de menores?

El Tratamiento de Datos de menores de edad tiene tres requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes;
- Que se asegure el respeto de sus derecho fundamentales;

Una vez se cumplan los anteriores requisitos, el representante legal del menor otorgará la Autorización para el Tratamiento una vez se tenga en cuenta la madurez, autonomía y capacidad del menor para comprender el asunto.

5 Art. 2.2.2.25.2.9. del Decreto 1074 de 2015.

DATOS PERSONALES A MENORES DE EDAD

41

¿El representante legal del menor de edad puede autorizar el tratamiento de sus Datos aun cuando el niño o niña no esté de acuerdo?

De acuerdo con el tercer requisito antes mencionado (“se tenga en cuenta la madurez, autonomía y capacidad del menor para comprender el asunto”), es relevante ponderar si la voluntad del menor de no permitir el Tratamiento de sus Datos Personales podría vulnerar el ejercicio de sus derechos fundamentales o podría afectarlo de una manera indebida, así como se tendrá que revisar la madurez del menor.

DATOS PERSONALES A MENORES DE EDAD

42 ¿Se necesita la autorización del acudiente siempre?

De acuerdo con el Decreto 1074 de 2015,6 luego de cumplir los requisitos para tratar los Datos Personales de un menor, deberá obtenerse en todos los casos la autorización del tutor o representante del menor, así como deberá ser tenida en cuenta la opinión del niño.

6 "Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto." (Art. 2.2.2.25.2.9., Decreto 1074 de 2015).

POLÍTICA DE TRATAMIENTO DE DATOS

43

¿Qué es una Política de Tratamiento de Datos?

La Política de Tratamiento de Datos tiene como fin que los Titulares y las personas interesadas tengan a su disposición la información necesaria y suficiente sobre los diferentes tratamientos y fines sobre los que serán objeto sus datos, así como los derechos que ellos, como titulares de datos personales, pueden ejercer frente al Responsable y/o Encargado del Tratamiento (SIC, s.f.).

7 Extraído de la Política de Tratamiento de Datos de la SIC. Enlace aquí.

URIBE · YÁÑEZ

POLÍTICA DE TRATAMIENTO DE DATOS

44

¿Quiénes están obligados a tener una Política de Tratamiento de Datos?

Cualquier persona natural o jurídica que trate Datos Personales.

POLÍTICA DE TRATAMIENTO DE DATOS

45

En relación con el acceso a la Política de Tratamiento, ¿debe ser de libre y público acceso o su disponibilidad debe ser restringida?

Debe ser puesta al conocimiento de los Titulares ya sea por medios físicos o electrónicos. Su disponibilidad debe ser abierta, para que el Titular pueda consultarla en el momento que desee (Decreto 1074 de 2015, art. 2.2.2.25.3.1).

URIBE · YÁÑEZ

POLÍTICA DE TRATAMIENTO DE DATOS

46

¿Qué requisitos mínimos debe contener la Política de Tratamiento de Datos?

Los requisitos mínimos del contenido de la Política de Tratamiento de Datos son:

A. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
B. Tratamiento al cuál serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.
C. Derechos que le asisten cómo Titular.
D. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. E. Procedimiento para que los titulares de la información puedan ejercer sus derechos. F. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

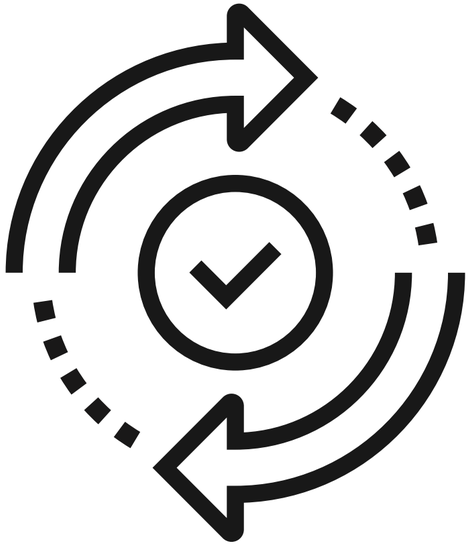
URIBE · YÁÑEZ

POLÍTICA DE TRATAMIENTO DE DATOS

47

En caso de realizar cambios sustanciales a la Política de Tratamiento, ¿se le debe informar al Titular? ¿Se debe solicitar su autorización nuevamente?

Según el art. 2.2.2.25.2.2 del Decreto 1074 de 2015, si hay cambios significativos en las políticas de tratamiento de datos que afecten la identificación del responsable o la finalidad del tratamiento, este debe informar al titular antes de implementar los cambios. Además, si la modificación afecta la finalidad del tratamiento, debe obtener una nueva autorización del titular.



POLÍTICA DE TRATAMIENTO DE DATOS

48

Suponiendo que el Responsable tiene autorización para transmitir los datos de forma genérica, sin especificar a quien ¿El Responsable puede proporcionar Datos Personales al Encargado a pesar que este último no ha sido expresamente mencionado o facultado en la Política de Tratamiento de Datos?

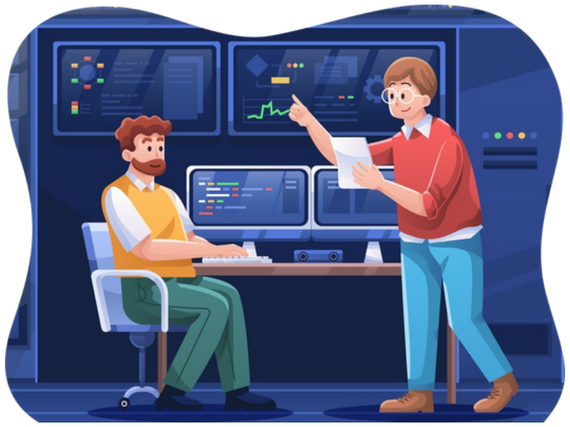
Para compartir datos personales con un tercero, el responsable debe informar al titular y obtener su autorización. Sin dicho consentimiento, no se puede compartir la información, violando el principio de acceso restringido.

POLÍTICA DE TRATAMIENTO DE DATOS

49

¿El Encargado puede, directamente con el Titular, solicitar y recolectar los Datos siempre y cuando se realice conforme a la Política de Tratamiento de Datos del Responsable?

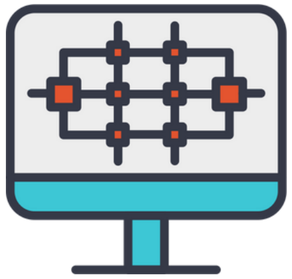
Sí, si el responsable autoriza al encargado a través de un contrato y política adecuada, el encargado puede solicitar directamente datos personales al titular. Por ejemplo, los Call Center actúan como encargados y obtienen datos del titular para resolver problemas relacionados con la empresa.



POLÍTICA DE TRATAMIENTO DE DATOS

50

¿Puede el Responsable recolectar cualquier tipo de dato sin importar el medio físico o tecnológico?



El responsable puede recopilar datos personales con autorización del titular. Si son datos sensibles, el titular puede optar por no dar su consentimiento. En el caso de datos de menores, se debe respetar sus derechos, considerar su madurez y obtener la autorización de su tutor o representante legal.

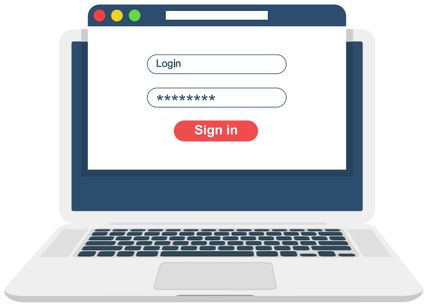
El responsable debe especificar en su Política de Tratamiento los propósitos legítimos para recopilar cualquier dato personal, sin importar el medio utilizado. Recolectar información sin un propósito claro y definido constituye una violación al Régimen General de Datos.

POLÍTICA DE TRATAMIENTO DE DATOS

51

¿Los tipos de Datos Personales que recolecte el Responsable deben estar taxativamente dispuestos en la Política de Tratamiento? En caso de que no se encuentren expresos en la Política, ¿el Responsable puede recolectarlos?

Aunque la ley no especifica todos los tipos de datos personales a tratar, el Decreto requiere que el titular sea informado a través de la Política de Tratamiento sobre cómo se tratarán sus datos. Por lo tanto, el responsable debe indicar generalmente qué datos se tratarán y cómo se procesarán.



AVISO DE PRIVACIDAD

52

¿Qué es el aviso de privacidad?

De acuerdo con el numeral 1° del art. 2.2.2.25.1.3. del Decreto 1074 de 2015, se establece que:

"1. Aviso de privacidad. Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cuál se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales."

URIBE · YÁÑEZ

AVISO DE PRIVACIDAD

53 ¿Cuáles son los requisitos mínimos del aviso de privacidad?

De acuerdo con lo establecido en el artículo 2.2.2.25.3.3. del Decreto 1074 de 2015:

1. Nombre o razón social y datos de contacto del responsable del tratamiento.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al titular.
4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información".

AVISO DE PRIVACIDAD

54

¿En qué casos se debe poner a disposición del Titular el aviso de privacidad?

De acuerdo con el artículo 2.2.2.25.3.2 del Decreto 1074 de 2015 el aviso de privacidad deberá estar a disposición del titular cuando:

"Artículo 2.2.2.25.3.2. Aviso de privacidad. En los casos en los que no sea posible poner a disposición del Titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales."

AVISO DE PRIVACIDAD

55

¿El aviso de privacidad reemplaza la autorización del Titular o sirve como esta?

La función del aviso de privacidad es la de dar a conocer a los Titulares la Política de Tratamiento de Información, pero no la de reemplazar la obligación de obtener la autorización de la persona. La Política de Tratamiento de Información no es necesario aceptarla. Lo que exige la regulación es que la misma sea puesta en conocimiento de los Titulares de los datos personales.

URIBE · YÁÑEZ

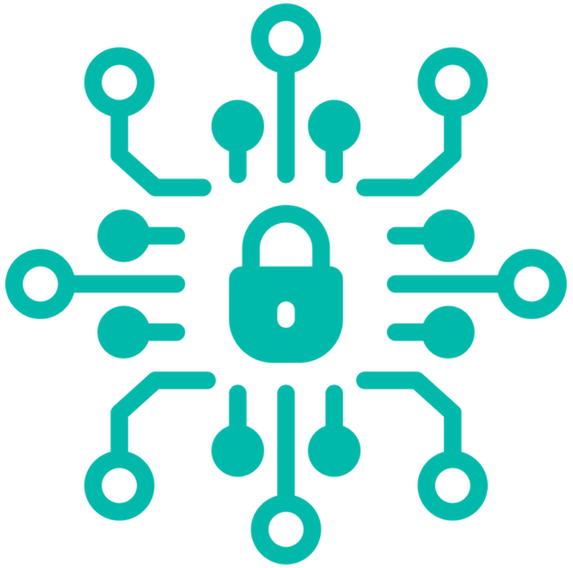
AVISO DE PRIVACIDAD

56

¿Qué medios de difusión se deben disponer para dar a conocer al Titular sobre el aviso de privacidad?

De acuerdo con lo que se establece en el artículo 2.2.2.25.3.5. del Decreto 1074 de 2015:

Medios de difusión del aviso de privacidad y de las políticas de tratamiento de la información. Para la difusión del aviso de privacidad y de la política de tratamiento de la información, el responsable podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.



AVISO DE PRIVACIDAD

57

Si el Responsable y/o Encargado no ponen a disposición del Titular el aviso de privacidad, ¿están incumpliendo sus obligaciones? ¿Esto da origen a alguna sanción?

El responsable cumple sus obligaciones dependiendo de si debe publicar o no el aviso de privacidad. Si la política de tratamiento es accesible para todos, incluido el titular al dar su autorización, no es necesario presentar el aviso de privacidad. Sin embargo, si no es accesible, debe hacerlo. Si no cumple con esta obligación, podría enfrentar una sanción de hasta 2 mil SMLMV.

DATOS SENSIBLES

58

¿Qué es un dato sensible?

De acuerdo con el Decreto 1074 de 2015, en el artículo mencionado, los datos sensibles son aquellos que pueden afectar la intimidad del titular o generar discriminación. Esto incluye información sobre origen racial o étnico, orientación política, creencias religiosas o filosóficas, afiliación a sindicatos u organizaciones, así como datos relacionados con salud, vida sexual y características biométricas.

DATOS SENSIBLES

59

¿Se puede realizar el tratamiento de datos sensibles? De ser así, ¿en qué casos ha dispuesto la normativa que se permite el tratamiento de datos sensibles?

El artículo 6 de la Ley 1581 de 2012 establece excepciones para el tratamiento de datos sensibles:

a) Cuando el titular otorgue su consentimiento explícito, excepto cuando la ley no lo requiera.
b) Si es necesario para proteger el interés vital del titular incapacitado, requiriendo autorización de sus representantes legales.
c) En actividades legítimas de fundaciones, ONGs, entre otros, con fines políticos, filosóficos, religiosos o sindicales, pero solo para sus miembros o contactos regulares, sin compartirlo con terceros sin consentimiento.
d) Cuando se necesiten datos para reconocer, ejercer o defender un derecho en un proceso judicial.
e) Con fines históricos, estadísticos o científicos, asegurando la supresión de la identidad de los titulares.

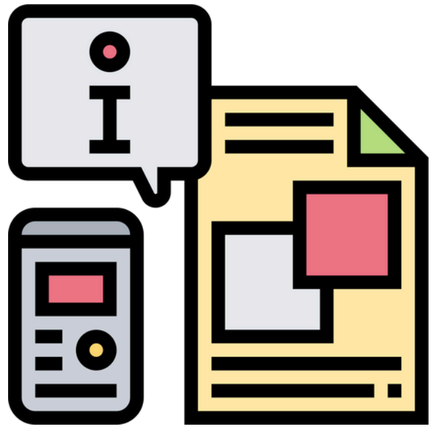
URIBE · YÁÑEZ

DATOS SENSIBLES

60

¿Es optativo u obligatorio entregar datos sensibles para su Tratamiento?

Optativo



URIBE · YÁÑEZ

DATOS SENSIBLES

61

¿Las fotografías son datos sensibles?

Sí, ya que algunas fotografías captan la imagen de la cara de las personas u otras partes del cuerpo que permiten identificarlas, y estas imágenes se consideran información biométrica, que a su vez son un ejemplo de dato sensible, tal como se puede constatar en la definición legal del artículo 5 de la ley estatutaria 1581 de 2012.

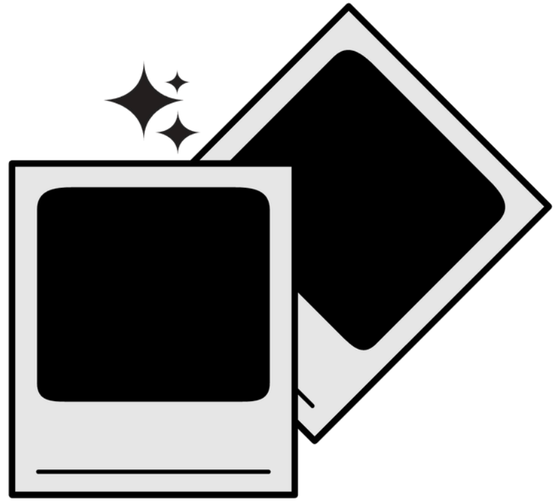
URIBE · YÁÑEZ

DATOS SENSIBLES

62

¿En qué casos la fotografía no es un Dato Personal?

La foto será un dato personal en la medida en que permita establecer la identidad de una persona o varias personas naturales en particular. Si por ejemplo, la foto contiene la imagen de personas con máscaras en su rostro o que están de espaldas de tal forma que no se pueda establecer la identidad de cada una de ellas, pues la fotografía no será un dato personal.



URIBE · YÁÑEZ

DATOS SENSIBLES

63

¿La información relacionada a la discapacidad de una persona puede constituirse como Dato Sensible?

Sí, ya que el artículo 5 de la ley 1581 de 2012 donde se define lo que es un dato sensible establece que lo serán los datos relativos a la salud de una persona, y en todo caso la información relacionada a la discapacidad que padece una persona hace parte de información relativa a su salud, y en ese sentido será un dato personal sensible.

URIBE · YÁÑEZ

DATOS BIOMÉTRICOS

64

Qué es un Dato Biométrico?

El Dato Biométrico es un Dato Personal "obtenido a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permita o confirme la identificación única de dicha persona, como la imagen facial o datos dactiloscópicos" (RGPD UE, 2016).8

8 Obtenido del RGPD, Unión Europea.

URIBE · YÁÑEZ

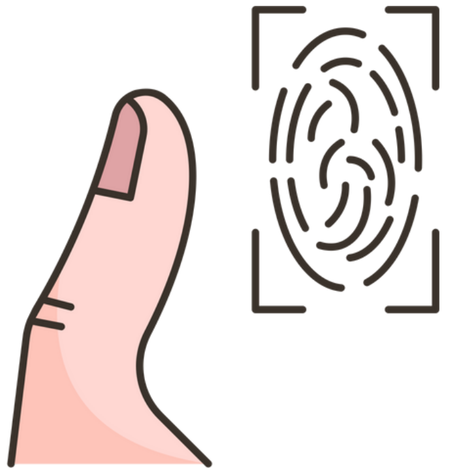
DATOS BIOMÉTRICOS

65

¿Los Datos Biométricos son Datos Sensibles?

Los Datos Biométricos son considerados sensibles debido a que capturan características físicas o comportamentales, permitiendo la discriminación en temas como raza, género, religión, salud, orientación sexual, entre otros.

Dado que estos datos están vinculados a la identidad de una persona, su tratamiento debe ser cuidadoso y sometido a una protección más rigurosa. Esto implica cumplir con requisitos específicos, como obtener el consentimiento explícito del titular, informándole sobre la naturaleza opcional de su autorización, y aplicar medidas de seguridad adecuadas para proteger los derechos y libertades de los titulares de los datos.

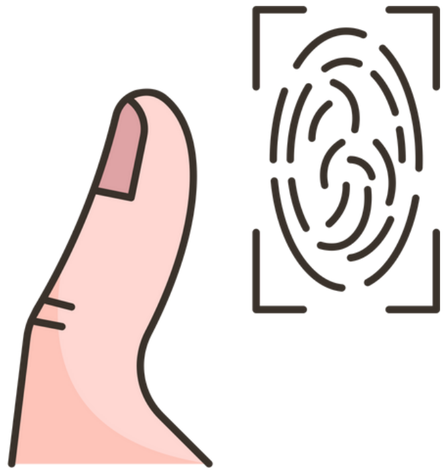


DATOS BIOMÉTRICOS

66

¿Qué ha dicho la SIC?

De acuerdo con el concepto No. 18-171259-1 de la SIC, “los datos biométricos son datos sensibles que permiten identificar a una persona natural a través del reconocimiento de una característica física e intransferible, que al ser única de cada individuo, permite distinguir a un ser humano de otro” (SIC, 2018).



DATOS BIOMÉTRICOS

67

¿Las características comportamentales de un individuo (forma de firma, tono de voz) son un Dato Biométrico?

Las características comportamentales de una persona, como la forma de firma o el tono de voz, pueden considerarse Datos Biométricos si se utilizan para identificar de manera única a una persona.

Por ejemplo, la firma es una característica que puede utilizarse para identificar a una persona y, por lo tanto, puede considerarse un Dato Biométrico. Lo mismo ocurre con el tono de voz, que puede utilizarse para identificar a una persona de manera única.

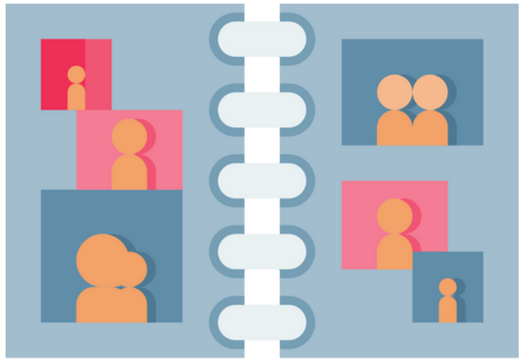
DATOS BIOMÉTRICOS

68

En caso de tomar fotografías a un familiar para guardarlas en un álbum familiar, ¿se necesitará de la autorización del Titular para tratar y almacenar dicha foto?

No se requiere autorización del titular para tomar y almacenar fotografías de un familiar con fines personales y domésticos, como guardarlas en un álbum familiar.

Esta exención se basa en el artículo 2, literal A, de la Ley 1581 de 2012, que establece que la norma no se aplica al tratamiento de datos personales realizado en el ámbito exclusivamente personal o doméstico.



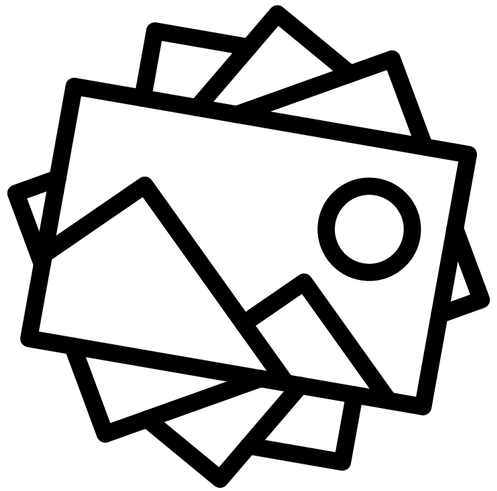
URIBE · YÁÑEZ

DATOS BIOMÉTRICOS

69

Las fotografías de una persona que sean publicadas en sitios web o redes sociales, ¿pueden ser usadas para un ámbito comercial sin contar con la autorización del Titular?

La publicación no autorizada de fotos en internet viola la Ley 1581 de 2012, que garantiza el derecho del titular a controlar sus datos. Se requiere consentimiento previo, expreso e informado del titular para el tratamiento de datos, especialmente en el caso de uso comercial o publicitario de las fotos.



URIBE · YÁÑEZ

DATOS BIOMÉTRICOS

70

En caso de instalar un Circuito Cerrado de Televisión (CCTV) dentro de su establecimiento comercial, ¿cómo podría obtener la autorización de los clientes que ingresan, más no firman una autorización escrita para el Tratamiento de sus Datos Biométricos?

La cartilla de Vigilancia de la SIC establece que la seguridad en espacios públicos es responsabilidad exclusiva del Estado, excluyendo a particulares. En entornos privados, la operación de sistemas de vigilancia puede incluir la captura de imágenes en la vía pública, pero solo lo necesario para garantizar la seguridad, evitando la recolección innecesaria.

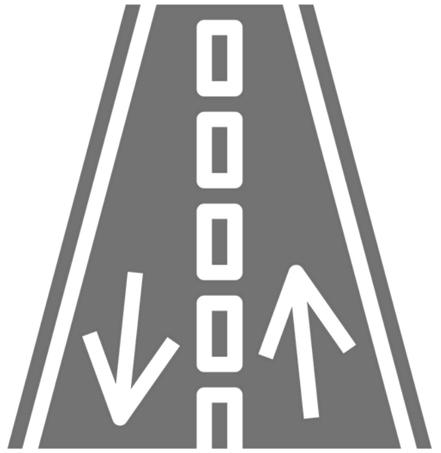
URIBE · YÁÑEZ

DATOS BIOMÉTRICOS

71

¿Se puede establecer un sistema de CCTV en vía pública? ¿Qué requerimientos se deben cumplir para que esta recolección de datos sea acorde a la normatividad?

La cartilla de Vigilancia de la SIC destaca que la seguridad en lugares públicos es responsabilidad del Estado, excluyendo a particulares de operar sistemas de vigilancia en esos espacios. No obstante, en entornos privados, la operación de sistemas de vigilancia puede incluir la captura de imágenes en la vía pública, pero solo cuando sea necesario para garantizar la seguridad, limitando la recolección a lo esencial para alcanzar el fin legítimo perseguido.



URIBE · YÁÑEZ

DATOS BIOMÉTRICOS

72

¿Es necesario obtener autorización de terceros para que un titular acceda a un video de CCTV en el que aparecen esos terceros, o se le debe permitir acceso sin restricciones?

Según la cartilla de vigilancia de la SIC, se requiere autorización de terceros titulares de datos personales que aparecen en imágenes. Si no se obtiene, los responsables del tratamiento deben asegurar la anonimización de esos datos, como hacer borrosa o fragmentar la imagen de dichos terceros.


Cámara en los probadores | Los Simpson
Copy link
Watch on YouTube

Tap Here

DERECHO AL USO DE LA IMAGEN

73

Desde la perspectiva de un productor o director de cine y televisión (o en general, un tercero que no sea el titular de los datos) ¿Qué es el Derecho al uso de la imagen?

La imagen, que incluye rasgos personales como el estilo de vestir, requiere un contrato de licencia para su uso. Este contrato debe especificar el tiempo, medios y territorio de uso, así como la remuneración del titular de la imagen.

DERECHO AL USO DE LA IMAGEN

74

¿Qué es la característica de temporalidad en el Derecho al uso de imagen?

La temporalidad en la cesión de imagen implica que el titular autoriza el uso por un tiempo específico, establecido en el contrato de licencia. Este periodo puede discutirse y no tiene límites si el cedente está de acuerdo.

DERECHO AL USO DE LA IMAGEN

75

¿Qué es la característica de geografía en el Derecho al uso de imagen?

Se delimita el uso de imagen a un espacio geográfico específico.

DERECHO AL USO DE LA IMAGEN

76

¿Qué diferencia hay, cuando una imagen de un modelo se usa conforme a un contrato de licencia de uso de la imagen y cuando se usa la imagen de una persona conforme a la autorización que dio dicho titular para el tratamiento de sus datos personales, según una política de privacidad?

El uso de la imagen está regulado por el contrato de licencia, impidiendo modificaciones arbitrarias. Existen excepciones, como usos literarios, científicos, didácticos o culturales que no requieren autorización. Si se trata de datos personales, el titular puede optar por no otorgar su imagen y puede revocar la autorización. Siempre se debe obtener autorización para el tratamiento de la imagen, informando sobre su carácter sensible y la opción de no otorgarla.

DERECHO AL USO DE LA IMAGEN

77

¿Puede un menor o su representante legal revocar la autorización de tratamiento de datos, incluso con un contrato de cesión del uso de imagen, dada la protección especial que tienen los menores en términos de Habeas Data?

La ley de habeas data asegura el respeto a los derechos de los niños y adolescentes, incluyendo la posibilidad de revocar su autorización. Se aplican parámetros especiales, como priorizar su interés superior, garantizar el respeto de sus derechos fundamentales, escuchar sus opiniones considerando su madurez y capacidad de comprensión.

DEBERES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

78

¿Qué requisitos debe cumplir el Responsable y/o Encargado para tratar los Datos Personales y respetar los derechos del Titular?

Según la Cartilla de la SIC y la Ley 1581 de 2012, el Responsable del tratamiento de datos debe tener procedimientos internos para obtener la autorización del titular al recolectar información. La ley exige un "consentimiento previo, expreso e informado", accesible para consultas futuras. Se necesita un manual interno para explicar parámetros y procedimientos, incluyendo cómo atender quejas y consultas. La política de tratamiento debe ser comunicada a los titulares de diversas formas para cumplir con el deber de informar.

DEBERES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

79

¿Cuáles son los deberes principales que existen para el Responsable del Tratamiento de los datos personales?

Según la cartilla de la SIC y la Ley 1581 de 2012, los deberes principales del responsable del tratamiento de datos son:

a) Garantizar al Titular el ejercicio pleno del derecho de hábeas data; b) Solicitar y conservar la autorización otorgada por el Titular; c) Informar al Titular sobre la finalidad de la recolección y sus derechos; d) Conservar la información de forma segura; e) Garantizar que la información entregada al Encargado del Tratamiento sea precisa y actualizada; f) Actualizar la información comunicando al Encargado todas las novedades respecto a los datos suministrados.
g) Rectificar información incorrecta y comunicarlo al Encargado del Tratamiento; h) Suministrar al Encargado datos autorizados previamente; i) Exigir al Encargado respetar condiciones de seguridad y privacidad; j) Gestionar consultas y reclamos según la ley; k) Adoptar un manual interno para cumplir la ley, especialmente en la atención de consultas y reclamos; l) Informar al Encargado cuando cierta información está en disputa por el Titular; m) Informar al Titular sobre el uso de sus datos; n) Notificar a la autoridad de protección de datos sobre violaciones a la seguridad; o) Cumplir instrucciones de la Superintendencia de Industria y Comercio.

URIBE · YÁÑEZ

DEBERES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

80

¿Cuáles son los deberes principales que existen para el Encargado del Tratamiento de los datos personales?

Según la política de tratamiento de datos personales de la sic y la ley 1581 de 2012, el encargado de datos personales debe: a) Asegurar el ejercicio pleno del derecho de hábeas data para el Titular; b) Salvaguardar la información contra adulteración, pérdida, consulta no autorizada, o uso fraudulento; c) Actualizar, corregir o eliminar datos según la ley; d) Actualizar información de los Responsables del Tratamiento en cinco días hábiles; e) Gestionar consultas y reclamos de Titulares; f) Establecer un manual interno para cumplir con la ley, especialmente para atender consultas y reclamos; g) Registrar "reclamo en trámite" en la base de datos, conforme a la ley.
h) Insertar "información en discusión judicial" en la base de datos al recibir notificación de procesos judiciales sobre la calidad del dato personal; i) No circular información disputada por el Titular y bloqueada por la Superintendencia de Industria y Comercio; j) Restringir el acceso a la información solo a personas autorizadas; k) Reportar a la Superintendencia de Industria y Comercio violaciones a códigos de seguridad y riesgos en la gestión de la información de Titulares; l) Cumplir instrucciones de la Superintendencia de Industria y Comercio. Parágrafo: Si una persona actúa como Responsable y Encargado del Tratamiento, debe cumplir con los deberes de ambos.

DATO PÚBLICO

81

¿Qué es un Dato Público?

Según el decreto 1074 de 2015, el dato público es aquel que no es semiprivado, privado o sensible. Incluye información sobre el estado civil, profesión, oficio y calidad de comerciante o servidor público. Estos datos pueden estar en registros públicos, documentos, gacetas y sentencias judiciales no sujetas a reserva.

URIBE · YÁÑEZ

DATO PÚBLICO

82

¿Los datos públicos se pueden tratar?

Sí, y según se establece en la ley 1581 de 2012 y la cartilla de formatos de datos personales de la SIC, los datos personales que sean de naturaleza pública pueden ser tratados y no necesitan autorización del titular para su uso, siempre y cuando se le dé el uso en concordancia con su naturaleza.

URIBE · YÁÑEZ

DATO PÚBLICO

83

En caso de que una persona decida publicar su número telefónico, correo electrónico, lugar donde reside, entre otros datos, en sus redes sociales, ¿esta información se puede tratar?

No, porque si bien es el mismo titular el que está dando a conocer sus datos personales, esto no es una autorización de su parte para que se haga el tratamiento de los mismos. En todo caso, independiente de si están publicados o no los datos personales de una persona, la autorización del titular para el tratamiento de sus datos sigue siendo un requisito obligatorio.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

84

¿Qué es la Transferencia de datos personales?

Según lo establece la cartilla sobre formatos modelo para el cumplimiento de obligaciones en materia de datos personales, la transferencia de datos personales se trata de la operación que realiza el responsable del tratamiento de los datos personales, cuando envía la información a otro receptor, que, a su vez, se convierte en responsable del tratamiento de esos datos.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

85

¿Qué es la Transmisión de datos personales?

Según la SIC en su sección de preguntas frecuentes sobre datos personales la transmisión de datos personales por su parte implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, la comunicación la realiza el responsable a un encargado.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

86

¿En qué casos se prohíbe la transferencia internacional de datos a otros países?

Según el artículo 26 de la ley 1581 de 2012 se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

87

¿Qué son los niveles adecuados de protección de datos y quién los fija?

Según las preguntas frecuentes de la SIC sobre tratamiento de datos personales se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

88

¿Qué excepciones existen a la prohibición de la Transferencia internacional de datos a otros países que no proporcionen niveles adecuados de seguridad de la información?

Según la SIC, la transferencia internacional de datos a países con niveles insuficientes de protección solo es posible si la Superintendencia de Industria y Comercio emite una DECLARACIÓN DE CONFORMIDAD. El Superintendente tiene la autoridad para solicitar información y verificar el cumplimiento necesario para aprobar dicha transferencia.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

89

Si una empresa colombiana de un grupo empresarial transfiere datos personales de titulares residentes en Colombia a otra empresa del grupo en México, ¿los datos deben tratarse según la normativa colombiana o mexicana?

En estos casos, considerar Normas Corporativas Vinculantes (NCV) es crucial para grupos empresariales, ya que son aplicables a todo el grupo, independientemente de su ubicación. Se puede presentar ante la SIC las NCV aplicables para verificar el cumplimiento de estándares de protección de datos según la ley, y también solicitar la verificación de estándares de protección de datos personales.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

90

¿Qué entidad determina los países con un nivel adecuado de protección de datos para realizar una transferencia internacional?

La Superintendencia de Industria y Comercio.

Industria y Comercio
SUPERINTENDENCIA

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

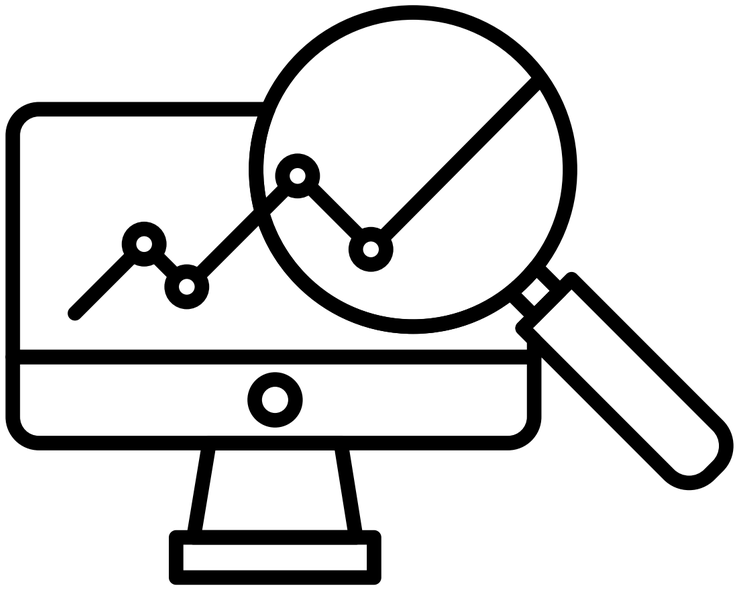
91

¿Dónde está regulada la transferencia internacional de datos personales?

Artículo 26 Ley 1581 de 2015

Capítulo Tercero del Título V de la Circular Única de la SIC (numeral 3.1., 3.2., 3.3.)

Decreto 1074 de 2015



TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

92

¿Qué es la Declaración de Conformidad y cómo se relaciona con la Transferencia internacional de Datos?

La SIC tiene la facultad de aprobar la transferencia de datos a países con niveles de seguridad diferentes a los de Colombia mediante la declaración de conformidad. El superintendente puede solicitar información y realizar diligencias para verificar el cumplimiento de los requisitos necesarios, declarando o negando la conformidad con la política de protección de datos personales.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

93

¿En qué se diferencia el tránsito transfronterizo con la Transferencia Internacional de Datos?

Según la circular externa 8 de 2017 de la SIC El tránsito transfronterizo de datos se refiere al simple paso de los datos por uno o varios territorios utilizando la infraestructura compuesta por todas las redes, equipos y servicios requeridos para alcanzar su destino final.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

94

Para realizar el tránsito transfronterizo de datos personales, ¿se necesita hacer diligenciamiento de la Declaración de Conformidad?

Según la circular externa 8 de 2017 de la SIC la declaración de conformidad se debe dar cuando haya transferencia de datos a terceros países que no cuentan con niveles adecuados para la protección de datos. En el caso del tránsito transfronterizo no porque el simple tránsito transfronterizo de datos no comporta una transferencia de datos a terceros países.

URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

95

¿Qué es el contrato de Transmisión de Datos Personales?

Según lo establecido en el decreto 1074 de 2015 artículo 2.2.2.25.5.2. el Contrato de transmisión de datos personales es el contrato que suscriba el Responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad, que en todo caso señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el Responsable.

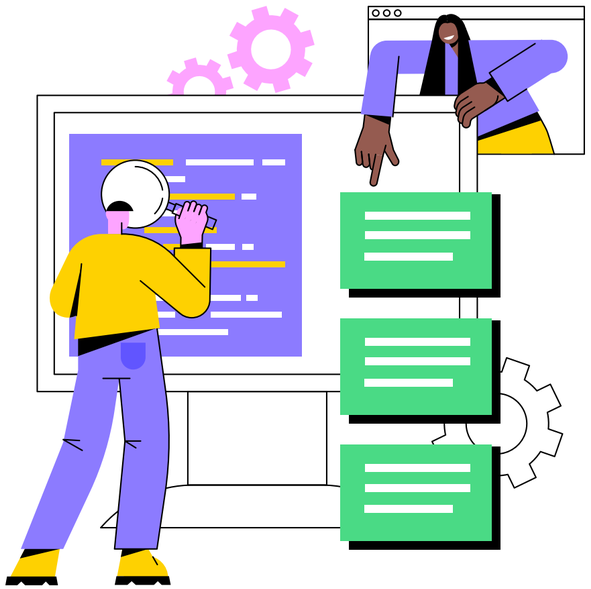
URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

96

¿Qué requisitos debe cumplir el contrato de Transmisión de Datos Personales?

- Dar tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
- Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales. (Decreto 1377 de 2013, artículo 25).



URIBE · YÁÑEZ

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

97

Para que exista la figura del Encargado, ¿debe mediar un contrato de Transmisión de Datos? ¿Sin dicho contrato el tercero no podrá obtener el título de Encargado?

Para ser considerado encargado, debe haber un encargo formalizado en un contrato. Según el decreto 1377, este contrato compromete al encargado a seguir la política de tratamiento del responsable y procesar los datos según la autorización de los titulares y las leyes vigentes.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

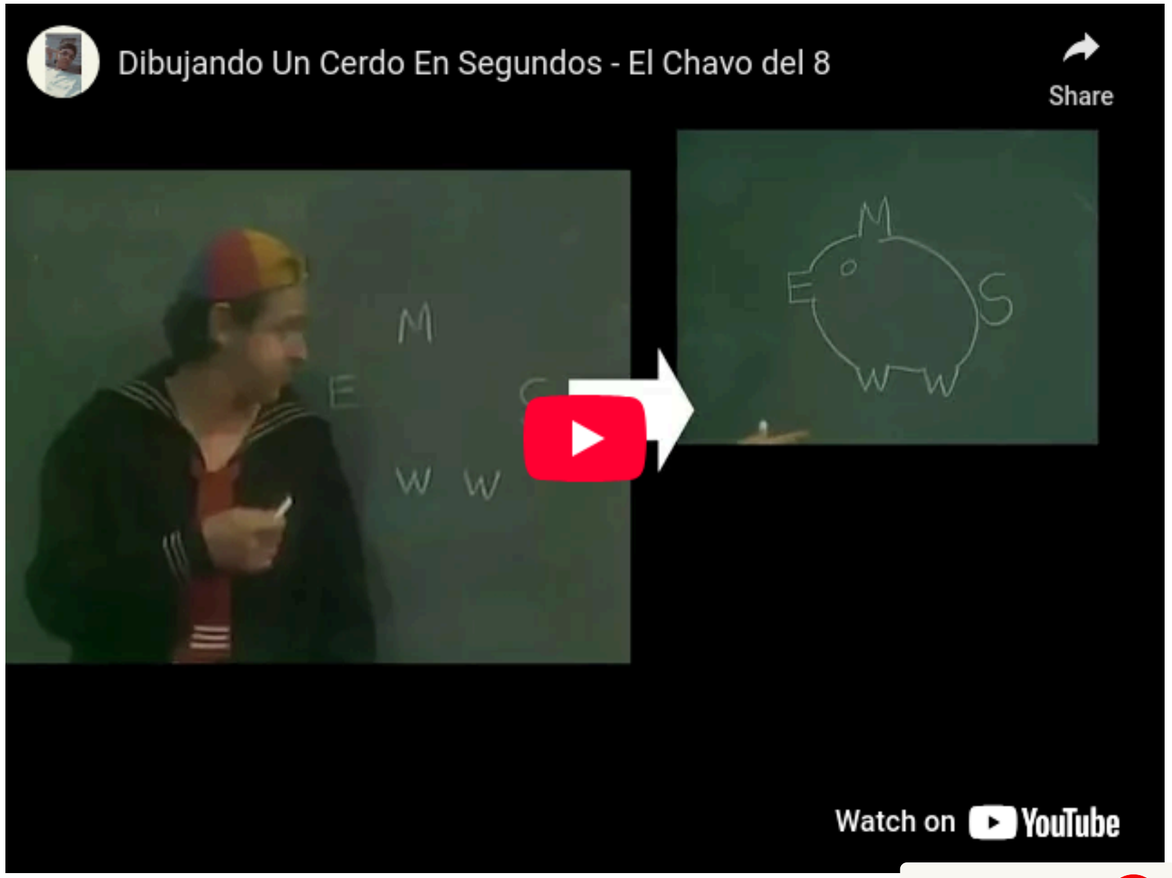
98

¿Qué es el Principio de Responsabilidad Demostrada?

El Principio de Responsabilidad Demostrada requiere que las empresas demuestren con pruebas escritas la implementación de medidas organizativas, técnicas y legales para proteger los Datos Personales y cumplir con la legislación de protección de datos. Esto implica un enfoque proactivo, evidenciando esfuerzos, y estar preparado para rendir cuentas ante la Autoridad de Datos y los Titulares.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA



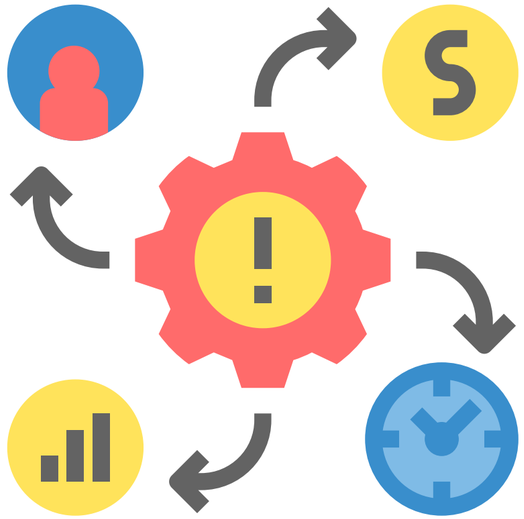
Tap Here

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

99

¿Qué es el Estudio de Impacto de Privacidad (Privacy Impact Assessment)?

Es una evaluación de impacto en la privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés), que tiene como objeto poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.



PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

100

¿Qué debe contener el estudio de Impacto de Privacidad?

Evaluar el proyecto de marketing, mercadotecnia y publicidad implica describir las operaciones de tratamiento de datos personales, analizar los riesgos específicos para los derechos de los titulares de datos y establecer un sistema de gestión de riesgos para demostrar responsabilidad.

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

101

¿Es obligatorio realizar un Estudio de Impacto de Privacidad?

La circular externa No. 003 del 22 de agosto de 2024 lo “sugiere”.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

102

¿Qué es el Sistema de Administración de Riesgos?

Es un sistema desarrollado por el Responsable de tratamiento, acorde con su estructura organizacional, procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases, datos y tipos de datos personales tratados por el Responsable.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

103

¿Qué significan las etapas de identificación, medición, control y monitoreo del Sistema de Administración de Riesgos?

- Medición: Evaluar la probabilidad y el impacto de los riesgos asociados al tratamiento de datos personales.
- Control: Implementar acciones para mitigar los riesgos, analizando su suficiencia, efectividad y oportunidad. Identificar el tipo de control, ya sea manual, automático, discrecional, obligatorio, preventivo o correctivo.
- Monitoreo: Realizar un seguimiento constante para asegurar la efectividad de las medidas establecidas.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

104

¿Qué es la privacidad desde el diseño y por defecto (Privacy by Design and by Default)?

La privacidad desde el diseño y por defecto (Privacy by Design and by Default) es considerada una medida proactiva para cumplir con el Principio de Responsabilidad Demostrada. Al introducir la privacidad desde el diseño se está buscando garantizar el correcto Tratamiento de los datos utilizados en los proyectos de marketing, mercadotecnia y publicidad.

URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

105

En una investigación sobre una aparente violación de los derechos del Titular por parte del Responsable del Tratamiento, ¿se debe verificar que el Responsable ha implementado medidas de responsabilidad demostrada para proteger la información personal?

Las violaciones a la seguridad de las organizaciones representan un alto riesgo para la información y pueden tener impactos graves en la reputación corporativa. Un Programa Integral de Gestión de Datos Personales debe incluir la gestión de riesgos para identificar vulnerabilidades y adoptar medidas que minimicen el impacto tanto para la organización como para los titulares de información.

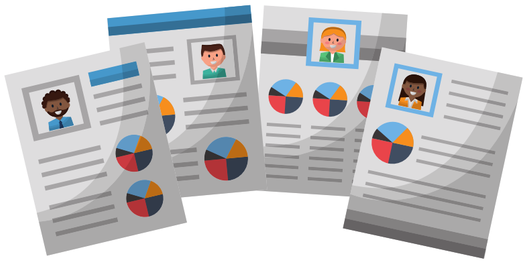
URIBE · YÁÑEZ

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

106

¿El Responsable y Encargado deben capacitar a los empleados que tengan acceso a los Datos Personales? De ser así, ¿cada cuánto deben capacitarlos?

La formación es esencial en un Programa Integral de Gestión de Datos Personales. A pesar de contar con políticas sólidas desde la alta dirección, es crucial capacitar continuamente al personal que maneja datos diariamente. Se requiere formación general para todos y una capacitación específica para aquellos que manejan datos directamente. La actualización periódica del programa es clave para mantener la relevancia de la formación.



PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

107

¿El Encargado puede tratar los Datos Personales de los Titulares sin que el Responsable le demuestre o le permita acceder a las autorizaciones?

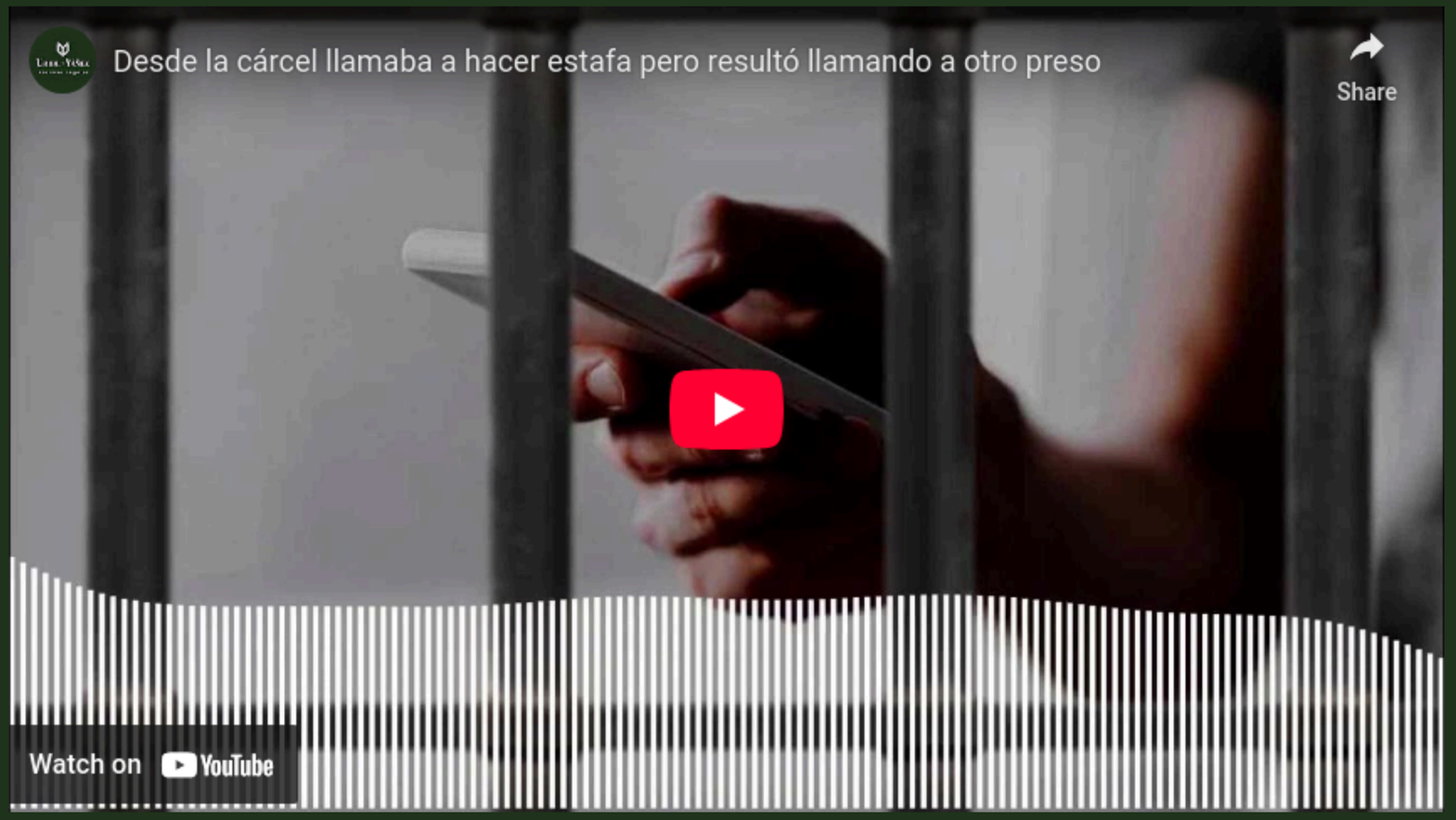
Sí, lo importante es que el Responsable tenga la prueba de la autorización que le otorga el Titular. Sin embargo, en este caso lo que se hace es que el Encargado debe pedir la certificación de que tiene la autorización del Titular al Responsable.

GESTIÓN DE INCIDENTES DE SEGURIDAD

108

¿Qué es un incidente de seguridad?

Es la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales de los Titulares a cargo del Responsable o encargado del Tratamiento.


Desde la cárcel llamaba a hacer estafa pero resultó llamando a otro preso
Share
Watch on YouTube

Tap Here

Tap Here

URIBE · YÁÑEZ

GESTIÓN DE INCIDENTES DE SEGURIDAD

109

¿Cuáles son las causas comunes que generan un incidente de seguridad?

Los incidentes de seguridad pueden generarse por diferentes razones como, entre otras, las siguientes:

- Inexistencia de políticas preventivas de seguridad
- Erroresonegligenciahumana
- Casosfortuitos
- Actosmaliciososocriminales
- Fallasenlossistemasdelaorganización
- Procedimientosdefectuosos
- Deficienciasodefectosenlasoperaciones
- Alteración;destrucción;roboopérdidadearchivosfísicos

GESTIÓN DE INCIDENTES DE SEGURIDAD

110

¿Qué medidas preventivas se deben tomar para hacer frente a un incidente de seguridad?

Medidas preventivas para incidentes de seguridad:

- Entrenamiento regular del personal para responder a incidentes de seguridad, con simulacros preventivos similares a los de incendios o temblores.
- Definir claramente cuándo se trata de un incidente de seguridad que afecta datos personales, ya que no todas las fallas de seguridad implican la confidencialidad, integridad y disponibilidad de información personal.
- Definir las medidas y el procedimiento interno para el manejo de los incidentes de seguridad.

URIBE · YÁÑEZ

GESTIÓN DE INCIDENTES DE SEGURIDAD

111

¿Qué debe hacer el Responsable cuando suceda un incidente de seguridad con los Datos Personales?

La Ley 1581 de 2012, en su artículo 17, establece los deberes de los Responsables del Tratamiento. En particular, el literal n obliga al responsable a informar a la autoridad de protección de datos sobre violaciones a los códigos de seguridad y riesgos en la administración de la información de los titulares.

URIBE · YÁÑEZ

GESTIÓN DE INCIDENTES DE SEGURIDAD

112

Si el Responsable no notifica al Titular por el incidente de seguridad con sus Datos Personales, ¿puede ser sancionado?

La Guía de Incidentes de Seguridad de la SIC destaca la importancia de documentar todos los aspectos de los incidentes de seguridad en los registros internos de las organizaciones. Estos registros no solo son fundamentales para demostrar el cumplimiento del régimen de protección de datos en caso de una investigación, sino que también son útiles para prevenir futuros incidentes en la organización.

GESTIÓN DE INCIDENTES DE SEGURIDAD

113

¿El Encargado debe reportar el incidente de seguridad a la Autoridad de Protección de Datos Personales?

De acuerdo con lo establecido en el literal el literal k. del artículo 18 de la Ley 1581 de 2012, los deberes de los encargados del tratamiento, ha establecido que estos, así como los responsables, *tienen el deber de "Informar a la SIC cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares".*

URIBE · YÁÑEZ

GESTIÓN DE INCIDENTES DE SEGURIDAD

114

¿Qué sucede si no se reportan los incidentes de seguridad a la Autoridad de Protección de Datos Personales?

La SIC puede multar por haber incumplido el deber de reportar, por no tener políticas internas que garanticen la seguridad en el tratamiento de los datos personales y por el incumplimiento del principio de responsabilidad demostrada que se establece en el Decreto 1074 de 2015. Las multas serán hasta por DOS MIL MILLONES DE PESOS (2.000.000.000)

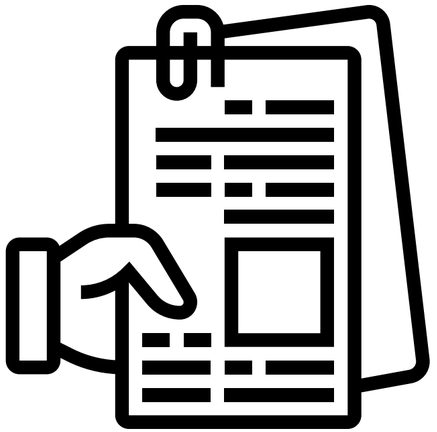
URIBE · YÁÑEZ

GESTIÓN DE INCIDENTES DE SEGURIDAD

115

¿Qué deben contener los registros documentales sobre el incidente de seguridad?

Los registros deben incluir: 1. Descripción del incidente y datos afectados. 2. Categorías de titulares afectados. 3. Fecha y hora del incidente y descubrimiento. 4. Indagaciones e investigaciones internas. 5. Medidas correctivas. 6. Responsables del manejo del incidente. 7. Pruebas del reporte a la SIC y comunicación a titulares si es necesario. 8. Evaluación del riesgo en los titulares y factores considerados. 9. Inclusión de detalles personales según necesidad.

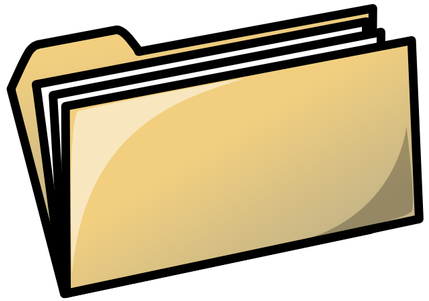


REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

116

¿Qué objeto tiene el Registro Nacional Bases de Datos (RNBD)?

El RNBD es el "directorio público de bases de datos con información personal bajo tratamiento en el país" (SIC, s.f.). Su propósito no es conocer los datos personales ni exponer a los titulares, sino mostrar información general sobre la cantidad de bases de datos, su finalidad, canales de atención a ciudadanos, políticas de tratamiento, tipo de datos y transferencias realizadas.



9 Preguntas frecuentes RNBD. Enlace aquí.

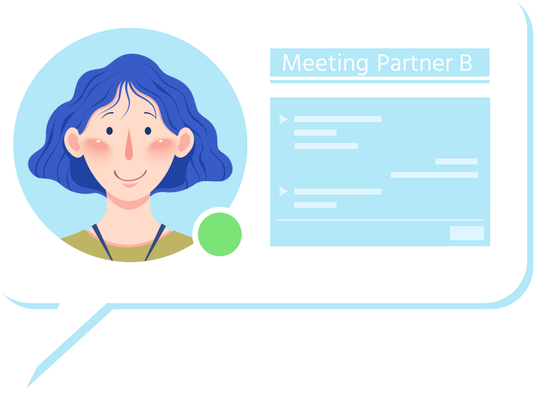
URIBE · YÁÑEZ

REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

117

¿Quiénes están obligados a registrarse en el RNBD?

El Responsable del Tratamiento debe registrar en el RNBD las bases de datos que cumplan con los requisitos establecidos para sociedades y entidades sin ánimo de lucro con activos totales superiores a 100,000 UVT y personas jurídicas de naturaleza pública (Decreto 1074 de 2015, art. 2.2.2.26.1.2.). Además, cualquier Responsable que experimente incidentes de seguridad debe informarlos y registrarse en el RNBD, incluso si no está obligado a hacerlo.



REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

118

¿Con qué periodicidad se debe actualizar el RNBD?

Los reportes deben presentarse según las siguientes fechas:

- Consultas o Reclamos presentados por Titulares: Primeros quince (15) días hábiles de febrero y agosto.
- Incidentes de seguridad: En los quince (15) días hábiles siguientes al suceso.
- Cambios sustanciales en bases de datos registradas: Primeros diez (10) días hábiles de cada mes.

REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

119

En caso de no registrarse o actualizar el RNBD, ¿la entidad que trata los Datos puede ser sancionada?

La Superintendencia de Industria y Comercio puede imponer sanciones a los Responsables y Encargados del Tratamiento que no registren en el RNBD cuando están obligados. Estas sanciones incluyen multas personales e institucionales, hasta el equivalente de dos mil (2,000) salarios mínimos mensuales legales vigentes en el momento de la imposición, siendo posibles multas sucesivas mientras persista el incumplimiento.

10 Extraído de SIC. (s.f.). Preguntas frecuentes RNBD. Enlace aquí.

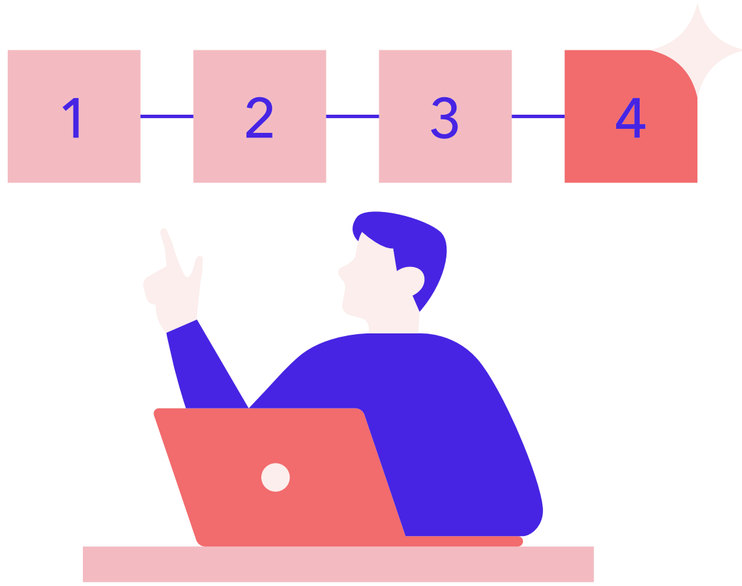
REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

119.a

¿Cómo opera la facultad sancionatoria de la SIC con entidades públicas?

La Superintendencia de Industria y Comercio no puede sancionar a entidades de naturaleza pública. Solo puede impartir órdenes.

Ejemplo: RESOLUCIÓN NÚMERO 14223 DE 2022

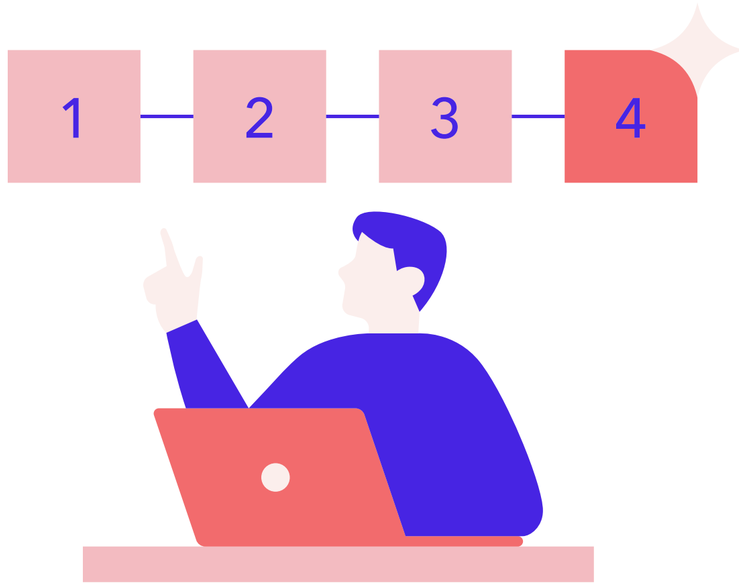


REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

119.b

¿Cuál fue la decisión que tomó la SIC en el caso del Huila frente al RNBD?

El Departamento del Huila registró sus bases de datos en el RNBD, sin embargo, afirmó no haber implementado ninguna medida de seguridad en ellas. Teniendo en cuenta que la SIC no tiene competencia para sancionar al Departamento, emitió varias órdenes en su rol de autoridad nacional de protección de datos personales a fin de garantizar los principios de seguridad consagrados en la Ley 1581 de 2012.



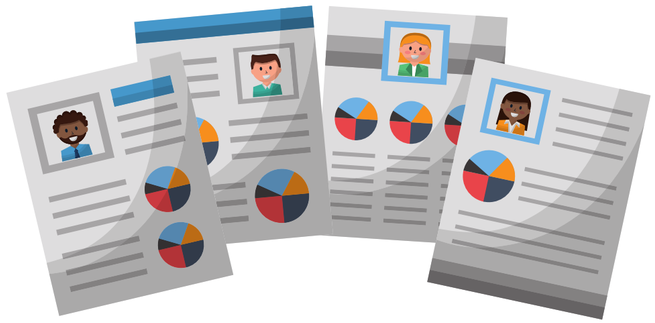
URIBE · YÁÑEZ

REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

120

Suponiendo que el Encargado cumple con los requisitos patrimoniales para verse en la obligación de registrarse en el RNBD, ¿este debe hacerlo?

El Encargado no debe reportar y/o actualizar las bases de Datos Personales de su Responsable. Por el contrario, el Encargado, en caso de estar en la obligación de inscribirse en el RNBD, deberá inscribir las bases de datos que él administre a título de Responsable.

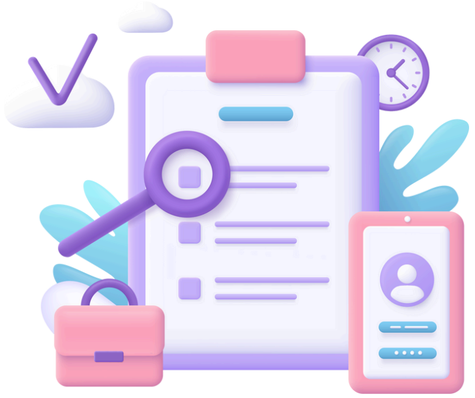


NORMAS CORPORATIVAS VINCULANTES

121

¿Qué son las Normas Corporativas Vinculantes (NCV)?

El Decreto 255 de 2022 define las Normas Corporativas Vinculantes como las políticas de cumplimiento obligatorio adoptadas por el responsable del tratamiento de datos en Colombia. Estas normas se aplican para transferencias de datos personales a un responsable fuera del país que forme parte del mismo grupo empresarial.



NORMAS CORPORATIVAS VINCULANTES

122

¿Quién debe implementar las Normas Corporativas Vinculantes?

Los grupos empresariales deberán aplicarlo en sus transferencias a Responsables ubicados fuera del territorio colombiano, de acuerdo con el art. 2.2.2.25.7.2 del Decreto 255 de 2022.

NORMAS CORPORATIVAS VINCULANTES

123

¿Qué entidad aprueba las Normas Corporativas Vinculantes?

La Superintendencia de Industria y Comercio aprobará las Normas Corporativas Vinculantes (Decreto 255 de 2022, art. 2.2.2.25.7.7.).

URIBE · YÁÑEZ

NORMAS CORPORATIVAS VINCULANTES

124

¿Las NCV permiten la Transferencia de Datos Personales a entidades que se encuentren fuera del grupo empresarial?

No. Las Normas Corporativas Vinculantes tienen, por objeto, la regulación de Transferencias de Datos Personales entre Responsables de un mismo grupo empresarial que se encuentren fuera del territorio colombiano. Sin embargo, las Transferencias y/o Transmisiones a Responsables y Encargados que estén fuera del grupo empresarial se regirán bajo las reglas establecidas en el art. 26 de la Ley 1581 de 2012 y la declaración de conformidad de la SIC.

URIBE · YÁÑEZ

SANCIONES POR INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE DATOS

125

¿Por qué motivos puede ser sancionado un Responsable o Encargado?

El Responsable o Encargado puede ser sancionado por diversas razones, como incumplimiento de deberes, tratamiento sin autorización, transferencia insegura de datos, falta de políticas y documentos esenciales, y uso indebido de datos.

URIBE · YÁÑEZ

SANCIONES POR INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE DATOS

126

¿De qué manera, usualmente, inician las investigaciones a los Responsables por violación del Régimen General de Datos?

Las quejas suelen surgir cuando no se responde a las PQRS. Cuando los Titulares agotan recursos con el Responsable o Encargado sin solución, recurren a la SIC, que investiga todas las prácticas de Tratamiento de Datos Personales. Por esta falta de respuesta, sancionan a los Responsables/Encargados, como en el caso de Stark GYM S.A.S. – Resolución 83874 de 2021.

URIBE · YÁÑEZ

SANCIONES POR INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE DATOS

127

Si el Encargado viola los derecho del Titular, ¿el Responsable es el único sancionado o el Encargado o ambos son penalizados?

Al amparo del art. 23 de la Ley 1581 de 2012, "la Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento".

URIBE · YÁÑEZ

SANCIONES POR INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE DATOS

128

¿Qué sanciones puede imponer la SIC por incumplimiento del régimen de datos personales?

La Superintendencia de Industria y Comercio puede imponer sanciones, como multas hasta el equivalente de dos mil salarios mínimos mensuales, suspensión de actividades por hasta seis meses con indicación de correctivos, cierre temporal tras la suspensión sin correctivos, y cierre inmediato y definitivo en casos de tratamiento de datos sensibles.

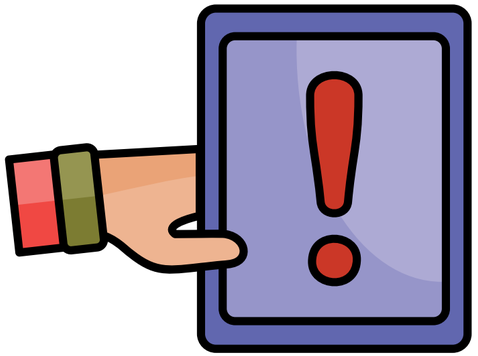
URIBE · YÁÑEZ

SANCIONES POR INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE DATOS

129

¿Qué sanciones puede imponer la SIC por incumplimiento del régimen de datos personales a entidades públicas?

Según el parágrafo del artículo 23 de la ley 1581 de 2012, en el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.



URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

130

¿Qué es un dato semiprivado?

De acuerdo con el literal g de la Ley 1266 de 2008, el dato semiprivado es aquel que “no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general”.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

131

¿Qué diferencia sustancial existe entre el Régimen de habeas data y habeas data financiero?

Régimen General de Datos (Habeas *Data)*	Régimen de Habeas Data Financiero
Aplica únicamente para personas naturales.	Aplica para personas naturales y jurídicas.
Regula, especialmente, los Datos Personales privados, públicos, sensibles, de menores de edad y datos biométricos.	Regula, especialmente, los datos semiprivados.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

132

¿Qué es la Fuente de información?

La Fuente es quien proporciona o conoce Datos Personales debido a una relación con el Titular. Con autorización del Titular o por ley, la Fuente entrega los datos al Operador, quien los transfiere al usuario final. Si la Fuente entrega directamente al usuario final sin pasar por un Operador, asume las responsabilidades de Fuente y Operador, siendo responsable de la calidad y protección de los datos.

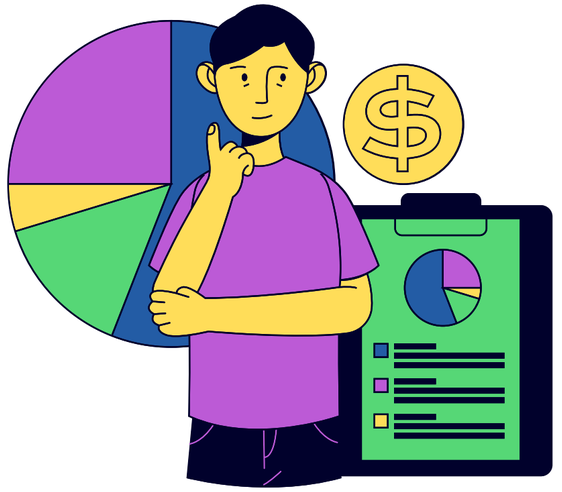
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

133

¿Qué es el Operador de la información?

El Operador no tiene ningún tipo de relación contractual, legal o comercial con el Titular, salvo que el Operador sea la misma Fuente de Información. En virtud de ello, no es responsable por la calidad de la información que le transmite la Fuente.

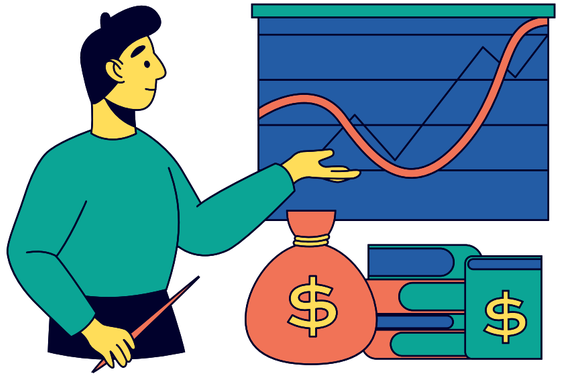


HABEAS DATA FINANCIERO

134

¿Qué es el Usuario?

Toda persona natura o jurídica que accede a los Datos Personales a través del Operador, la Fuente o directamente del Titular con el objeto de analizar información financiera, crediticia, etc., de interés para el posible acuerdo comercial o de servicios que desee celebrar con el Titular.



URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

135

¿El Titular puede ser reportado ante una central de riesgo sin que haya otorgado su autorización?

Siempre se deberá contar con la autorización del Titular para que la Fuente pueda suministrar los Datos Personales al Operador y/o Usuario.
Los Titulares podrán solicitar prueba de la autorización a la Fuente, Operador o Usuario para considerarse legítimo el Tratamiento (Art. 6, numerales 1.3, 2.3 y 3.2, Ley 1266 de 2008).

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

136

Respecto a la circulación de la información del Operador, ¿Quiénes pueden tener acceso a los datos del Titular?

El Operador puede compartir Datos Personales con Titulares, personas autorizadas, causahabientes, usuarios de la información, entidades públicas, órganos de control, otros Operadores con autorización y cualquier persona autorizada por la ley.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

137

¿Qué derechos posee el Titular respecto al Operador, la Fuente de información y los Usuarios?

Frente al Operador, el Titular puede: A. Ejercer su derecho de habeas data mediante consultas y reclamos. B. Solicitar respeto y protección de sus derechos a través de reclamos y peticiones. C. Pedir prueba de la certificación de la autorización de la Fuente o el Usuario. D. Solicitar información sobre los Usuarios autorizados para acceder a la información.

Frente a la Fuente de la Información, el Titular puede: A. Ejercer su derecho de habeas data y petición mediante consultas y reclamos. B. Conocer, actualizar o rectificar su información, gestionando cambios a través del operador.

Frente a los Usuarios, los Titulares pueden: A. Solicitar información sobre cómo se trata su información, si no fue suministrada por el operador. B. Pedir prueba de la autorización. Para Titulares de información crediticia y/o financiera, se añaden los derechos de: A. Presentar quejas ante la autoridad de vigilancia por violación de normas sobre administración de información financiera y crediticia. B. Solicitar a la autoridad de vigilancia la corrección o actualización de sus datos personales cuando sea procedente según la ley.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

138

¿El Operador o Fuente de información puede cobrarle al Titular por consultar su historial crediticio?

Su información personal contenida en las centrales de riesgo puede ser consultada gratuitamente una (1) vez al mes por usted, razón por la cual los operadores de la información solo pueden cobrarle por el acceso a la historia de crédito a partir de la segunda consulta en el mes.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

139

Si el Titular desea revocar la autorización para el Tratamiento de sus Datos Personales, no obstante, aún media una obligación dineraria que se encuentra en mora, ¿el Operador o la Fuente de información debe suprimirla información del Titular?

Según el Artículo 2.2.2.25.2.6 del decreto 1074 La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

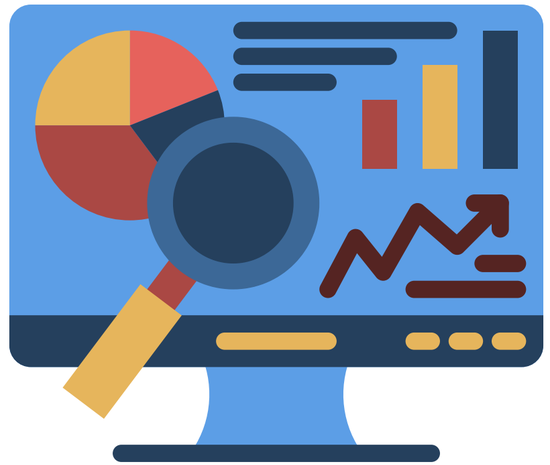
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

140

¿Qué es un dato positivo?

Toda aquella información relacionada con el cumplimiento y pago oportuno de las obligaciones dinerarias, como buenos hábitos de pago.



URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

141

¿El Titular puede solicitar la supresión de un dato positivo?

Sí, toda vez que tiene derecho a suprimir la información.

HABEAS DATA FINANCIERO

142

¿Qué es un dato negativo?

Toda aquella información que se relacione con el incumplimiento de obligaciones y/o la constitución en mora por no pago de obligaciones dinerarias.

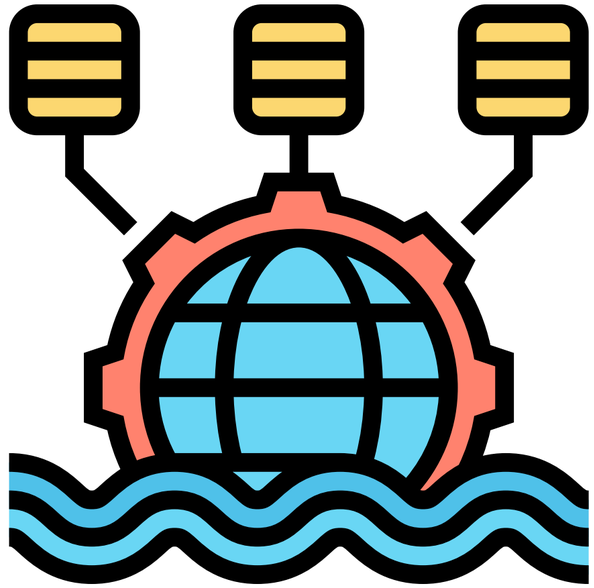
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

143

¿Se debe informar previamente al Titular cuando se reporte un dato negativo al Operador o Fuente de información?

Según lo establece el artículo 2.2.2.28.2 del decreto 1074 el reporte de información negativa sobre incumplimiento de obligaciones sólo procederá previa comunicación al titular de la información, la cuál podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes, siempre y cuando se incluya de manera clara y legible.



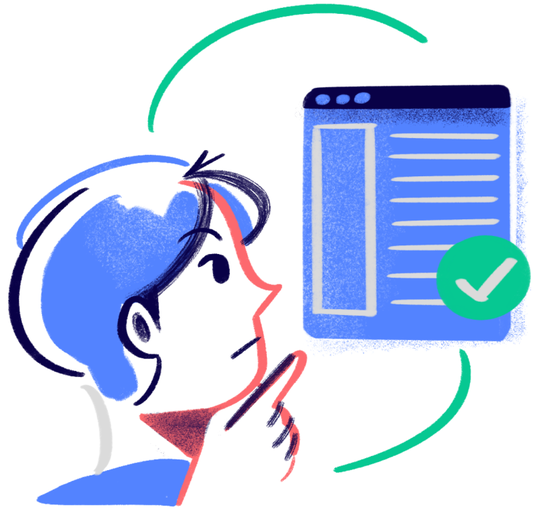
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

144

¿Qué término máximo de permanencia, en los bancos de datos, se dispone para los datos positivos?

Según lo establecido en el artículo 13 de la ley 1266 de 2008 La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información.



URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

145

¿Qué término máximo de permanencia, en los bancos de datos, se dispone para los datos negativos?

Según el artículo 13 de la Ley 1266 de 2008, la información sobre mora tiene un plazo máximo de permanencia de cuatro (4) años, contados desde el pago de las cuotas vencidas o la extinción de la obligación. Los datos negativos y aquellos relacionados con la mora, tipo de cobro y estado de la cartera caducan después de ocho (8) años desde el inicio de la mora y deben ser eliminados de la base de datos.

HABEAS DATA FINANCIERO

146

Si ya transcurrió el término para que el Operador o la Fuente de información eliminaran el dato negativo, sin embargo, esto no ha sucedido. En caso de que el Titular realice la solicitud de supresión del dato negativo, ¿cuál es el plazo para que el Operador elimine la información inexacta?

Deberá ser eliminada inmediatamente.

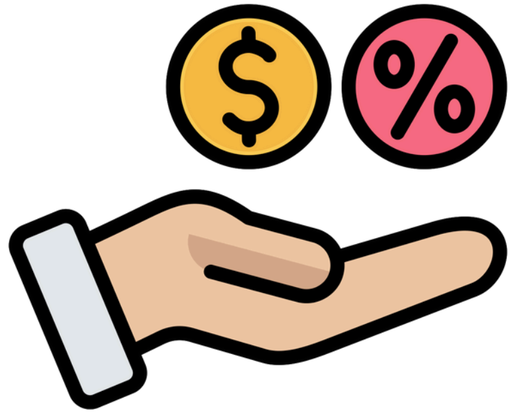
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

147

Si la deuda en mora de un Titular permanece impagada indefinidamente, ¿el dato negativo podrá durar, de igual manera, indefinidamente hasta que se extinga la obligación?

Los datos negativos relacionados con mora, tipo de cobro y estado de la cartera caducarán y deben ser eliminados de la base de datos después de ocho (8) años desde el inicio de la mora en la obligación.



URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

148

Cuando se retira el dato negativo del banco de datos, ¿se puede mantener un score, récord o calificación negativa sobre el titular en la plataforma?

Toda información negativa o desfavorable que se encuentre en bases de datos y se relacione con calificaciones, récord (scorings-score), o cualquier tipo de medición financiera, comercial o crediticia, deberá ser actualizada de manera simultánea con el retiro del dato negativo o con la cesación del hecho que generó la disminución de la medición.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

149

Si se elimina el dato negativo del banco de datos, ¿se extingue la obligación del Titular?

No, se elimina la información según mandato de la ley, sin embargo la obligación del titular sigue vigente.

HABEAS DATA FINANCIERO

150

Si el deudor principal no realiza el pago de la obligación, ¿el Usuario puede reportar al codeudor, fiador, deudor solidario, etc., ante las Fuentes de información o el Operador?

Sí, siempre y cuando haya obtenido autorización del titular de la información para realizar dicho reporte.

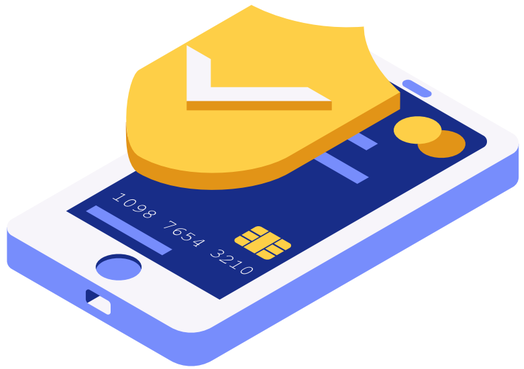
URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

151

¿Con qué finalidades puede acceder el Usuario a la información contenida en los bancos de datos?

Se puede utilizar la información con fines de análisis para establecer y mantener relaciones contractuales, evaluación de riesgos en relaciones contractuales, estudios de mercado o investigaciones comerciales, estadísticas, trámites ante autoridades públicas o privadas, y cualquier otra finalidad autorizada por el titular de la información.

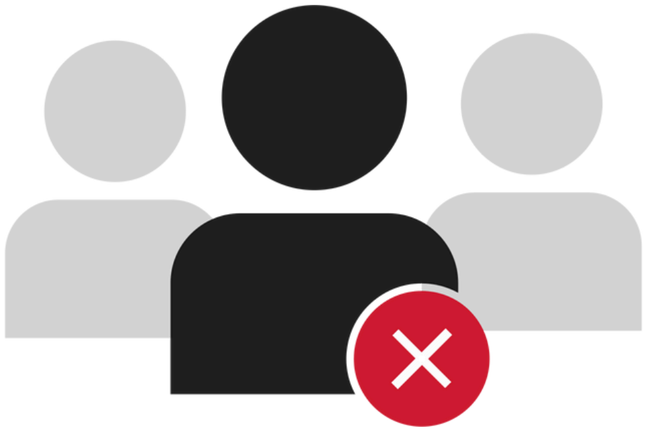


HABEAS DATA FINANCIERO

152

¿Qué es el “blacklisting” o listas negras?

Son una serie de listas que contienen el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos con fines maliciosos o malévolos.



HABEAS DATA FINANCIERO

153

En Colombia, ¿está permitido realizar listas negras sobre usuarios y/o consumidores con baja reputación crediticia?

No, en un primer momento se establece en la ley 1266 que se prohíbe la administración de datos personales con información exclusivamente desfavorable. (Sentencia T-987 de 2012 que estableció la corte.)

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

154

¿De qué se trata el caso de “Lista de viajeros no conformes” y cómo violó el principio de administración de los Datos Personales?

Una aerolínea del sector aéreo creó una lista de viajeros no conformes con el objetivo de negarles el acceso al servicio de aerolíneas. La lista incluía datos personales de personas involucradas en altercados con empleados, independientemente de la naturaleza de la controversia. La Corte Constitucional consideró esta práctica como abusiva y contraria a la finalidad legítima de la administración de datos personales. La creación de "listas negras" se considera una práctica que impone barreras injustificadas para el acceso al mercado comercial y financiero.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

155

En caso de que el Titular desee presentar un reclamo sobre sus datos semiprivados, ¿lo debe presentar al Operador, a la Fuente de Información o al Usuario?

El Artículo 16 de la Ley 1266 permite a los titulares y sus causahabientes consultar su información personal en cualquier banco de datos, ya sea público o privado. El operador debe proporcionar toda la información relacionada con la identificación del titular a aquellos debidamente identificados. Además, pueden presentar reclamos a la fuente de la información en caso de errores o necesidad de actualización.

HABEAS DATA FINANCIERO

156

Si el Titular presenta una consulta, queja o reclamo a un Operador o Fuente de información, pero no hay la debida respuesta, ¿puede proteger sus derechos como Titular a través de la tutela?

Sí, en todo caso tras haber agotado los requisitos de procedibilidad el titular tendrá derecho a interponer acción de tutela como mecanismo de protección constitucional a su derecho fundamental de habeas data que está siendo vulnerado.

HABEAS DATA FINANCIERO

157

¿De qué forma deben corroborar las entidades financieras la identidad del Titular de forma que no se suplante su identidad?

Las entidades financieras deben adoptar mecanismos eficaces para verificar la identidad del titular de los datos y prevenir suplantaciones. Aunque la norma no especifica un método concreto, se requiere la implementación de herramientas adecuadas que cumplan con los principios de seguridad y responsabilidad demostrada.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

158

En caso de que el Titular sufra el delito de falsedad personal en una obligación financiera que no ha adquirido, ¿podrá solicitar la modificación o remoción del dato negativo?

Según el artículo 16 de la Ley 1266, si un titular de información alega ser víctima del delito de falsedad personal y se le exige el pago de obligaciones como resultado de dicha conducta, debe presentar una petición de corrección a la fuente adjuntando los documentos de respaldo. La fuente, en un plazo de diez (10) días, deberá cotejar los documentos utilizados para adquirir la obligación con los presentados por el titular. Si encuentra evidencia de falsedad, la fuente puede optar por denunciar el delito de estafa.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

159

En caso de que una petición o reclamo no sea atendida en el plazo establecido por ley, ¿el Operador o Fuente de información deberá aceptar lo solicitado en la petición?

Según lo establecido en el numeral 8 del título II del artículo 16 de la ley 1266 de 2008: las peticiones o reclamos deberán resolverse dentro de los quince (15) días hábiles siguientes a la fecha de su recibo. Prorrogables por ocho (8) días hábiles más, según lo indicado en el numeral 3, parte II, artículo 16 de la presente ley. Si en ese lapso no se ha dado pronta resolución, se entenderá, para todos los efectos legales, que la respectiva solicitud ha sido aceptada.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

160

¿Qué entidades tienen la facultad sancionatoria en caso de que una entidad incumpla el Régimen de Habeas Data financiero?

Según el artículo 17 de la Ley 1266 de 2008, la Superintendencia de Industria y Comercio generalmente tiene la función de vigilancia y sanción. Sin embargo, la Superintendencia Financiera de Colombia tiene la autoridad para investigar y sancionar a fuentes, usuarios y operadores de la información bajo su supervisión. Además, la Superintendencia Financiera puede imponer sanciones cuando un usuario niega un crédito basándose únicamente en informes de datos negativos del solicitante, según el Artículo 10, párrafo 1° de la Ley 1266 de 2008.

URIBE · YÁÑEZ

HABEAS DATA FINANCIERO

160.a

¿Qué es el portal “SIC FACILITA”?

SICFACILITA es una herramienta gratuita de resolución de conflictos, en donde la SIC actúa como facilitadora entre las partes.

Actualmente en SICFACILITA los consumidores pueden acudir para facilitar soluciones en temas de:

- Garantías de productos o servicios.
- Servicios de telecomunicaciones (internet, telefonía y televisión).
- **Suplantación de identidad.**
- **Reportes a centrales de riesgo.**

HABEAS DATA FINANCIERO

161

Las entidades vigiladas por la Superintendencia Financiera, ¿pueden comercializar la información financiera del Titular?

Según el Decreto 1297 de 2022, las entidades supervisadas por la Superintendencia Financiera pueden comercializar el uso, almacenamiento y circulación de Datos Personales con la autorización del Titular. No obstante, esta medida no afecta la obligación de mantener la "reserva bancaria" sobre los consumidores financieros, por lo que se deben seguir aplicando principios como el acceso y circulación restringida o de confidencialidad.


Dejen dormir al projimo | Los Simpsons
Copy link
Watch on YouTube

Tap Here

URIBE · YÁÑEZ

LEY 2300 DE 2023 “DEJEN DE FREGAR”

162

¿Cuál es el objeto de la Ley 2300 de 2023?

Artículo 1. Objeto.

La presente ley tiene por objeto proteger el derecho a la intimidad de los consumidores, estableciendo los canales, el horario y la periodicidad en la que estos pueden ser contactados por las entidades vigiladas por la Superintendencia Financiera y todas las personas naturales y jurídicas que adelanten gestiones de cobranzas de forma directa, por medio de terceros o por cesión de la obligación.

URIBE · YÁÑEZ

LEY 2300 DE 2023 “DEJEN DE FREGAR”

163

¿A quién aplica la Ley 2300 de 2023?

Artículo 1. Objeto. Parágrafo:

Las disposiciones aquí señaladas serán aplicadas por todas las personas naturales y jurídicas que adelanten gestiones de cobranza de forma directa, por tercerización o por cesión de la obligación financiera o crediticia

URIBE · YÁÑEZ

LEY 2300 DE 2023 “DEJEN DE FREGAR”

164

¿Qué canales de comunicación autoriza la Ley 2300 de 2023?

Artículo 2. Canales autorizados.

Las entidades vigiladas por la Superintendencia Financiera y todas las personas naturales y jurídicas que ejerzan actividades de cobranza sólo podrán contactar a los consumidores mediante los canales que estos autoricen para tal efecto, los cuales deberán ser informados y socializados previamente por parte de las entidades de cobranza con el fin de que los consumidores elijan cuáles autoriza.

URIBE · YÁÑEZ

LEY 2300 DE 2023 “DEJEN DE FREGAR”

165

¿Qué horarios y periodicidad establece la Ley 2300 de 2023?

Artículo 3. Horarios y periodicidad.

Una vez establecido un contacto directo con el consumidor, este no podrá ser contactado por parte de gestores de cobranza mediante varios canales dentro de una misma semana ni en más de una ocasión durante el mismo día.

Las prácticas de cobranza deberán realizarse de manera respetuosa y sin afectar la intimidad personal ni familiar del consumidor, dentro del horario de lunes a viernes y de 7:00 am a 7:00 pm, y sábados de 8:00 am a 3:00 pm, excluyendo cualquier tipo de contacto con el consumidor los domingos y días festivos.

LEY 2300 DE 2023 “DEJEN DE FREGAR”

166

Respecto de los deudores solidarios o codeudores, ¿qué establece la Ley 2300 de 2023?

Artículo 4.

En ningún caso, las entidades vigiladas por la Superintendencia Financiera y todas las entidades que adelanten gestiones de cobranza de forma directa, por medio de terceros o por cesión de la obligación incluyendo a las personas naturales; podrán contactar a las referencias personales o de otra índole. Al avalista, codeudor o deudor solidario se le contactará en le misma condición que establece la presente ley.

URIBE · YÁÑEZ

LEY 2300 DE 2023 “DEJEN DE FREGAR”

167

¿Esta Ley aplica para mensajes de texto (SMS)?

Artículo 5.

Lo dispuesto en la presente ley se aplicará en los mismos términos a las relaciones comerciales entre los productores y proveedores de bienes y servicios privados o públicos y el consumidor comercial frente al envío de mensajes publicitarios a través de menajes cortos de texto (SMS), mensajería por aplicaciones web, correos electrónicos y llamadas telefónicas de carácter comercial o publicitario.

URIBE · YÁÑEZ

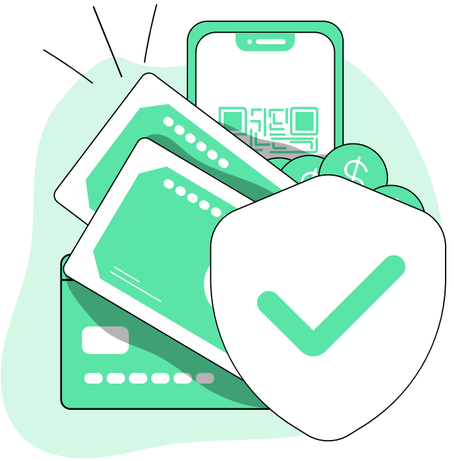
LEY 2300 DE 2023 “DEJEN DE FREGAR”

168

¿Qué establece la Ley sobre las visitas de cobranza a domicilio?

Artículo 6.

Las personas naturales y jurídicas se abstendrán de adelantar gestiones de cobranza mediante visitas al domicilio o lugar de trabajo del consumidor financiero o de servicios.



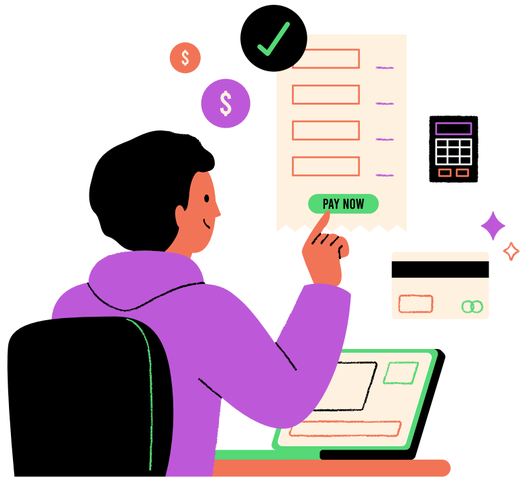
LEY 2300 DE 2023 “DEJEN DE FREGAR”

169

¿Puede consultarse al consumidor los motivos del incumplimiento?

Artículo 7.

Las entidades que adelanten gestiones de cobranza deberán abstenerse de consultar al consumidor financiero el motivo del incumplimiento de la obligación.



LEY 2300 DE 2023 “DEJEN DE FREGAR”

170

¿Qué excepción establece la Ley 2300 de 2023?

Artículo 8.

Se exceptúan de las medidas anteriores los contactos que tengan como finalidad informar al consumidor sobre confirmación oportuna de las operaciones monetarias realizadas, sobre ahorros voluntarios y cesantías, enviar información solicitada por el consumidor o generar alertas sobre transacciones fraudulentos, inusuales o sospechosas.

URIBE · YÁÑEZ

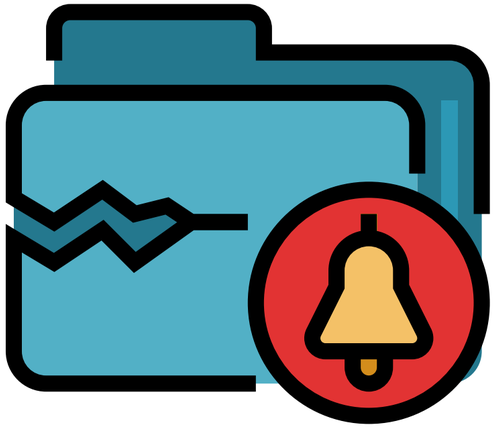
LEY 2300 DE 2023 “DEJEN DE FREGAR”

171

¿Qué pasa si se incumplen las medidas establecidas en la Ley?

Artículo 9.

El incumplimiento de las medidas de protección de que trata la presente ley, se sancionará por la Superintendencia Financiera de Colombia y la Superintendencia de Industria y Comercio, de acuerdo con el marco de competencias previsto en la Ley Estatutaria 1266 de 2008 o las normas que lo modifiquen, adicionen o sustituyan.



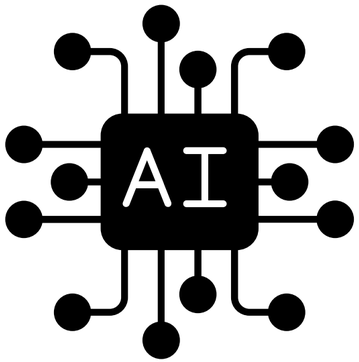
URIBE · YÁÑEZ

INTELIGENCIA ARTIFICIAL

172

¿Qué es la Inteligencia Artificial?

El CONPES 39754 define la inteligencia artificial como "(...) un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos".



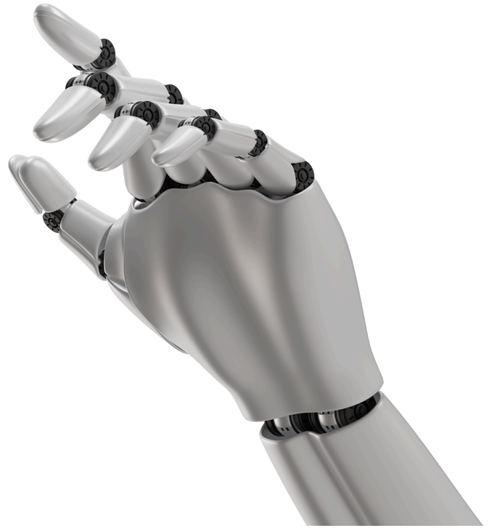
URIBE · YÁÑEZ

INTELIGENCIA ARTIFICIAL

173

¿A los datos tratandos por IA les aplica el régimen de datos personales?

Sí. El tratamiento de datos personales que se realice mediante uso de inteligencias artificiales debe ajustarse a lo dispuesto en la Ley 1581 de 2015, Ley 1266 de 2008 y decretos reglamentarios. Adicionalmente, los administradores de datos personales que manejen inteligencia artificial para el manejo de datos personales deben ejecutar las medidas necesarias a fin de garantizar la seguridad de la información de conformidad con el principio de responsabilidad demostrada.



Sentencia T-323 del 2024 Corte Constitucional

URIBE · YÁÑEZ

INTELIGENCIA ARTIFICIAL

174

¿Cuáles son las instrucciones de la SIC en el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial?

1. Ponderación de los siguientes criterios: idoneidad, necesidad, razonabilidad, proporcionalidad.
2. Ante la duda de los posibles riesgos asociados el administrador deberá abstenerse o adoptar medidas precautorias o preventivas para proteger los derechos del Titular del dato, su dignidad y otros derechos humanos.
3. Estudio y clasificación de riesgos, los administradores deberán adecuar sistemas de administración de riesgos asociados al Tratamiento de aquella información.
4. Antes del desarrollo de la IA se deberá documentar un estudio de impacto de privacidad.
5. Veracidad e integridad de los datos tratados a través de IA.

URIBE · YÁÑEZ

INTELIGENCIA ARTIFICIAL

174

¿Cuáles son las instrucciones de la SIC en el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial?

6. Medidas de privacidad desde el disefio y por defecto por medio de técnicas matemáticas.
7. Garantía de información al Titular sobre el tratamiento de datos realizado por la IA.
8. Cumplir el principio de seguridad, en el desarrollo y despliegue de la IA, se requiere adoptar medidas tecnológicas", humanas, administrativas, físicas, contractuales y de cualquier otra índole.
9. El tratamiento de datos privados, semiprivados o sensibles recolectados por internet se hará conforme el principio de finalidad.
10. El tratamiento mediante IA deberá garantizar los derechos de los Titulares de la información establecidos en las leyes estatutarias 1266 de 2008 y 1581 de 2012 y sus decretos reglamentarios".

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

175

¿Qué otros regímenes protegen la información?

Existen disposiciones sobre el manejo de información y protección de la misma en el régimen de propiedad industrial, laboral, penal, de derecho de la competencia, entre otros.

URIBE · YÁÑEZ

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

176

¿Qué es la propiedad intelectual?

La propiedad intelectual (PI) se relaciona con las creaciones de la mente, como las invenciones, las obras literarias y artísticas, y los símbolos, nombres e imágenes utilizados en el comercio.

La PI está protegida por la legislación, por ejemplo, en el ámbito de las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de PI procura fomentar un entorno propicio para que prosperen la creatividad y la innovación.

URIBE · YÁÑEZ

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

177

¿Qué información se protege como propiedad industrial?

La propiedad industrial otorga derechos exclusivos a los titulares de las creaciones, lo que les permite decidir quién y cómo se pueden usar.
Algunos ejemplos de lo que protege la propiedad industrial son:

- **Patentes:** Protegen invenciones, como procedimientos, aparatos o productos nuevos, o mejoras de los mismos.
- **Marcas:** Protegen signos distintivos, como nombres comerciales o combinaciones gráficas, que identifican productos o servicios.
- **Diseños industriales:** Protegen la apariencia externa de los productos, ya sea en dos o tres dimensiones.

178

¿QUÉ INFORMACIÓN SE PROTEGE COMO SECRETO EMPRESARIAL?

Art. 260 Decisión 486: Cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida que dicha información:

- Sea secreta.
- Tenga valor comercial por ser secreta.
- Sea objeto de medidas razonables destinadas a mantenerla secreta.

URIBE · YÁÑEZ

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

179

¿Qué son los derechos de autor?

Es el derecho que reconoce de manera adecuada y efectiva la protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino. Los criterios que se evalúan son:

- Originalidad
- Protección a la forma y no a las ideas
- Ausencia de formalidades
- Indistinción del mérito y la destinación de la obra
- Soporte material

Guía del derecho de autor para creadores y usuarios, Dirección Nacional de Derecho de Autor.

URIBE · YÁÑEZ

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

180

¿Cuál es la diferencia entre los derechos de autor y la propiedad industrial?

	Derecho de Autor	Propiedad Industrial	Derechos de Obtentor
Objeto de protección	Obras literarias, artísticas y científicas	Signos distintivos y nuevas creaciones	Nuevas variedades vegetales homogéneas, distinguibles y estables.
Sujeto que obtiene la protección	Autor	Titular o inventor	Obtentor
Forma en que se da la protección	Automática	A través del registro	A través del registro
Entidad encargada en Colombia	Dirección Nacional de Derecho de Autor	Superintendencia de Industria y Comercio	Instituto Colombiano Agropecuario

Guía del derecho de autor para creadores y usuarios, Dirección Nacional de Derecho de Autor.

URIBE · YÁÑEZ

OTRAS FORMAS DE PROTEGER LA INFORMACIÓN

181

¿Cómo se protege la información desde el punto de vista contractual?

- Cláusula de confidencialidad.
- NDA.
- Cláusula penal en caso de incumplimiento.
- Obligación de tener estándares de seguridad.

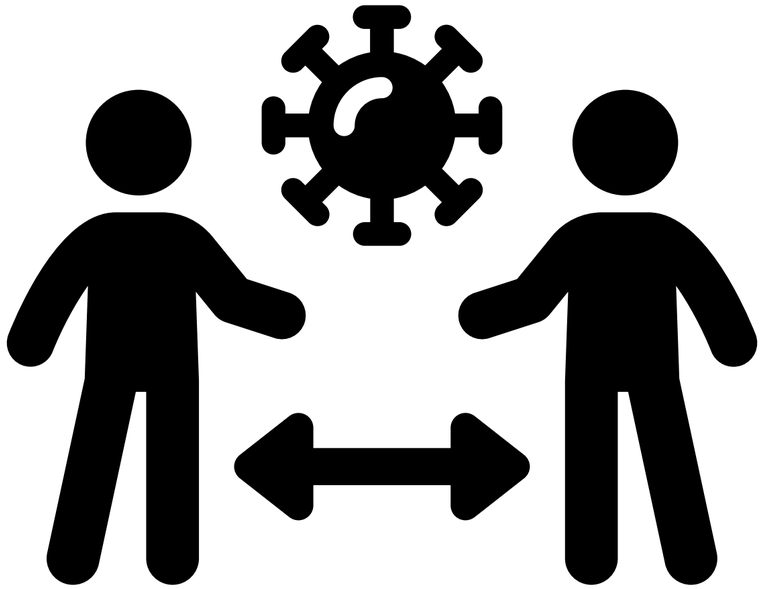
¿EN QUÉ CONTRATOS O RELACIONES HAY ENTREGA DE INFORMACIÓN?

- Servicios TICs.
- Servicios de nube .
- Desarrollo de software.
- Bases de datos.
- Maquilas.
- Concursos.
- Empleados.
- Administradores.
- Miembros de junta.
- M&A.

183

¿Qué es un subencargado del tratamiento de datos?

Un subencargado del tratamiento es una persona o entidad que procesa datos personales en nombre de un encargado del tratamiento.



URIBE · YÁÑEZ

184

¿Qué medidas debe tomar un encargado con su subencargado para garantizar la seguridad de la información?

- Debe contar con autorización del responsable para transmitir al subencargado.
- Auditorías y seguimiento de medidas de seguridad de la información.
- Inclusión de cláusulas de transmisión.
- Inclusión de cláusulas de disposición de información una vez terminado el contrato.

URIBE · YÁÑEZ

185

¿Cuáles son las obligaciones del subencargado?

- Cumplir con las disposiciones contempladas en la Ley 1581 del 2012, sus decretos reglamentarios y las instrucciones impartidas por la Superintendencia de Industria y Comercio.
- Cumplir con las obligaciones derivadas del contrato de transmisión celebrado con el encargado de tratamiento de datos.

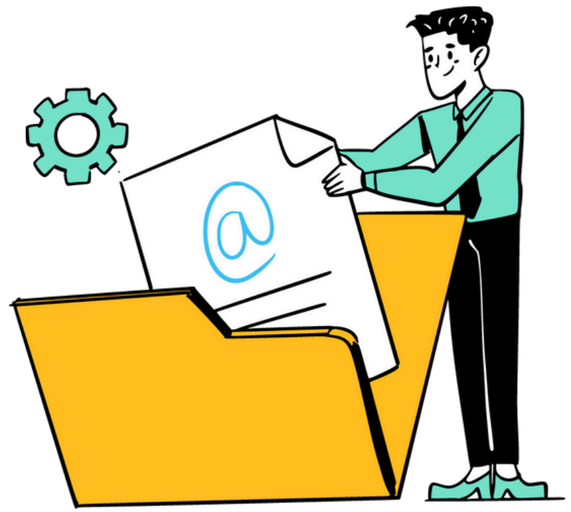
URIBE · YÁÑEZ

OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

186

¿Qué son las tablas de retención documental y para qué sirven?

Las Tablas de Retención Documental (TRD) son un instrumento que clasifica los documentos de una entidad o empresa y establece cuánto tiempo deben conservarse. También indican qué hacer con ellos una vez que ya no sean útiles.

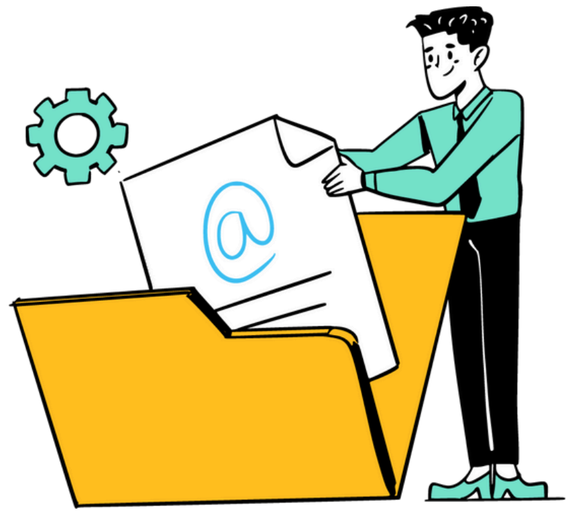


OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

187

¿Por cuánto tiempo es necesario retener o conservar la información documental?

Dependiendo del tipo de información, existen disposiciones que determinan el tiempo que debe almacenarse.



URIBE · YÁÑEZ

OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

188

¿Por cuánto tiempo es necesario retener o conservar la información contable en una empresa?

Según dispone el artículo 60 del Código de Comercio, debe conservarse como mínimo por 10 años.

URIBE · YÁÑEZ

OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

189

¿Por cuánto tiempo es necesario retener o conservar la información laboral en una empresa?

Según lo dispuesto en el Decreto único reglamentario del sector trabajo 1072 de 2015, resultados de perfiles laborales y relacionados con seguridad social deben ser conservados por un periodo mínimo de veinte (20) años, contados a partir del momento en que cese la relación laboral del trabajador con la empresa.

URIBE · YÁÑEZ

OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

189

¿Por cuánto tiempo es necesario retener o conservar la autorización para el tratamiento de datos personales?

Si bien la normativa no lo dispone expresamente, se recomienda mantenerla hasta que se ejecute la finalidad autorizada para el tratamiento.

URIBE · YÁÑEZ

OBLIGACIONES DE RETENCIÓN DE INFORMACIÓN

189

¿Por cuánto tiempo es necesario retener o conservar información relacionada con el consumidor?

Según el artículo 58 de la Ley 1480 de 2011 las demandas sobre efectividad de la garantía deberán presentarse a más tardar dentro del año siguiente a la expiración de la misma. Así que se recomienda retener la información hasta la prescripción de dicha acción.

URIBE · YÁÑEZ

LEY DE COMERCIO ELECTRÓNICO

197

¿Qué es un mensaje de datos?

Según el artículo 2 de la Ley 527 de 1999 es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

URIBE · YÁÑEZ

LEY DE COMERCIO ELECTRÓNICO

198

¿Qué es un sistema de información?

Según el artículo 2 de la Ley 527 de 1999 se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos

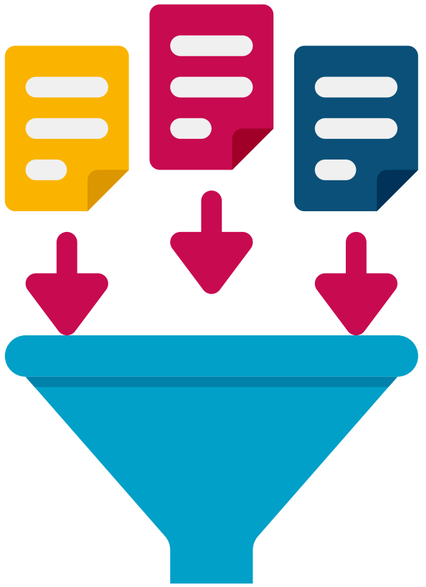
URIBE · YÁÑEZ

LEY DE COMERCIO ELECTRÓNICO

199

¿Un mensaje de datos puede satisfacer el requisito normativo de que la información sea presentada en su forma original?

Sí, según el artículo 8 de la Ley 527 de 1999:
Siempre que:
a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.



URIBE · YÁÑEZ

LEY DE COMERCIO ELECTRÓNICO

200

¿Cuál es la admisibilidad y fuerza probatoria de los mensajes de datos?

El artículo 8 de la LEY 527 DE 1999 dispone que:
"Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.
En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original."

URIBE · YÁÑEZ

Asesores Legales

Bogotá - Colombia
info@uribeyanez.com; gerencia@uribeyanez.com
Cra. 19B No. 83-02 oficina 304, Edificio Time Square

WWW.URIBEYANEZ.COM