**Ley de habeas data.**

**Disposiciones Generales**

A los fines de la presente ley se entiende por:

— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

**En su Capítulo II**

Principios generales relativos a la protección de datos

* Archivos de datos – Licitud
* Calidad de los datos
* Consentimiento
* Información
* Categoría de datos
* Datos relativos a la salud
* Seguridad de los datos
* Deber de confidencialidad
* Cesión
* Transferencia internacional

**Capítulo III**

Derechos de los titulares de datos

* Derecho de Información
* Derecho de acceso
* Contenido de la información
* Derecho de rectificación, actualización o supresión
* Excepciones
* Comisiones legislativas
* Gratuidad
* Impugnación de valoraciones personales

**Capítulo IV**

Usuarios y responsables de archivos, registros y bancos de datos

* Registro de archivos de datos. Inscripción
* Archivos, registros o bancos de datos públicos
* Supuestos especiales
* Archivos, registros o bancos de datos privados
* Prestación de servicios informatizados de datos personales
* Prestación de servicios de información crediticia
* Archivos, registros o bancos de datos con fines de publicidad

**Introducción**

La ley de Habeas Data es una ley argentina que establece los derechos de los ciudadanos a acceder, rectificar y cancelar sus datos personales. Esta ley es importante para proteger la privacidad y la seguridad de los datos personales.

**Objetivo**

El objetivo de este informe es identificar las normativas que se deben implementar para cumplir con la ley de Habeas Data.

**Metodología**

Para realizar este informe, se analizaron las siguientes normativas:

Ley 25.326 de Protección de Datos Personales

Ley 25.506 de Firma Digital

Ley 26.951 de Ciberseguridad

Ley 27.409 de Infraestructura Crítica

Reglamento General de Protección de Datos (RGPD)

**Resultados**

En base al análisis de las normativas, se identificaron las siguientes normativas que se deben implementar para cumplir con la ley de Habeas Data:

Clasificación de la información: Esta normativa es fundamental para identificar los datos personales que se deben proteger.

Consentimiento informado: Esta normativa establece que los datos personales solo se pueden recopilar con el consentimiento del titular de los datos.

Seguridad de la información: Esta normativa establece que los datos personales deben ser protegidos contra el acceso no autorizado, el uso indebido, la divulgación, la alteración o la destrucción.

**Conclusiones**

Las normativas identificadas en este informe son necesarias para cumplir con la ley de Habeas Data. Estas normativas proporcionan un marco para la protección de los datos personales y garantizan el derecho de los ciudadanos a acceder, rectificar y cancelar sus datos personales.

**Recomendaciones**

Se recomienda implementar las siguientes medidas adicionales para mejorar la protección de los datos personales:

Implementar un sistema de gestión de la seguridad de la información (SGSI): Un SGSI ayuda a las organizaciones a identificar, evaluar y mitigar los riesgos de seguridad de la información.

Formar a los empleados sobre la protección de datos personales: Los empleados deben estar capacitados sobre la importancia de la protección de datos personales y sobre las medidas que deben tomar para proteger los datos.

Implementar auditorías periódicas: Las auditorías periódicas ayudan a garantizar que las medidas de seguridad de la información sean efectivas.

Normativas específicas

A continuación, se describen las normativas específicas que se deben implementar para cumplir con la ley de Habeas Data:

**Clasificación de la información (Normativa 203)**

La ley de Habeas Data establece que los datos personales deben ser clasificados de acuerdo con su nivel de sensibilidad. Los datos personales se pueden clasificar en las siguientes categorías:

**Datos sensibles:** Son datos personales que revelan la raza, el origen étnico, las opiniones políticas, las convicciones religiosas, la salud o la vida sexual de una persona.

**Datos no sensibles**: Son datos personales que no revelan la información mencionada anteriormente.

La clasificación de la información es importante para garantizar que los datos personales sensibles se protejan de manera más estricta.

**Consentimiento informado (articulo 5 de la ley 25.326)**

La ley de Habeas Data establece que los datos personales solo se pueden recopilar con el consentimiento del titular de los datos. El consentimiento debe ser libre, expreso e informado.

El consentimiento libre significa que el titular de los datos debe dar su consentimiento sin presión ni coacción. El consentimiento expreso significa que el titular de los datos debe manifestar su consentimiento de manera clara y explícita. El consentimiento informado significa que el titular de los datos debe estar informado sobre el propósito de la recopilación de datos y sobre sus derechos en relación con sus datos personales.

La normativa sobre el consentimiento informado de datos informáticos en Argentina se encuentra regulada por la Ley 25.326 de Protección de Datos Personales. Esta ley establece que el tratamiento de datos personales debe estar basado en el consentimiento del titular de los datos personales.

El consentimiento del titular de los datos personales debe ser libre, expreso e informado. El consentimiento debe ser libre cuando el titular de los datos personales no se sienta obligado a otorgarlo. El consentimiento debe ser expreso cuando el titular de los datos personales manifiesta su voluntad de otorgar el consentimiento. El consentimiento debe ser informado cuando el titular de los datos personales recibe información adecuada y completa sobre el tratamiento de sus datos personales.

El consentimiento del titular de los datos personales puede ser otorgado por escrito, verbalmente o por medios electrónicos.

El consentimiento del titular de los datos personales no es necesario en los siguientes casos:

* Cuando el tratamiento de los datos personales sea necesario para el cumplimiento de una obligación legal.
* Cuando el tratamiento de los datos personales sea necesario para la ejecución de un contrato en el que el titular de los datos personales sea parte.
* Cuando el tratamiento de los datos personales sea necesario para la protección de intereses vitales del titular de los datos personales o de otras personas.
* Cuando el tratamiento de los datos personales sea necesario para la realización de una investigación científica o histórica, siempre que los datos personales no se utilicen para fines de lucro.

El consentimiento del titular de los datos personales puede ser revocado en cualquier momento. La revocación del consentimiento debe ser notificada al responsable de tratamiento de datos personales.

Las personas que consideren que su derecho al consentimiento informado de datos informáticos ha sido vulnerado pueden presentar una denuncia ante la Agencia de Acceso a la Información Pública (AAIP).

A continuación, se describen con más detalle algunos aspectos relacionados con el consentimiento informado de datos informáticos:

* **La información adecuada y completa:** La información que debe ser proporcionada al titular de los datos personales debe ser adecuada y completa. La información debe ser clara, precisa y accesible para el titular de los datos personales. La información debe incluir los siguientes aspectos:
  + La finalidad del tratamiento de los datos personales.
  + Los tipos de datos personales que serán tratados.
  + Los destinatarios de los datos personales.
  + Los derechos del titular de los datos personales.
* **El consentimiento libre y voluntario:** El consentimiento del titular de los datos personales debe ser otorgado de forma libre y voluntaria. El titular de los datos personales debe tener la oportunidad de preguntar todas las dudas que tenga sobre el tratamiento de sus datos personales.
* **La revocación del consentimiento:** El consentimiento del titular de los datos personales puede ser revocado en cualquier momento. La revocación del consentimiento debe ser notificada al responsable de tratamiento de datos personales.

El consentimiento informado de datos informáticos es un derecho fundamental que permite a las personas controlar sus datos personales. Este derecho es importante para garantizar la transparencia y la accountability en el tratamiento de datos informáticos.

En el caso particular de los datos sensibles, el consentimiento del titular de los datos personales debe ser expreso y por escrito. Los datos sensibles son aquellos que están relacionados con la intimidad de las personas, por ejemplo, la información sobre la religión, la ideología política, o la orientación sexual.

**Seguridad de la información (Normativa 205 seguridad física – Normativa 208 plan de contingencias – Normativa 221 acceso a los datos)**

La ley de Habeas Data establece que los datos personales deben ser protegidos contra el acceso no autorizado, el uso indebido, la divulgación, la alteración o la destrucción.

Para proteger los datos personales, las organizaciones deben implementar medidas de seguridad de la información, como:

**Control de acceso**: Las organizaciones deben restringir el acceso a los datos personales a las personas que necesitan acceder a ellos para cumplir con sus funciones.

**Encriptación**: Las organizaciones deben encriptar los datos personales para protegerlos de la divulgación no autorizada.

**Backup:** Las organizaciones deben realizar copias de seguridad de los datos personales para protegerlos de la pérdida o la destrucción.

Implementación

La implementación de las normativas identificadas en este informe requiere un esfuerzo significativo por parte de las organizaciones. Sin embargo, estas normativas son necesarias para cumplir con la ley de Habeas Data y para proteger los datos personales de los ciudadanos.

Normativas que considero aplicables a la ley de habeas data:

* **Normativa 203 – Clasificación de los datos**

Es importante ya que debemos cumplir con lo siguiente:

* **El consentimiento expreso del titular de los datos:** El responsable de tratamiento de datos personales sólo puede tratar datos sensibles con el consentimiento expreso del titular de los datos.
* **La finalidad específica del tratamiento:** El tratamiento de datos sensibles debe tener una finalidad específica y legítima.
* **La proporcionalidad del tratamiento:** El tratamiento de datos sensibles debe ser proporcional a la finalidad para la cual se han obtenido.

El incumplimiento de estos requisitos puede acarrear sanciones administrativas para los responsables de tratamiento de datos personales.

A continuación, se muestran algunos ejemplos de datos personales sensibles:

* **Datos genéticos:** Información sobre la composición genética de una persona, por ejemplo, la información sobre el riesgo de desarrollar ciertas enfermedades.
* **Datos biométricos:** Información sobre las características físicas de una persona, por ejemplo, la información sobre la huella dactilar o la retina.
* **Datos de salud:** Información sobre el estado de salud de una persona, por ejemplo, la información sobre las enfermedades que padece o los tratamientos que recibe.
* **Datos sobre la orientación sexual:** Información sobre la orientación sexual de una persona, por ejemplo, la información sobre sus relaciones sentimentales.
* **Datos sobre la religión:** Información sobre las creencias religiosas de una persona, por ejemplo, la información sobre su fe o sus prácticas religiosas.
* **Datos sobre la ideología política:** Información sobre las creencias políticas de una persona, por ejemplo, la información sobre su partido político o sus ideas políticas.
* **Normativa 206 –** PROYECTOS DE SISTEMAS DE INFORMACIÓN

**Esta normativa es importante ya que recae la responsabilidad sobre los desarrolladores**

Esta normativa es importante porque establece quienes son los responsables de estos proyectos los cuales son:

RESPONSABLES

Comité Información Pública (COMIP)

Lideres de Proyectos Informáticos

Responsables de Áreas de Desarrollo de Sistemas de Información.

Desarrolladores de Sistemas.

Programadores.

Implementadores.

Auditoría de Sistemas de Información evalúa y verifica el cumplimiento de la norma.

La normativa 206 de la Ley de Habeas Data de Argentina establece los requisitos que deben cumplir los proyectos de sistemas de información que tratan datos personales. Estos requisitos están orientados a garantizar la protección de los datos personales durante todo el ciclo de vida del sistema.

Los requisitos establecidos en la normativa 206 son los siguientes:

* **Identificación del responsable de tratamiento de datos personales:** El responsable de tratamiento de datos personales debe ser identificado en el proyecto de sistema de información.
* **Declaración de finalidad:** El proyecto de sistema de información debe declarar la finalidad para la cual se van a tratar los datos personales.
* **Declaración de medidas de seguridad:** El proyecto de sistema de información debe declarar las medidas de seguridad que se van a adoptar para proteger los datos personales.
* **Consulta previa a la Agencia de Acceso a la Información Pública:** Los proyectos de sistemas de información que traten datos sensibles deben ser consultados previamente a la Agencia de Acceso a la Información Pública (AAIP).

El incumplimiento de estos requisitos puede acarrear sanciones administrativas para los responsables de tratamiento de datos personales.

La normativa 206 es importante para garantizar la protección de los datos personales en los proyectos de sistemas de información. Estos requisitos ayudan a los responsables de tratamiento de datos personales a identificar los riesgos asociados al tratamiento de datos personales y a adoptar medidas para mitigar estos riesgos.

A continuación, se describen con más detalle algunos de los requisitos establecidos en la normativa 206:

* **Identificación del responsable de tratamiento de datos personales:** El responsable de tratamiento de datos personales es la persona física o jurídica que decide sobre el tratamiento de los datos personales. El responsable de tratamiento de datos personales debe ser identificado en el proyecto de sistema de información para que las personas titulares de los datos personales puedan ejercer sus derechos.
* **Declaración de finalidad:** El proyecto de sistema de información debe declarar la finalidad para la cual se van a tratar los datos personales. La finalidad del tratamiento de datos personales debe ser específica, lícita y no excesiva.
* **Declaración de medidas de seguridad:** El proyecto de sistema de información debe declarar las medidas de seguridad que se van a adoptar para proteger los datos personales. Las medidas de seguridad deben ser adecuadas para garantizar la seguridad de los datos personales.
* **Consulta previa a la Agencia de Acceso a la Información Pública:** Los proyectos de sistemas de información que traten datos sensibles deben ser consultados previamente a la AAIP. La AAIP puede emitir recomendaciones sobre el proyecto de sistema de información para garantizar la protección de los datos sensibles.

Los responsables de tratamiento de datos personales deben cumplir con los requisitos establecidos en la normativa 206 para garantizar la protección de los datos personales en los proyectos de sistemas de información.

* **Normativa 220 – GESTIÓN DE LOS DATOS**

**Asegurar** la correcta definición de niveles de autorización de accesos a los datos.

Lo considero importante ya que no todos deben acceder a los datos, ya que esto podría generar conflictos o filtraciones innecesarias, de esta manera se podrá identificar fácilmente a los responsables.