Universidad de los Andes
Colombia

Hacia un enfoque preventivo en el tratamiento de datos personales: PbD & accountability:

Nelson Remolina Angarita
nremolin@uniandes.edu.co

@Nelson Remolina

InfoDF, Ciudad de México, 26 de enero de 2018

Universidad de los Andes Colombia

https://gecti.uniandes.edu.co

GECTI

INICIO | NOSOTROS | PUBLICACIONES | CURSOS | EVENTOS | OPINIÓN | DERECHO del Espacio Ultraterrestre

BUSCAR...

GECTI

Grupo de
Estudios en internet,
Comercio electrónico
Telecomunicaciones e
Informática

BIENVENIDO (A)

El GECTI (Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática) fue creado el 5 de octubre de 2001 por el profesor ***Nelson Remolina Angarita*** *y un grupo de expertos (as) en derecho y tecnología. Busca fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la Internet, la Sociedad de la Información y temas convergentes.*

IN BLOG

SIC debe modificar guía de accountability e incluir medidas útiles, medibles y verificables para proteger los derechos de los colombianos cuando sus datos son exportados a los países avalados por la SIC

Por. Nelson Remolina Angarita (12/X/2017)

Read More

IN BLOG

Senado de la República cita a la SIC a control político por incluir a USA dentro del listado de países con nivel adecuado de protección de datos personales

Por. Nelson Remolina Angarita (02/IX/2017)

Read More

IN BLOG

Antecedentes de la Circular 5 de 2017 de la SIC: transferencias internacionales de datos personales

Por: Nelson Remolina Angarita (11/08/2017).

Read More

Buscar

Artículos Recientes

SIC debe modificar guía de accountability e incluir medidas útiles, medibles y verificables para proteger los derechos de los colombianos cuando sus datos son exportados a los países avalados por la SIC

Senado de la República cita a la SIC a control político por incluir a USA dentro del listado de países con nivel adecuado de protección de datos personales

Antecedentes de la Circular 5 de 2017 de la SIC: transferencias internacionales de datos personales

Right to be forgotten in cyberspace? International principles and considerations about Latin American regulations

Debe Colombia incluir a los Estados Unidos dentro del listado de países que proporcionan niveles adecuados de protección de datos?. Decálogo de reflexiones académicas y ciudadanas.

Tags

América Latina
Colombia
Corte
Autoridad de control
Navidad
Cloud computing
Ley
Corte Constitucional
Internet
Objeción
Redes Sociales
Gecti
International
Recolección
personal
data
Retos
Presidente de Colombia
Protección de datos
internacional
colección
personales

Denominación	Significado
***Privacy* – Norteamérica-**	Control información (CSJ, USA, 1989); "self determination" Westin (1967)
***Autodeterminación Informativa* – Alemania-**	Protección de las personas frente a la ilimitada recolección, archivo, uso, retransmisión y "reciclaje" de sus datos personales (Nicaragua 2012, Costa Rica 2011, México, 2010)
***Libertad informática* –Italia-**	"diritto a la riservatezza", facultad de la persona de controlar su información
***Habeas data* – Latinomerica-**	Brasil, CN (1988); Paraguay, CN (1992); Perú , CN (1993) Venezuela, CN (2000); Panamá , CN (2004); Honduras, CN (2006); República Dominicana, CN (2010)
***Protección de datos personales* –Europa, Latam-**	Europa (2000), Panamá (2004), Ecuador (2008) y México (2009). *Perú –Ley 29733/11-*
Derecho al debido tratamiento de los datos personales	"Debido proceso" en la recolección, almacenamiento, uso, circulación y demás actividades que involucra el tratamiento de datos personales


BBC
THE
VIRTUAL
REVOLUTION

internet live stats

3,830,304,000

Internet Users in the world

1,322,900

Total number of Websites

61,031

Websites hacked today

2,089,293,417

Facebook active users

Fuente: http://www.internetlivestats.com
23-I-2018. 14:45

https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

CBC NEWS

'Data is the new oil': Your personal information is now the world's most valuable commodity

Huge amounts of data are controlled by just 5 global mega-corporations that are bigger than most governments

Ramona Pringle · Technology Columnist · CBC News
August 25, 2017

The five most valuable companies in the world today — Apple, Amazon, Facebook, Microsoft and Google's parent company Alphabet — have commodified data and taken over their respective sectors. (Pawel Kopczynski/Reuters)

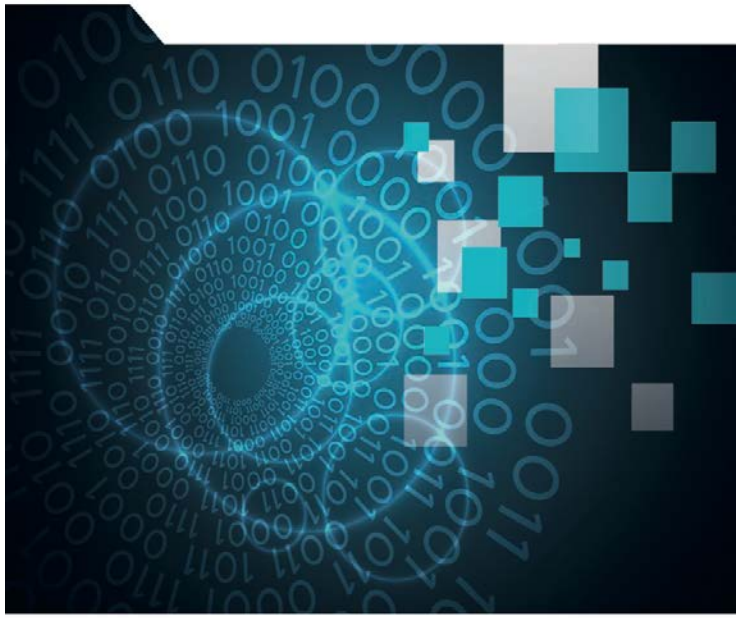
http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677

$ 26,885 (2016) https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx

CNN. 27-I-2016

"Our mission to connect the world is more important now than ever," said Mark Zuckerberg, Facebook founder and CEO. "Our business did well in 2016, but we have a lot of work ahead to help bring people together."

OECD Digital Economy Outlook 2017



OECD

Executive summary

Concerns about digital security and privacy restrain ICT adoption and business opportunities

With growing intensity of ICT use, businesses and individuals face greater digital security and privacy risks. SMEs in particular need to introduce or improve digital security risk management practices. Many countries respond with national digital security strategies, but few have a national privacy strategy so far. Meanwhile, privacy risks add to consumers'

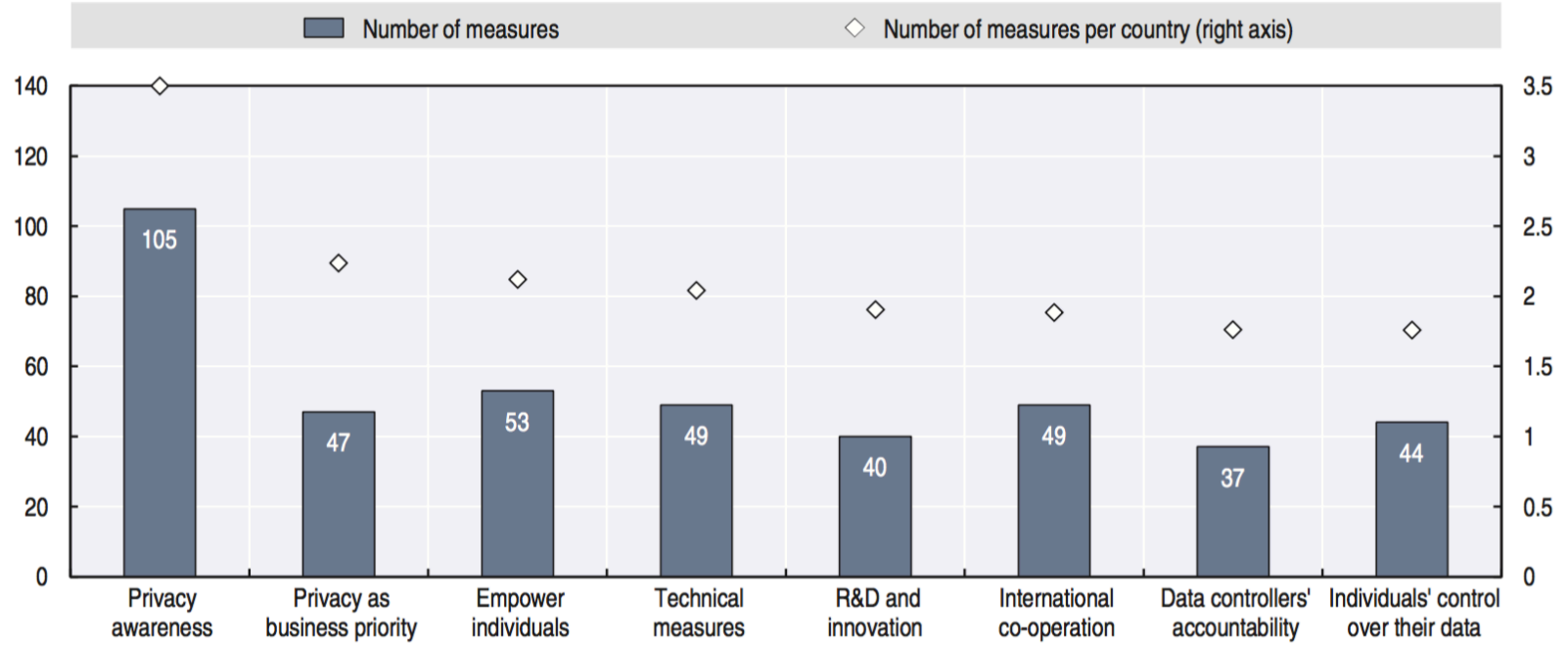
SME Small and medium-sized enterprise

OECD Digital Economy Outlook 2017

OECD

Countries are implementing a growing range of measures to address increasing challenges to privacy

Figure 2.10. **Policy measures to promote privacy**



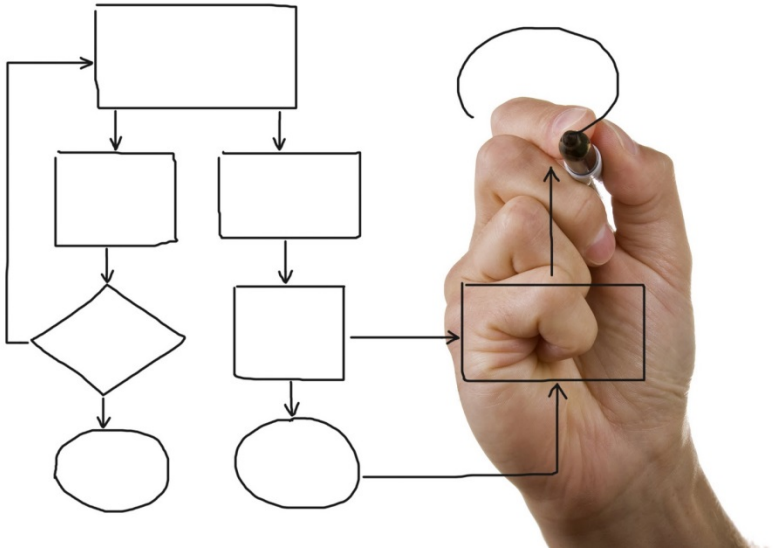
Note: This figure is based on a total of 424 policy measures to promote privacy reported by 30 countries.

StatLink http://dx.doi.org/10.1787/888933584678

- Incorporar la privacidad en el interior de los sistemas de información, de las arquitecturas y las redes de comunicación y de los procesos productivos, para que sea la opción "por defecto", desde el inicio hasta el fin de su ciclo de vida.
- http://www.abc.es/blogs/ley-red/public/post/el-potencial-revolucionario-de-la-privacidad-por-diseno-14670.asp

Privacidad por Diseño promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización.

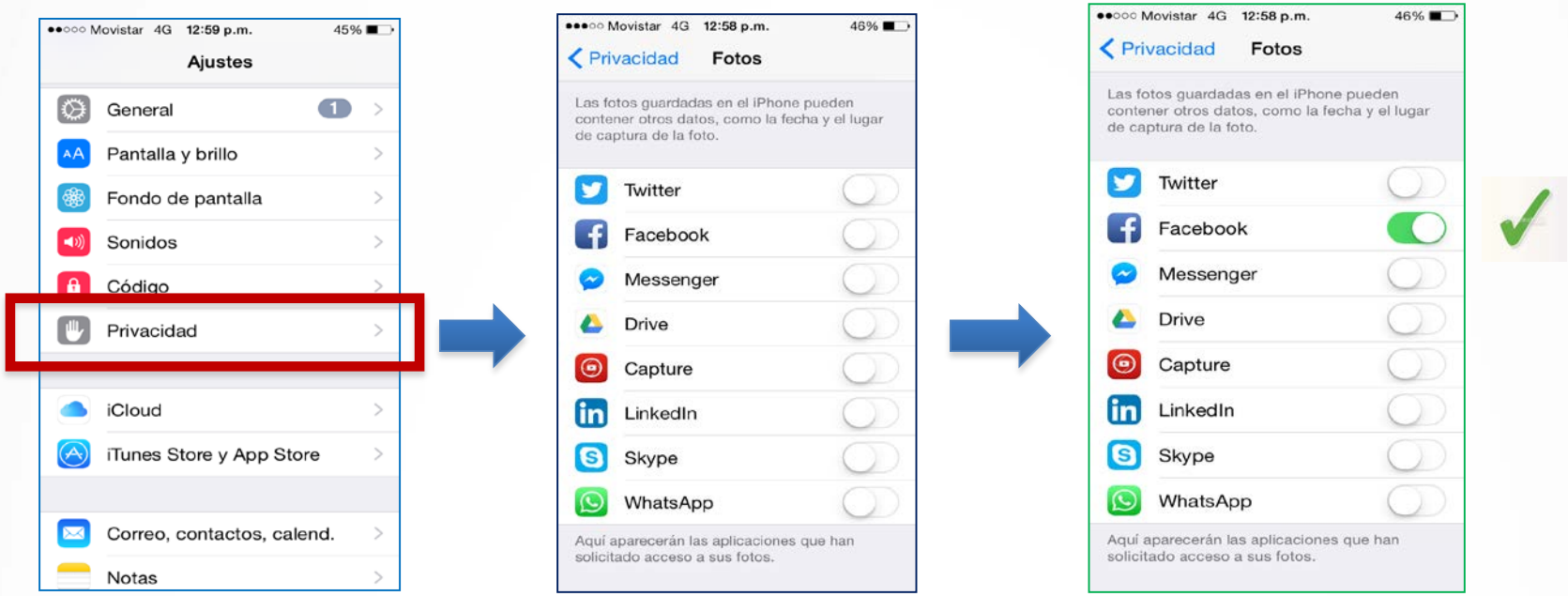
Los 7 Principios Fundamentales



2. Privacidad como la ***Configuración Predeterminada***

Todos podemos estar seguros de una cosa – ¡Lo predeterminado es lo que manda! La *Privacidad por Diseño* busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios. Si una la persona no toma una acción, aún así la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad – está interconstruida en el sistema, como una configuración *predeterminada*.

Privacidad por diseño & por defecto: en la infraestructura y en la autorización



La persona decide sobre su privacidad

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Artículo 25

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Principio de Responsabilidad

La persona responsable deberá:

a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y

b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.

Accountability desde la perspectiva de entidades internacionales

	Año	Énfasis
RED IBEROAMERICANA DE PROTECCIÓN DE DATOS	2006	Valor agregado + mecanismos para medir el nivel de eficacia del cumplimiento de la ley y el grado de protección de los datos personales
31 conferencia internacional de autoridades de protección de datos y privacidad	2009	Medidas necesarias para cumplir la ley y evidenciar dicho cumplimiento
OECD BETTER POLICIES FOR BETTER LIVES	2012	Programa gestión de privacidad
	2016	Asegurar y demostrar cumplimiento **+** verificar eficacia de la medidas adoptadas
RED IBEROAMERICANA DE PROTECCION DE DATOS ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES	2017	Mecanismos necesarios para acreditar el cumplimiento **+** revisar y evaluar con el objeto de medir su nivel de eficacia

BUEN GOBIERNO CORPORATIVO EN TRATAMIENTO DE DATOS

Fuente: https://www.youtube.com/watch?v=4RMdGZz1zBk

- Es imprescindible que los instrumentos de autorregulación estén acompañados de herramientas que los hagan **eficaces**.
- Consagrar mecanismos de **control** interno y externo de verificación del cumplimiento
- Establecer **niveles de efectividad** de cumplimiento de las normas.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

GRUPO DE TRABAJO TEMPORAL SOBRE AUTORREGULACIÓN Y PROTECCIÓN DE DATOS PERSONALES (2006)

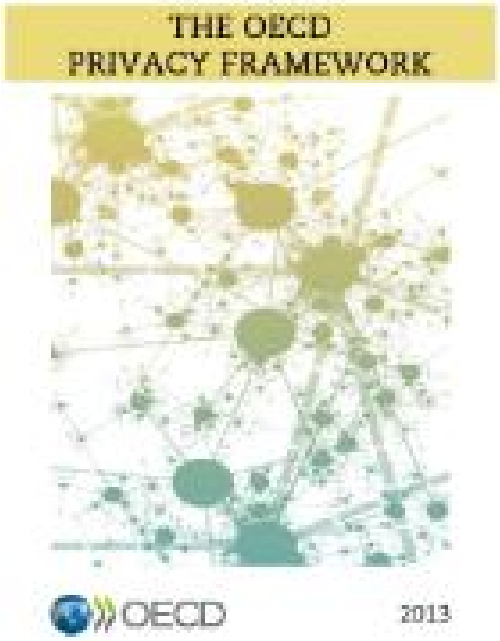
RECOMENDACIONES

"1. Incorporar en las futuras regulaciones disposiciones explícitas tendentes a utilizar mecanismos de autorregulación que: (a) Representen un valor añadido en su contenido respecto de lo dispuesto en las leyes, y (b) Contengan o estén acompañados de ***mecanismos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales****. "*

.

BETTER POLICIES FOR BETTER LIVES

Novedades:



1. **Las estrategias nacionales de privacidad** (*National privacy strategies*). Necesidad de estrategia nacional multifacética coordinado en los más altos niveles del gobierno.
2. **Programas de gestión de Privacidad** (*Privacy management programmes*). Mecanismo operativo a través del cual las organizaciones implementan la protección de privacidad.
3. **Notificación de violación de la seguridad de datos** (*Data security breach notification*). Esta disposición abarca tanto la notificación a la autoridad y a la persona afectada por una falla de seguridad que afecta a los datos personales.

http://www.oecd.org/sti/ieconomy/privacy.htm

BETTER POLICIES FOR BETTER LIVES

PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:

b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

OECD
BETTER POLICIES FOR BETTER LIVES

PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:

a) Have in place a privacy management programme that:

i. gives effect to these Guidelines for all personal data under its control;

ii. is tailored to the structure, scale, volume and sensitivity of its operations;

iii. provides for appropriate safeguards based on privacy risk assessment;

iv. is integrated into its governance structure and establishes internal oversight mechanisms;

v. includes plans for responding to inquiries and incidents;

vi. is updated in light of ongoing monitoring and periodic assessment;

COMISIÓN EUROPEA

Bruselas, 25.1.2012
COM(2012) 11 final

Propuesta de **REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)

Artículo 22

Obligaciones del responsable del tratamiento

1. El responsable del tratamiento adoptará políticas e implementará medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento.

3. El responsable del tratamiento implementará mecanismos para verificar la eficacia de las medidas contempladas en los apartados 1 y 2. Siempre que no sea desproporcionado, estas verificaciones serán llevadas a cabo por auditores independientes internos o externos.

ESTÁNDARES
DE PROTECCIÓN
DE DATOS PERSONALES

20. Principio de responsabilidad

20.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

20.2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

20.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

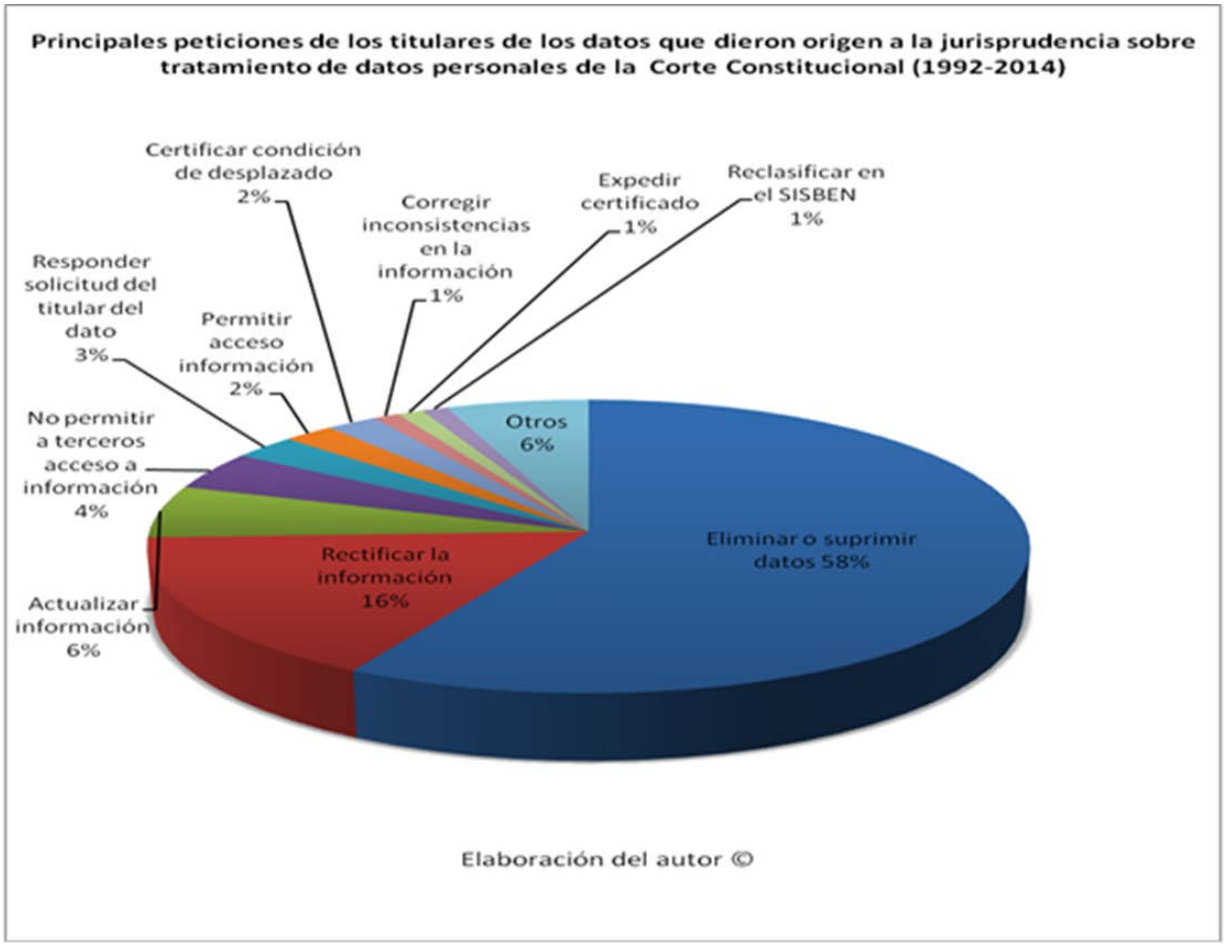
20.4. El responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.


Compromiso de la organización
Controles del PGD
Evaluación
Revisión
Demostración
ACCOUNTABILITY

“Accountability” y calidad de la información

80% de las solicitudes de tutela revisada por la Corte Constitucional son sobre calidad de información

53% de las multas de la SIC es por principio de veracidad (SIC, dic 2015)



Remolina Angarita, Nelson ©

Universidad de los Andes Colombia

GECTI

Gracias

- nremolin@uniandes.edu.co
- http://gecti.uniandes.edu.co/
- http://habeasdatacolombia.uniandes.edu.co/

- @GECTIXXI @Nelson Remolina