JURÍDIA - Cursos en Línea sobre Derecho Preventivo para las Tecnologías de la Información y las Comunicaciones (TIC)

EL DERECHO PREVENTIVO EN LA GESTIÓN DE DATOS PERSONALES DIGITALES

Camilo Alfonso Escobar Mora

Fundador de JURÍDIA®

gerencia@juridia.co - www.juridia.co

Cont@ctenos

Móvil: (57) 320 803 4090

Dirección: Calle 108 # 57-09, oficina 507

Bogotá D.C., Colombia, Suramérica.

Página web: www.juridia.co

Correo: comunicaciones@juridia.co

AGENDA

1. Explicación del derecho de protección de datos personales en Colombia.
2. Implicaciones principales en los medios digitales.
3. Recomendaciones de derecho preventivo.

OBJETIVOS

- Explicar la normatividad jurídica principal de protección de datos personales digitales en Colombia.
- Explicar la forma en que el derecho aplica en los medios digitales.
- Explicar mí doctrina del derecho preventivo en los medios digitales.
- Presentar recomendaciones de derecho preventivo para la protección y uso adecuado de los datos personales digitales.

VIDEO DE SENSIBILIZACIÓN

Explicación del derecho de protección de datos personales en Colombia

Introducción

CONSTITUCIÓN POLÍTICA DE COLOMBIA

ARTICULO 15. *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.* ***De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.***

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Introducción

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley”.

Introducción

Se debe tener muy claro que este derecho al ser fundamental solo aplica para las personas naturales (las personas jurídicas se protegen por medio del derecho comercial y otras normas dirigidas especialmente a la protección y gestión de las empresas).

CONTENIDO Y ALCANCE DEL DERECHO DE PROTECCIÓN A LOS DATOS PERSONALES

1). PROTECCIÓN A LA INFORMACIÓN PERSONAL *(hace referencia a la calidad de la información -integridad, autenticidad, disponibilidad, actualidad, custodia, etc.-).*

2). LA AUTODETERMINACIÓN INFORMATIVA *(hacer referencia a que es el titular quien determina el alcance que le autoriza a un tercero cuando éste vaya a tratar sus datos personales -el titular es quien decide qué finalidades y tratamientos son permitidos sobre sus datos personales, salvo que una norma explícitamente permita un(os) tratamiento(s) para cierta(s) finalidades sin tener que obtener el consentimiento del titular-).*

3). EL EJERCICIO DE LA ACCIÓN DE HÁBEAS DATA *(hace referencia a la acción de reclamación que tiene el titular para que le traten adecuadamente sus datos personales -reclamación en principio ante el responsable del tratamiento y en segundo orden ante la Autoridad de Protección de Datos Personales, que en Colombia es la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio-).*

Evolución Jurisprudencial

Líneas jurisprudenciales que han existido sobre la naturaleza, contenido y alcance de este derecho:

1) LÍNEA JURISPRUDENCIAL QUE CONCIBE AL **DERECHO FUNDAMENTAL DE PROTECCIÓN A LOS DATOS PERSONALES COMO UN DERECHO ESTRECHAMENTE LIGADO AL DERECHO FUNDAMENTAL A LA INTIMIDAD.**

2) LÍNEA JURISPRUDENCIAL QUE CONCIBE AL **DERECHO FUNDAMENTAL DE PROTECCIÓN A LOS DATOS PERSONALES COMO UN DERECHO ESTRECHAMENTE LIGADO AL DERECHO FUNDAMENTAL A LA LIBERTAD.**

3) LÍNEA JURISPRUDENCIAL QUE CONCIBE AL **DERECHO FUNDAMENTAL DE PROTECCIÓN A LOS DATOS PERSONALES COMO UN DERECHO AUTÓNOMO E INDEPENDIENTE.**

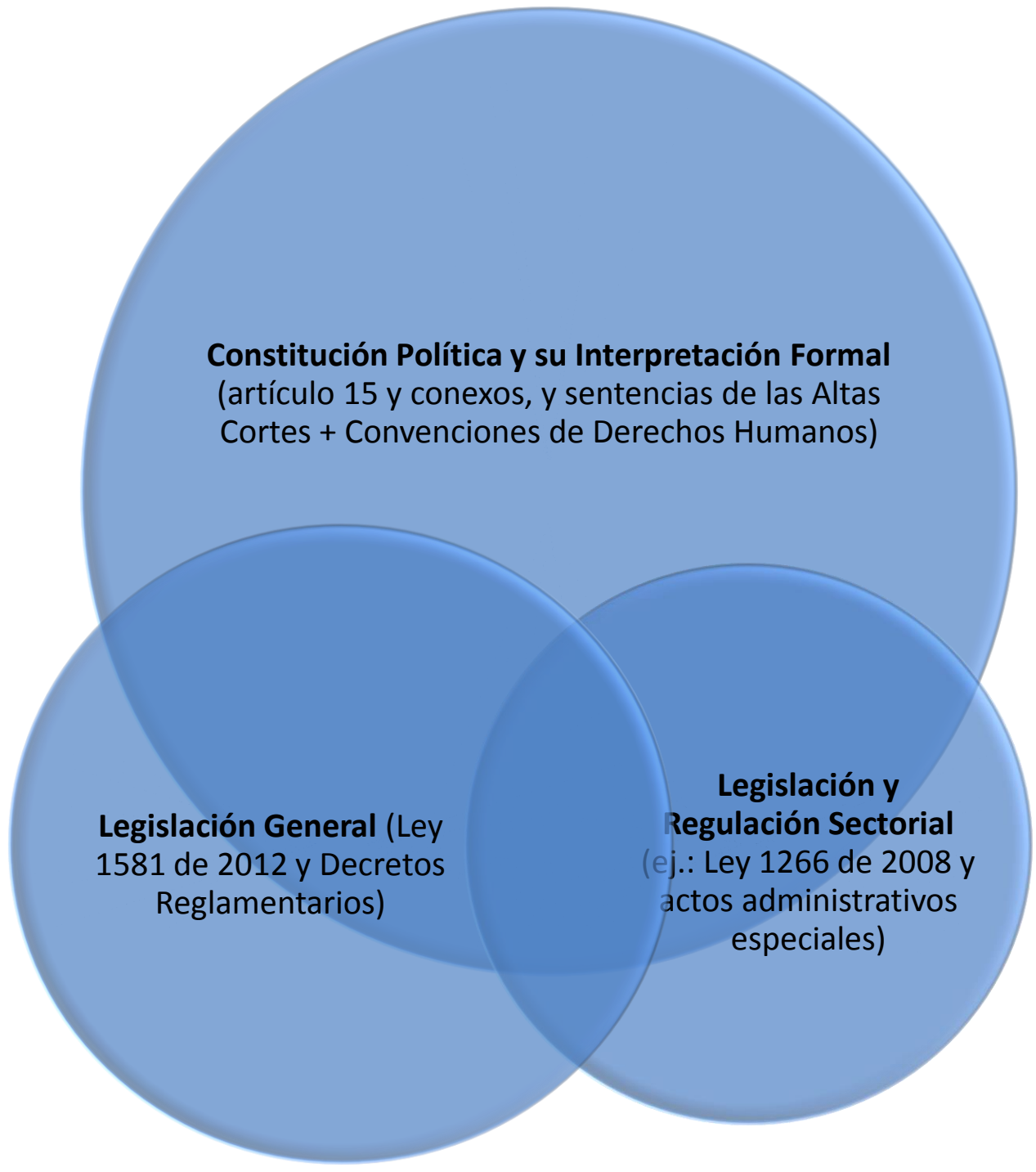
OTRO ARTÍCULO DE LA CONSTITUCIÓN POLÍTICA DE COLOMBIA RELACIONADO CON EL TEMA

"ARTICULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".

VIDEO DE APROPIACIÓN

FUENTES JURÍDICAS PRINCIPALES DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA



LA INTERPRETACIÓN, ARGUMENTACIÓN, APLICACIÓN Y, EN GENERAL, FUNDAMENTACIÓN DEL DERECHO

- **Normas de textura abierta** (premisas y consecuencias altamente abstractas).

- **Normas de textura cerrada** (silogismo jurídico: premisas y consecuencias jurídicas delimitadas. Todo depende del control de la vaguedad y la ambigüedad en el contenido de la norma, es decir de su claridad, precisión y coherencia).

- **Concreta** (subsunción: el supuesto de hecho está contemplado directamente en la norma, por lo tanto se le aplica el supuesto de derecho y la consecuencia jurídica respectiva).

- **Extensiva** (otros métodos inexactos pero susceptibles de validez).

TEORÍA DEL DERECHO

- CAMPOS DE ACCIÓN DEL DERECHO

a). Privado (concepto del derecho enfocado a intereses privados, por ende se tiene más libertad para actuar).

b). Público (concepto del derecho enfocado al interés general de los miembros de una sociedad, por ello se tiene más restricción para actuar).

PANORAMA PRINCIPAL

Clasificación general de la Información:

Reflexión

SE DEBE APLICAR TANTO UN **MÉTODO DEDUCTIVO** (DE LO GENERAL A LO PARTICULAR) COMO UN **MÉTODO INDUCTIVO** (DE LO PARTICULAR A LO GENERAL) **PARA PODER DETERMINAR CON CLARIDAD, PRECISIÓN, VALIDEZ Y EFICACIA LA NATURALEZA, EL OBJETO Y EL ALCANCE DEL DERECHO FUNDAMENTAL DE PROTECCIÓN A LOS DATOS PERSONALES.**

ES DECIR QUE SE DEBE DETERMINAR TANTO EL TODO COMO SUS PARTES PARA SABER DE QUÉ CLASE DE DRRECHO SE ESTÁ HABLANDO Y APLICAR CON PRECISIÓN DICHO DERECHO EN CADA CASO CONCRETO.

Definiciones Relevantes

Información Personal (dato personal): Todo dato o conjunto de datos que se asocian o vinculan con una persona natural.

Información Personal Pública (dato personal público): Toda información personal cuyo tratamiento se puede realizar sin contar con la autorización del titular, pero que en todo caso se debe tratar con base en los lineamientos, deberes y principios consagrados en la Ley 1581 de 2012 y sus Decretos Reglamentarios.

Información Personal Restringida (dato personal restringido): Toda información personal cuyo tratamiento solo se puede realizar si se cuenta con la autorización previa, expresa e informada del titular (aquí se incluye a los **Datos Sensibles**, que son todos aquellos que puedan causar un tratamiento desigual, limitativo o degradatorio de los derechos del titular. Igualmente se incluye como Datos Sensibles a los **Datos de Menores de Edad** y a los **Datos Biométricos**, cuyo tratamiento solo se puede realizar si se autoriza expresamente -y en el caso de los menores de edad la autorización la debe hacer el representante formal del menor de edad, previo a escucharse la opinión del menor acerca del tratamiento que se solicita-).

Definiciones Relevantes

Clasificación especial de la información, propiamente de la información personal (datos personales):

- **Privada.**
- **Semiprivada.**
- **Sensible.**
- **Pública.**
- **Semipública.**
- **Clasificada.**
- **Confidencial.**
- **Reservada.**
- **Secreta.**

Definiciones Relevantes

Tratamiento: Toda gestión que se realice sobre los datos personales de un titular, como lo es la recolección, el almacenamiento, la circulación, el uso y la supresión de los datos.

Titular de la Información Personal: Toda persona natural cuyos datos personales vayan, estén o hayan sido tratados (existen titulares tanto en la compañía como por fuera de esta).

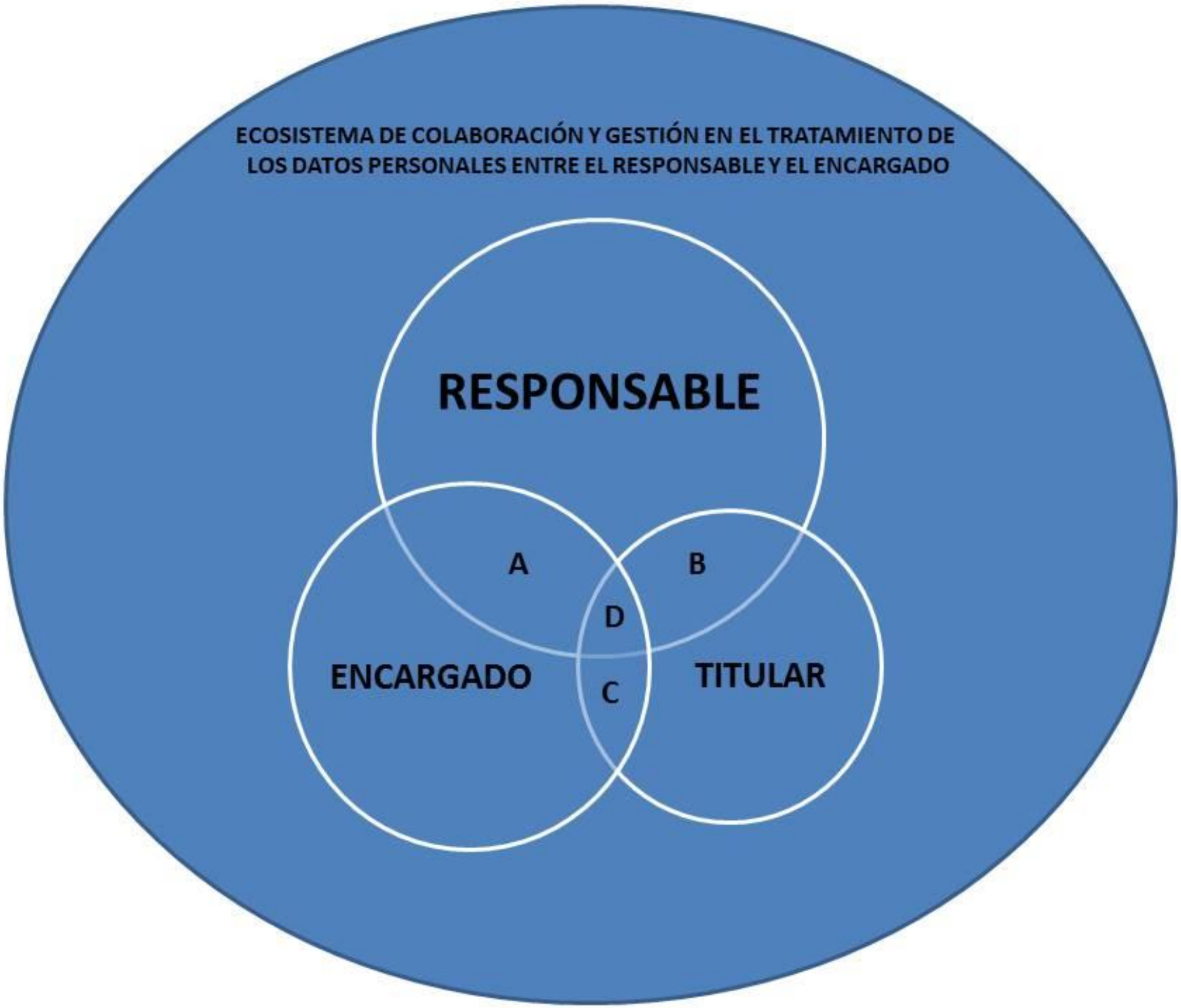
Responsable del tratamiento de la información personal: Persona natural o jurídica, pública o privada, que decida de forma directa y autónoma sobre el tratamiento de los datos personales.

NOTA: Es importante aclarar que frente al titular el Responsable del Tratamiento siempre es la empresa, cosa distinta a que sus trabajadores y/o contratistas tengan la obligaciones de realizar adecuadamente los tratamientos en el desempeño de sus funciones (en este caso estos trabajadores y/o contratistas responderán pero frente a la empresa y no como responsables del tratamiento formalmente sino como sujetos obligados a realizar tratamientos adecuadamente).

Definiciones Relevantes

Encargado del tratamiento de la información personal: Persona natural o jurídica, pública o privada, que realice los tratamientos a nombre y bajo las instrucciones del Responsable del Tratamiento.

NOTA: Es importante aclarar que Encargado del Tratamientos siempre debe ser un tercero distinto a la empresa, es decir que pueden ser los contratistas o aliados de la empresa cuando estos realicen tratamientos en representación y bajo las indicaciones de la empresa (los trabajadores no pueden ser encargados porque precisamente hacen parte de la empresa, estos como se indicó anteriormente son sujetos obligados a realizar tratamientos adecuadamente en el desempeño de sus funciones y responderán por ello ante la empresa).


ECOSISTEMA DE COLABORACIÓN Y GESTIÓN EN EL TRATAMIENTO DE LOS DATOS PERSONALES ENTRE EL RESPONSABLE Y EL ENCARGADO
RESPONSABLE
A
B
D
ENCARGADO
C
TITULAR

LOS TITULARES ESTÁN PRESENTES EN TODOS LOS GRUPOS DE INTERÉS DE LA EMPRESA O ENTIDAD

Son todos los sujetos involucrados o afectados con una gestión empresarial o institucional, tales como:

- Consumidores (usuarios).
- Trabajadores.
- Proveedores.
- Comunidad de impacto.
- Aliados.
- Socios.

La validez jurídica de un modelo de protección y uso de datos personales se logra si se protegen los derechos de la empresa o entidad y los de todos y cada uno de los grupos de interés. Se debe lograr una armonía entre todos.

Ley 1581 de 2012

DERECHOS DEL TITULAR

Los derechos del titular son:

- Conocimiento.
- Acceso.
- Rectificación.
- Actualización.
- Revocatoria.
- Supresión.

(la recolección de los datos personales siempre requiere de la autorización previa, expresa e informada del titular salvo que exista un mandato legal o contractual que faculte expresamente la compañía para recolectar o usar los datos personales directamente).

Definiciones Relevantes

Autoridad Pública de Protección de Datos Personales: Ente público encargado de velar porque se cumplan en debida forma las normas sobre protección de datos personales que apliquen en cada caso concreto.

Por **regla general es la <u>Superintendencia de Industria y Comercio (SIC)</u>, salvo:**

1. Que se trate de entidades financieras vigiladas por la <u>Superintendencia Financiera</u> (en cuyo caso ésta es su autoridad de protección de datos personales).

2. Que se trate de autoridades o de personas que ejerzan función pública (en este caso la <u>Procuraduría General de la Nación</u> es la autoridad que los investiga de fondo y si hay lugar a ello los sanciona).

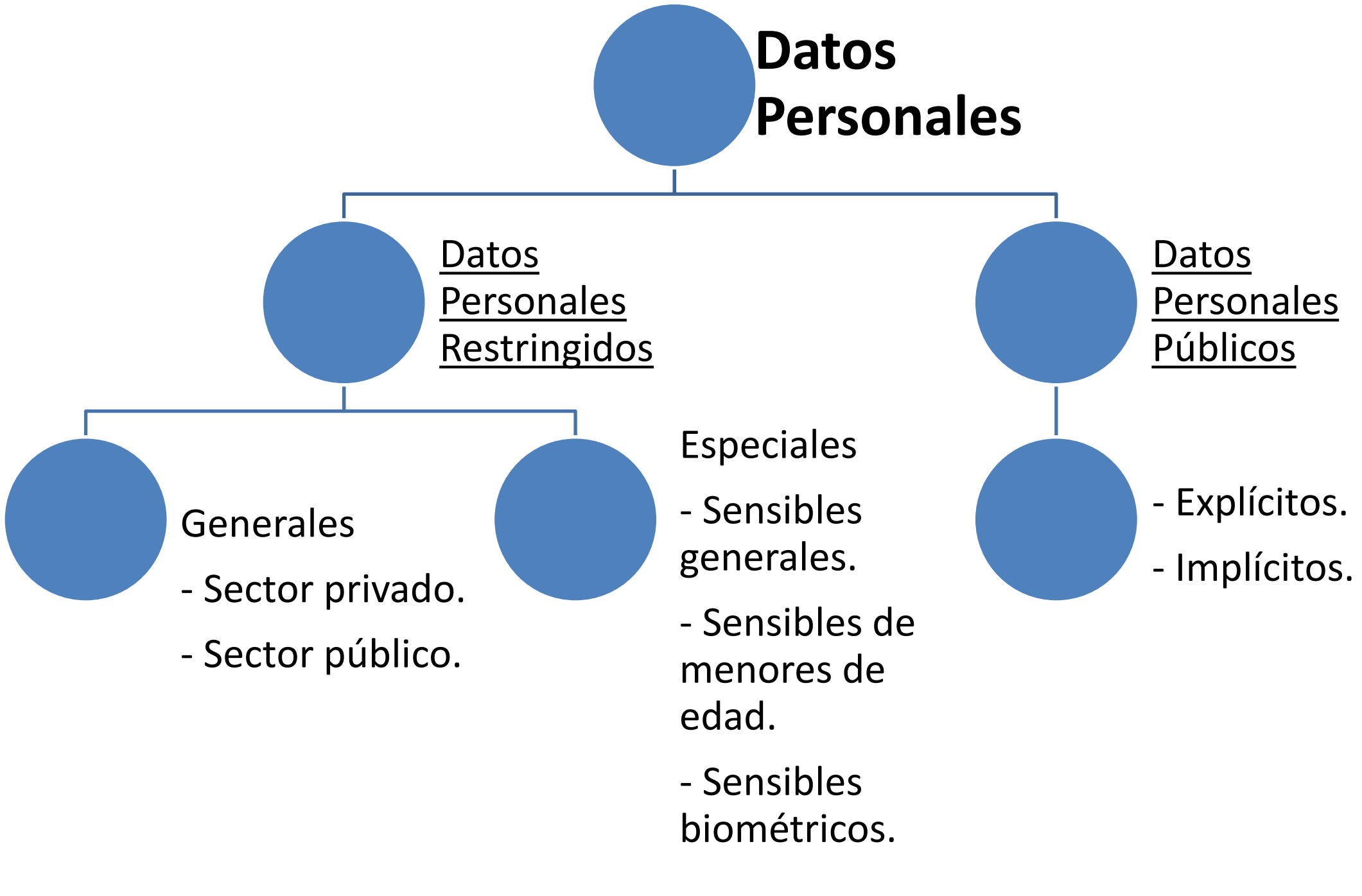
Definiciones Relevantes

Información Personal: Todo dato o conjunto de datos que se asocian o vinculan con una persona natural.

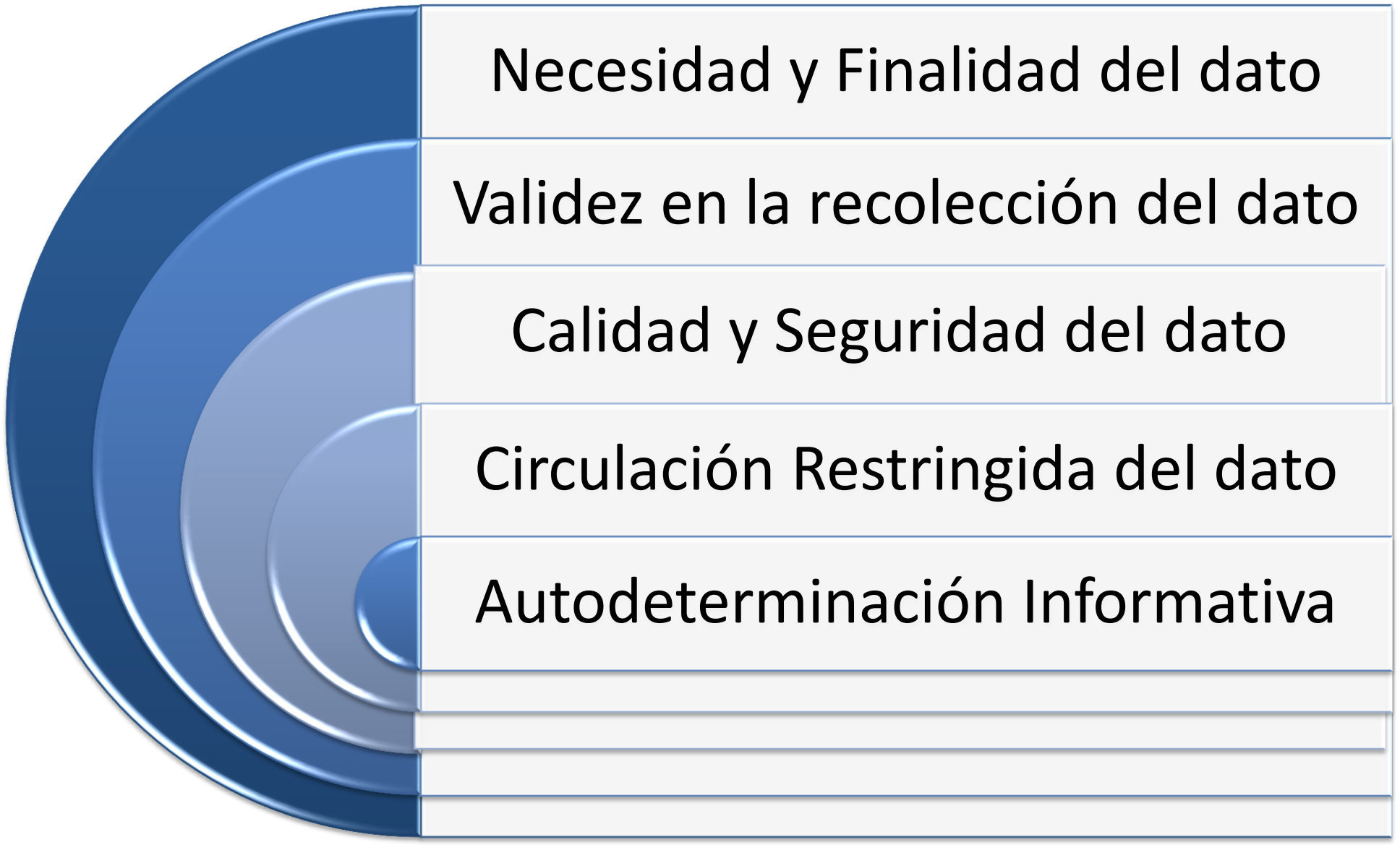
Información Personal Pública: Toda información personal cuyo tratamiento se puede realizar sin contar con la autorización del titular, pero que en todo caso se debe tratar con base en los lineamientos, deberes y principios consagrados en la Ley 1581 de 2012 y sus Decretos Reglamentarios.

Información Personal Restringida: Toda información personal cuyo tratamiento solo se puede realizar si se cuenta con la autorización previa, expresa e informada del titular (aquí se incluye a los **Datos Sensibles**, que son todos aquellos que puedan causar un tratamiento desigual, limitativo o degradatorio de los derechos del titular. Igualmente se incluye como Datos Sensibles a los **Datos de Menores de Edad** y a los **Datos Biométricos**, cuyo tratamiento solo se puede realizar si se autoriza expresamente -y en el caso de los menores de edad la autorización la debe hacer el representante formal del menor de edad, previo a escucharse la opinión del menor acerca del tratamiento que se solicita-).

CLASIFICACIÓN DE LOS DATOS PERSONALES



PRINCIPIOS MEDULARES PARA EL TRATAMIENTO DE DATOS PERSONALES



Ley 1581 de 2012

PRINCIPIOS JURÍDICOS PARA EL TRATAMIENTO DE INFORMACIÓN PERSONAL

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

Ley 1581 de 2012

PRINCIPIOS JURÍDICOS PARA EL TRATAMIENTO DE INFORMACIÓN PERSONAL

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

Ley 1581 de 2012

PRINCIPIOS JURÍDICOS PARA EL TRATAMIENTO DE INFORMACIÓN PERSONAL

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

Ley 1581 de 2012

PRINCIPIOS JURÍDICOS PARA EL TRATAMIENTO DE INFORMACIÓN PERSONAL

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Ley 1581 de 2012

OTROS PRINCIPIOS CONSAGRADOS EN LA SENTENCIA C-748 DE 2011

1) Principios derivados directamente de la Constitución: (i) la prohibición de discriminación por las informaciones recaudadas en las bases de datos, **(ii)** el principio de interpretación integral de los derechos constitucionales y **(iii)** la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración de datos.

2) Principios derivados del núcleo temático del proyecto de ley estatutaria: (i) principio de la proporcionalidad del establecimiento de excepciones, **(ii)** principio de autoridad independiente, y **(iii)** principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos.

NORMATIVIDAD PRINCIPAL DIRECTA

- **Constitución Política de Colombia de 1991** (incluyendo el bloque de constitucionalidad)

- **Ley 1581 de 2012** – Ley general de protección de datos personales.

- **Decreto 1377 de 2013** – Reglamenta en términos generales a la Ley 1581 de 2012.

- **Decreto 886 de 2014** – Reglamenta a la Ley 1581 de 2012 en relación con el Registro Nacional de Bases de Datos Personales (RNBD).

- **Decreto 1074 de 2015** – Unifica todos los Decretos Reglamentarios de la Ley 1581 de 2012, se encuentran en el capítulo 25 de éste Decreto.

- **Ley 1266 de 2008 (y sus Decretos Reglamentarios)** – Habeas Data Financiero.

- **Ley 1712 de 2014** – Ley de Transparencia y de Acceso a la Información Pública.

- **Circular Externa No. 02 del 3 de noviembre de 2015 de la SIC** – Instrucciones a ciertos Responsables del Tratamiento para la inscripción de sus bases de datos en el RNBD.

NORMATIVIDAD PRINCIPAL

- **Circular Única de la Superintendencia de Industria y Comercio** – Establece pautas en diferentes temas, entre ellos sobre habeas data financiero en el capítulo V.

- **Acuerdo 003 de 2015, Archivo General de la Nación** – Lineamientos para las entidades del Estado en relación a los documentos electrónicos generados como resultado del uso de medio electrónicos.

- **Resolución SIC 8934 de 2014** – Establece directrices sobre gestión documental y organización de archivos para los vigilados por la SIC.

- **Guía de la SIC para la implementación del Principio de Responsabilidad Demostrada (Accountability)** – Brinda buenas prácticas y parámetros para aplicar y demostrar debida diligencia en protección de datos personales.

- **Manual de Usuario del Registro Nacional de Bases de Datos – RNBD** – Dicta los lineamientos y pasos para registrar bases de datos ante la SIC.

- **Reglas de Heredia** – Reglas mínimas para la difusión de Información Judicial en Internet (TEMA VINCULADO CON EL **DERECHO AL OLVIDO EN INTERNET**, VER **SENTENCIA T-040 DE 2013**).

NORMATIVIDAD PRINCIPAL

- **Código Civil** – Dicta las pautas generales de la diligencia.

- **Código de Procedimiento Administrativo y de los Contencioso Administrativo** – Señala las pautas de diligencia en el desarrollo de la función administrativa.

- **Leyes 57 y 153 de 1887** – Sobre aplicación de las Leyes.

- **Legislación Especial** (ej. Ley 489 de 1998 sobre la función administrativa) **o General y Regulación sectorial** (ej.: salud).

FUENTES DEL DERECHO

FUENTES JURÍDICAS

- **CONSTITUCIÓN POLÍTICA** (INCLUÍDO EL BLOQUE DE CONSTITUCIONALIDAD).
- **NORMATIVIDAD** (NACIONAL, EXTRANJERA E INTERNACIONAL).
- **LEGISLACIÓN ESPECIAL** (particular, ej. Normatividad aplicable a la Registraduría Nacional del Estado Civil , - Ley de Ética Médica, art. 34, o general, ej. Ley General de Archivos) **Y REGULACIÓN SECTORIAL** (ej. Resolución 1995/95 MIN. SALUD sobre disposiciones para el manejo de la histórica clínica).
- **AUTORREGULACIÓN.**
- **CASO CONCRETO.**

NORMATIVIDAD PRINCIPAL

- **Principios Generales del Derecho.**
- **Sentencias Judiciales y Fallos Administrativos.**
- **Normatividad Extranjera.**
- **Doctrina – Lógica – Argumentación – Fuentes Auxiliares Idóneas.**
- **Autorregulación.**
- **Casos Concretos.**

REFLEXIÓN

SIN AXIOMAS NO HAY TEOREMAS

Los axiomas son las reglas y principios jurídicos, y el teorema es cada ecosistema de derecho preventivo que se diseña para cada proyecto de TIC

Ley 1581 de 2012

CONTENIDO:

1. Título I. Objeto, ámbito de aplicación y definiciones.

2. Título II. Principios rectores.

3. Título III. Categorías especiales de datos.

4. Título IV. Derechos y condiciones de legalidad para el tratamiento de datos.

5. Título V. Procedimientos.

6. Título VI. Deberes de los responsables del tratamiento y encargados del tratamiento.

Ley 1581 de 2012

CONTENIDO:

7. Título VII. De los mecanismos de vigilancia y sanción.

Se divide en:

- CAPÍTULO I. De la autoridad de protección de datos.
- CAPÍTULO II. Procedimiento y sanciones.
- CAPÍTULO III. Del Registro Nacional de Bases de Datos.

8. Título VIII. Transferencia de datos a terceros países.

9. Título IX. Otras disposiciones.

Decreto 1377 de 2013

CONTENIDO:

1. Considerandos.
2. Capítulo I. Disposiciones generales.
3. Capítulo II. Autorización.
4. Capítulo III. Políticas de tratamiento.
5. Capítulo IV. Ejercicio de los derechos de los titulares.
6. Capítulo V. Transferencias y transmisiones internacionales de datos personales.
7. Capítulo VI. Responsabilidad demostrada frente al tratamiento de datos personales.

Decreto 1377 de 2013

CAPÍTULO VI. RESPONSABILIDAD DEMOSTRADA FRENTE AL TRATAMIENTO DE DATOS PERSONALES

1. DEMOSTRACIÓN (la compañía debe demostrar su debida diligencia según su tamaño empresarial -MICRO, PYME, GRANDE EMPRESA-, de conformidad con lo consagrado en la Ley 905 de 2004).

2. POLÍTICAS INTERNAS EFECTIVAS (hace referencia al modelo de autorregulación sobre protección a la información personal en la compañía).

Decreto 886 de 2014

CONTENIDO:

1. Considerandos.

2. Capítulo I. Disposiciones generales.

3. Capítulo II. Del Registro Nacional de Bases de Datos.

4. Capítulo III. Términos y condiciones de inscripción en el Registro Nacional de Bases de Datos.

Decreto 886 DE 2014

REGISTRO NACIONAL DE BASES DE DATOS EN COLOMBIA

1. Todas las bases de datos existentes de forma previa a la fecha en que la Superintendencia de Industria y Comercio ponga en operación el registro nacional de bases de datos se deberán registrar dentro del año siguiente a esa fecha en que inicie a operar el registro nacional de bases de datos.

2. Las nuevas bases de datos creadas desde que la Superintendencia de Industria y Comercio ponga en operación el registro nacional de bases de datos se deberán registrar dentro de los dos meses siguientes a su respectiva creación.

Circular Externa No. 02 del 3 de noviembre de 2015 de la SIC

- Indica algunas instrucciones que deben seguir los responsables y encargados del tratamiento de datos personales para inscribir sus bases de datos ante el Registro Nacional de Bases de Datos.

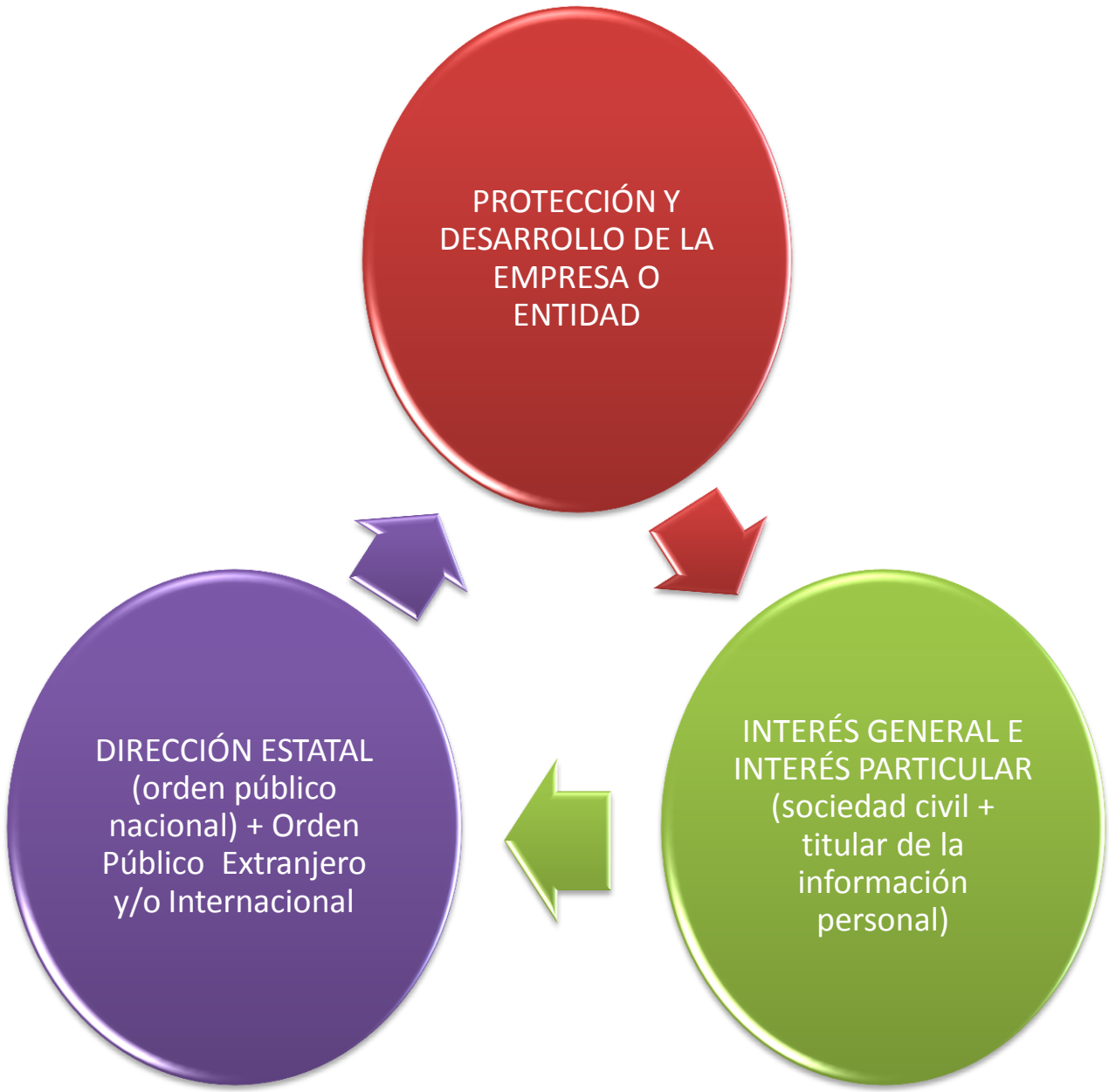
- Sólo aplica a las personas jurídicas de naturaleza privada inscritas en las Cámaras de Comercio y a las sociedades de economía mixta.

- Desde el 9 de noviembre de 2015 inició el deber de inscripción de bases de datos por parte de dichos perfiles específicos de Responsables del tratamiento.

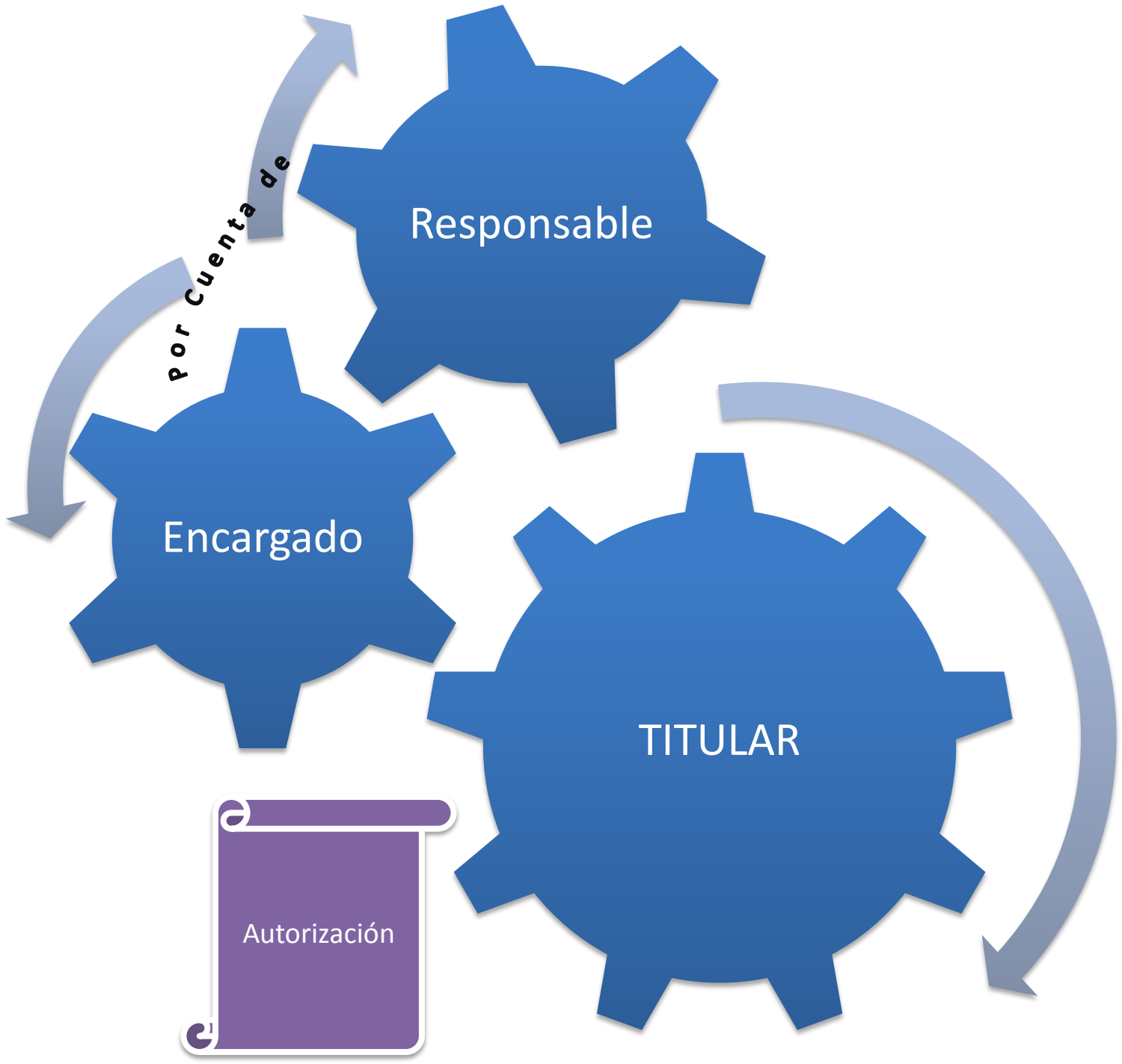
- En una norma posterior la Superintendencia de Industria y Comercio (SIC) tiene que indicar las instrucciones para los demás Responsables del tratamiento que se encuentren sujetos a su competencia.

Reflexión y Mensaje Contundente

RELACIÓN JURÍDICA ESPERADA CON UN MODELO DE AUTORREGULACIÓN DE DERECHO PREVENTIVO DE PROTECCIÓN Y USO DE DATOS PERSONALES



RELACIÓN TITULAR-RESPONSABLE-ENCARGADO



MODELO DE RECOLECCIÓN DE LA INFORMACIÓN PERSONAL

Requisitos de la autorización de acuerdo con cada titular

Requieren de

Autorización

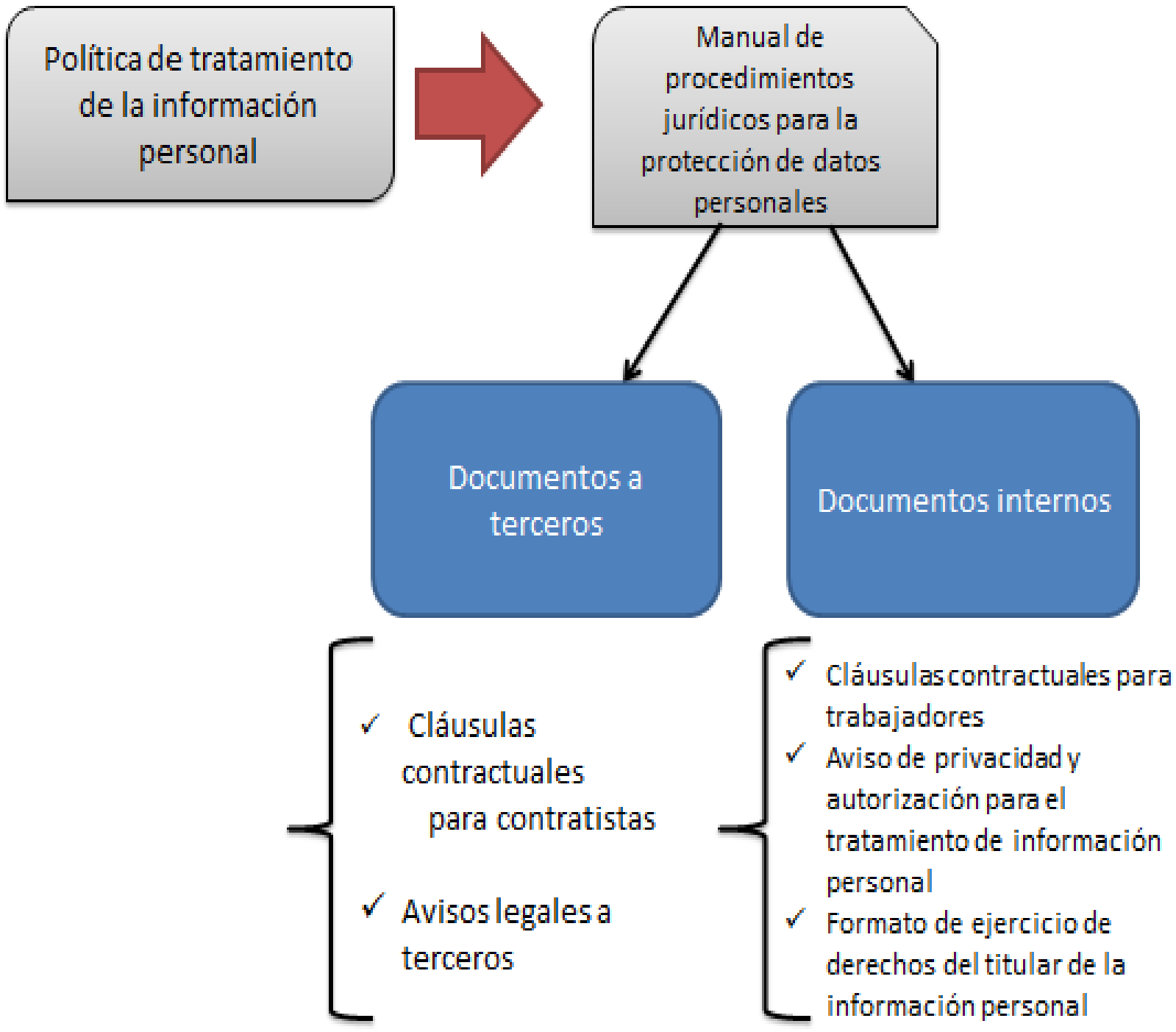
Para recolectar información de

- Trabajadores y contratistas → Cláusulas contractuales
- Incapaces legales → Representante acreditado
- Incapaces legales → Derecho de ser oído en caso de ser menor de edad
- Otros Titulares → Previa, expresa e informada

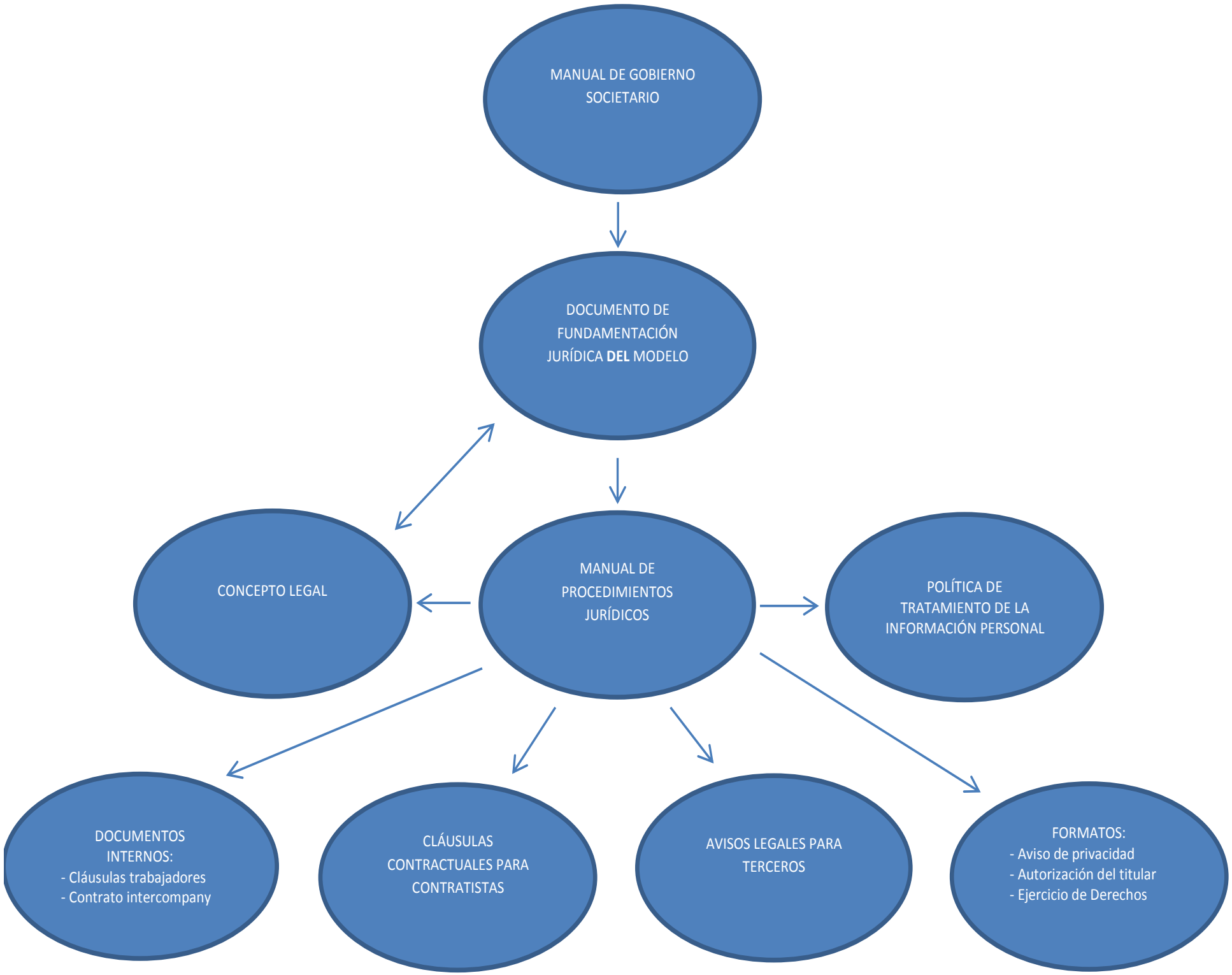
- ✓ Informar que no está obligado
- ✓ Informar la finalidad
- ✓ No condicionar el consentimiento del titular

MODELO OPERATIVO PARA LA ATENCIÓN DE CONSULTAS Y RECLAMOS DEL TITULAR

ILUSTRACIÓN DE UN MODELO DE AUTORREGULACIÓN GENERAL



EL MODELO DE AUTORREGULACIÓN JURÍDICA PRINCIPAL -DETALLADO-



REFLEXIÓN

SIN AXIOMAS NO HAY TEOREMAS

Los axiomas son las reglas y principios jurídicos, y el teorema es cada ecosistema de derecho preventivo que se diseña para cada proyecto o gestión con el fin de brindar un adecuado, oportuno, integral y eficaz cumplimiento de dichas normas.

Implicaciones principales en los medios digitales

¿EXISTE UN CLARO, SUFICIENTE, COHERENTE Y ADECUADO RÉGIMEN JURÍDICO APLICABLE A LAS TIC?

- **Regulación por servicios** (Decreto-Ley 1900 de 1990, clasifica los servicios de telecomunicaciones de manera taxativa en: básicos, de difusión, de valor agregado, auxiliares o de ayuda, y especiales).

- **Regulación transversal** (brinda pautas generales que deben cumplirse según los mercados relevantes o contextos involucrados - Leyes 527 de 1999 y 1341 de 2009).

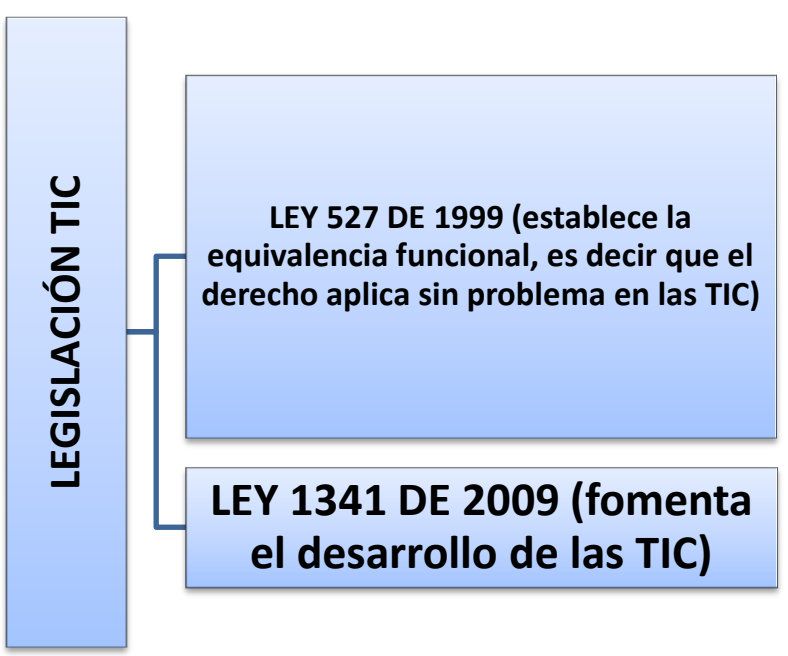
PRINCIPIOS JURÍDICOS

- Existe una **Equivalencia Funcional** entre el Medio Físico y el Medio Digital, es decir que el derecho aplica en cualquier clase de medio, como lo son las TIC. Va ligado al principio de **Prevalencia del Derecho Preexistente y al de Buena Fe**.

- El derecho aplica con **Neutralidad Tecnológica** (el derecho aplica sin importar la clase de tecnología que esté involucrada, es decir que aplica a cualquier clase de TIC).

- Se debe tener en cuenta la **Internacionalidad** (es decir que si se causan efectos en ámbitos internacionales se debe cumplir con las normas internacionales que le sean aplicables).

- **Neutralidad de la Red** (según cada clase de proyecto de TIC se debe balancear el nivel de control con el nivel de libertad).



EL MENSAJE DE DATOS (LEY 527 DE 1999)

- **DEFINICIÓN:** Cualquier audio, voz, imagen o texto generado, soportado y, en general, gestionado en un medio o elemento digital.

- **CLASES DE MENSAJES DE DATOS:**

a). Original.

b). Derivado.

- **REQUISITOS DE LOS MENSAJES DE DATOS:**

a). Integridad.

b). Autenticidad.

c). No repudiación.

d). El cumplimiento de los requisitos esenciales, naturales y/o accidentales del silogismo o silogismos jurídicos que se van a emplear, o que están involucrados materialmente, para la producción de un determinado negocio jurídico.

ANÁLISIS DEL PRINCIPIO DE EQUIVALENCIA FUNCIONAL

Clases de Mensajes de Datos

- a) Originalmente electrónico.
- b) Derivado.

EQUIVALENCIA FUNCIONAL

Equivalentes funcionales	• **REQUISITOS**
Escrito = Mensaje de Datos	• Integridad, autenticidad y no repudiación + Trazabilidad + Posterior Consulta.
Original = Integridad	• Integridad, autenticidad y no repudiación + Trazabilidad + Posterior Consulta.
Firma = Autenticidad y no repudio	• Integridad, autenticidad y no repudiación + Trazabilidad + Posterior Consulta.
Archivo y conservación = Archivo digital	• Integridad, autenticidad y no repudiación + Trazabilidad + Posterior Consulta + Estampado Cronológico.

SOBRE LOS CERTIFICADOS DIGITALES (Parte III, Capítulo III, Ley 527 de 1999)

ARTÍCULO 35. Contenido de los certificados. *Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:*

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.

SOBRE LA GESTIÓN DE ONAC EN RELACIÓN CON LAS ENTIDADES DE CERTIFICACIÓN DIGITAL

"ONAC informa que a partir del 18 de Agosto de 2015, pone a disposición de los interesados el programa de acreditación para ENTIDADES DE CERTIFICACIÓN DIGITAL – ECD quienes podrán acreditar sus servicios de certificación digital en el marco de la ***Ley 527 de 1999****,* ***Decreto Ley 0019 de 2012****,* ***Decreto 333 de 2014****, el* ***Decreto 1471 de 2014****, los* ***Criterios Específicos de Acreditación CEA-4.1-10****, y a lo dispuesto el 22 de abril de 2015 por la Corte Constitucional en* ***sentencia C-219/15****, que declaró exequibles los artículos 160 a 163 del Decreto Ley 0019 de 2012, relacionados con la acreditación de las entidades de certificación Digital "por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública". Este fallo de la Corte reconoce con claridad indiscutible la función acreditadora, en manos de ONAC, para la República de Colombia.*

Las ECD interesadas en el proceso de acreditación deberán presentar la solicitud respectiva, descargando y presentado el formulario e información anexa en el siguiente vínculo: http://www.onac.org.co/modulos/contenido/default.asp?idmodulo=235 "

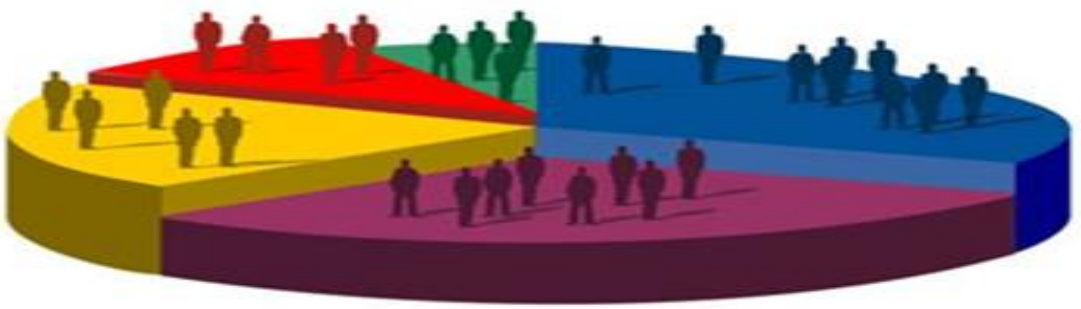
SOBRE LA GESTIÓN DE ONAC EN RELACIÓN CON LAS ENTIDADES DE CERTIFICACIÓN DIGITAL

Los Criterios Específicos de Acreditación CEA-4.1-10 se encuentran disponibles en el siguiente enlace: *http://www.onac.org.co/anexos/documentos/CEAs/CEA-4%201-10%202015-02-02%20en%20consulta%20p%C3%BAblica%20v%2001.pdf Último acceso: 24 de agosto de 2016 a las 5:00 p.m.*

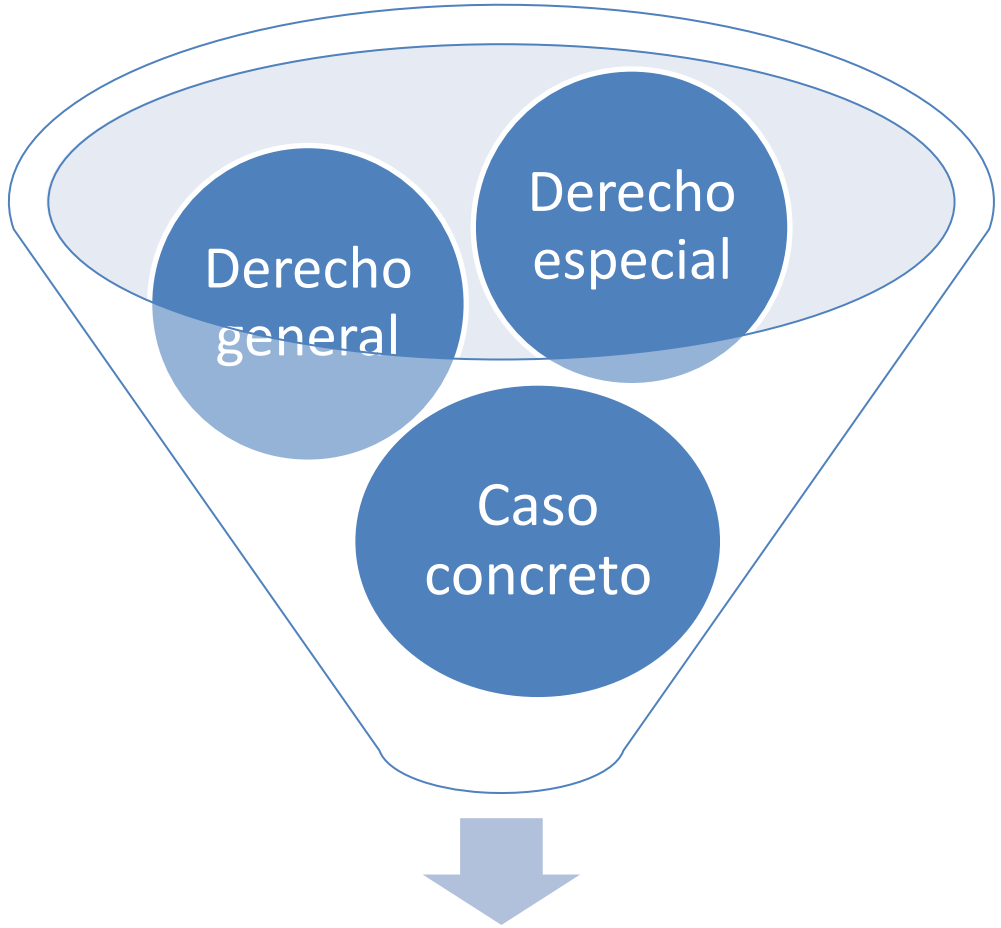
ENTONCES ¿CÓMO SE APLICA EL DERECHO PREVENTIVO EN LOS PROYECTOS DIGITALES?

DETECTANDO Y ATIENDO EL SEGMENTO DE CADA PROYECTO, Y SEGÚN LAS VARIABLES QUE SE DETECTEN SE SABRÁ CUÁL ES LA NORMATIVIDAD QUE LE APLICA Y SE DISEÑARÁN SOLUCIONES JURÍDICAS A LA MEDIDA.

- Mercado Territorial
- Mercado de Producto
- Clase de Modelo de Negocio o Gestión
- Perfil de los Usuarios



SE DEBE ATERRIZAR EL DERECHO A LA MEDIDA DE LAS VARIABLES DE CADA PROYECTO DE TIC -ES DECIR QUE EL ABOGADO Y EN GENERAL LA HUMANIDAD DEBE DESARROLLAR COMPETENCIAS Y HABILIDADES PARA ATENDER ESTOS FENÓMENOS, PERO NO REPLANTEAR RADICALMENTE TODO-



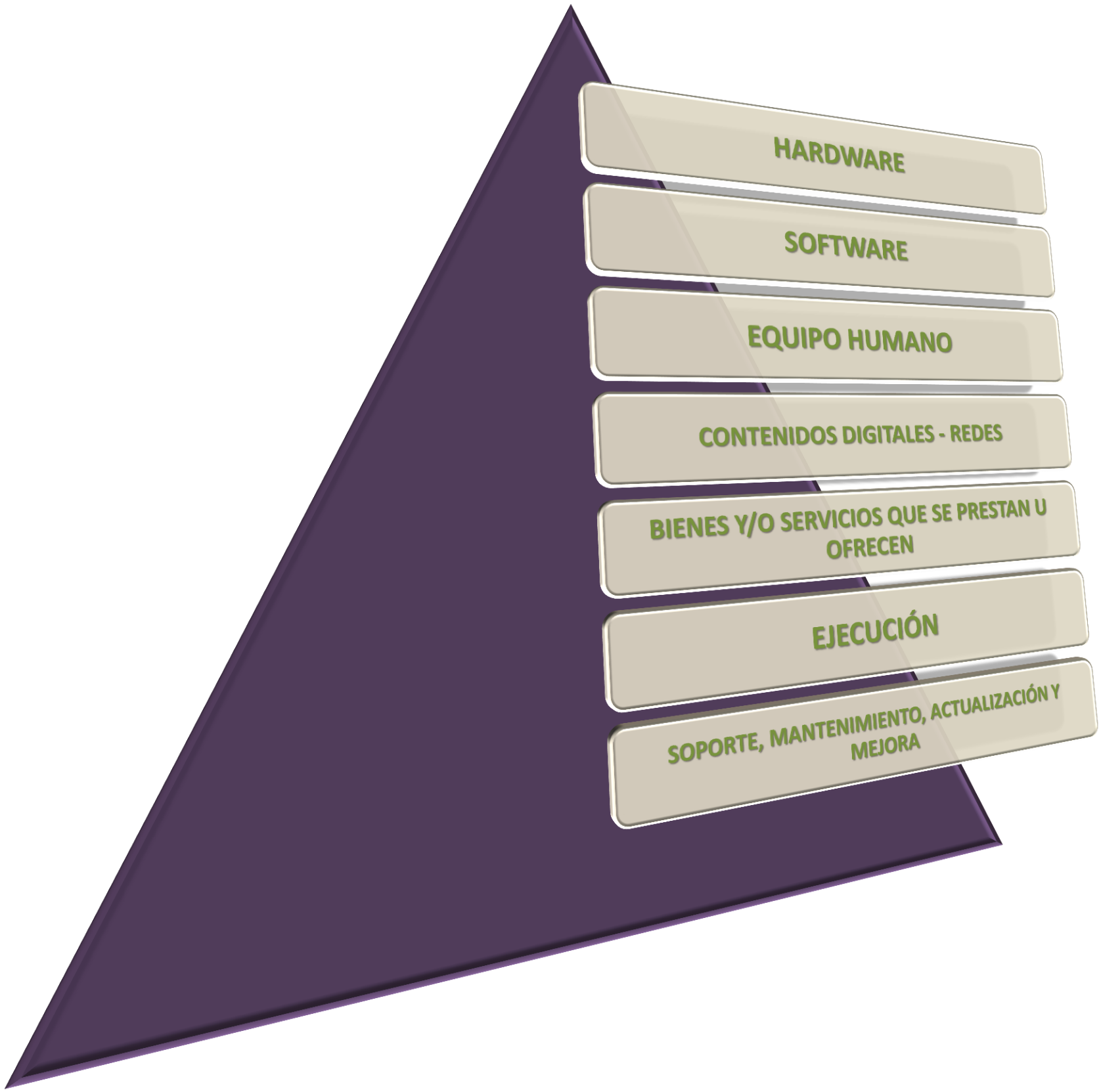
DERECHO PREVENTIVO EN CADA PROYECTO DE TIC

REFLEXIÓN

SIN AXIOMAS NO HAY TEOREMAS

Los axiomas son las reglas y principios jurídicos, y el teorema es cada ecosistema de derecho preventivo que se diseña para cada proyecto digital.

COMPONENTES DE UN PROYECTO TECNOLÓGICO



PRINCIPIO DE HUMANIZACIÓN DE LAS TIC

- Analista de riesgos-planeador
- Programador
- Desarrollador
- Consultor experto
- Planta administrativa y operativa

- Outsourcing
- Aliados
- Auditor
- Certificador
- Consumidor
- Control Público

EL DILEMA

¿Debo permitirlo todo?

¿Debo controlarlo todo?

LA LIBERTAD DE EMPRESA (OBJETO, CONTENIDO Y ALCANCE)

CONSTITUCIÓN POLÍTICA DE COLOMBIA

*ARTÍCULO 333. "**La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley.***

La libre competencia económica es un derecho de todos que supone responsabilidades.

La empresa, como base del desarrollo, tiene una función social que implica obligaciones. El Estado fortalecerá las organizaciones solidarias y estimulará el desarrollo empresarial.

LA EMPRESA

- **Definición** (art. 25, Código de Comercio): *Se entenderá por empresa toda actividad económica organizada para la producción, transformación, circulación, administración o custodia de bienes, o para la prestación de servicios. Dicha actividad se realizará a través de uno o más establecimientos de comercio.*

- **Formas de desarrollar una empresa:**

a) Comerciantes (ej.: ser agente comercial para comercializar los productos de una empresa).

b) Sociedades (ej.: una sociedad por acciones simplificada, S.A.S.).

c) Asociaciones (ej.: alianzas).

NORMATIVIDAD PRINCIPAL APLICABLE A LA EMPRESA

- **Constitución Política de 1991** (incluyendo el bloque de constitucionalidad).

- **Código Civil y de Comercio** – Dictan las pautas generales de la diligencia.

- **Normas generales o especiales que apliquen en cada caso concreto.**

LÍMITES A LA LIBERTAD DE EMPRESA

- ABUSO DEL DERECHO (CONCEPCIÓN INDIVIDUALISTA DE DERECHO).

- FUNCIÓN SOCIAL DE LA PROPIEDAD Y DEL DERECHO EN GENERAL (CONCEPCIÓN SOCIAL Y COLECTIVISTA DEL DERECHO).

Ambas concepciones aplican para establecer, según las variables de cada caso, los límites a la libertad de empresa.

CRITERIOS PARA LA LIBERTAD DE EMPRESA

- PROFESIONALISMO EN EL DESARROLLO DE ACTOS DE COMERCIO.

- HABITUALIDAD (EXPERIENCIA EN EL RAMO).

- SE RESPONDE POR LO PREVISIBLE NO POR LO IRRESISTIBLE.

ENTONCES, SURGE ESTE DILEMA EN LA RESPONSABILIDAD INSTITUCIONAL

O protejo a la empresa o entidad

O protejo a los grupos de interés de la empresa o entidad (usuarios, proveedores, aliados, entidades estatales, competidores, comunidad de impacto, etc.)

FASES PRINCIPALES DEL DERECHO PREVENTIVO EN LAS TIC

Fase 1. Se detectan los Componentes del Proyecto (tipos de datos, hardware, software, multimedia, redes, modelo de gestión, proveedores, aliados, usuarios, normatividad aplicable, etc.)

Fase 2. Esos componentes se atienden mediante el diseño de Instrumentos Jurídicos Preventivos

Fase 3. Se brinda seguridad y confianza jurídica a Usuarios, Proveedores, Aliados y Estados involucrados, y valor agregado y competitividad al proyecto .

AQUÍ ESTÁ EL DERECHO PREVENTIVO QUE SE PROPONE

Disminución de Riesgos de Daño

Disminución de Amenazas de Daño

Aumentando la Competitividad, Seguridad, Confianza, Validez y Generación de Valor en el Proyecto

AQUÍ ESTÁ EL DERECHO PREVENTIVO QUE SE PROPONE

Producción de soluciones jurídicas preventivas, prospectivas, válidas, eficientes, y que generan valor agregado a las gestiones digitales (y físicas) a la medida de cada proyecto

LA SUPERACIÓN DEL DILEMA

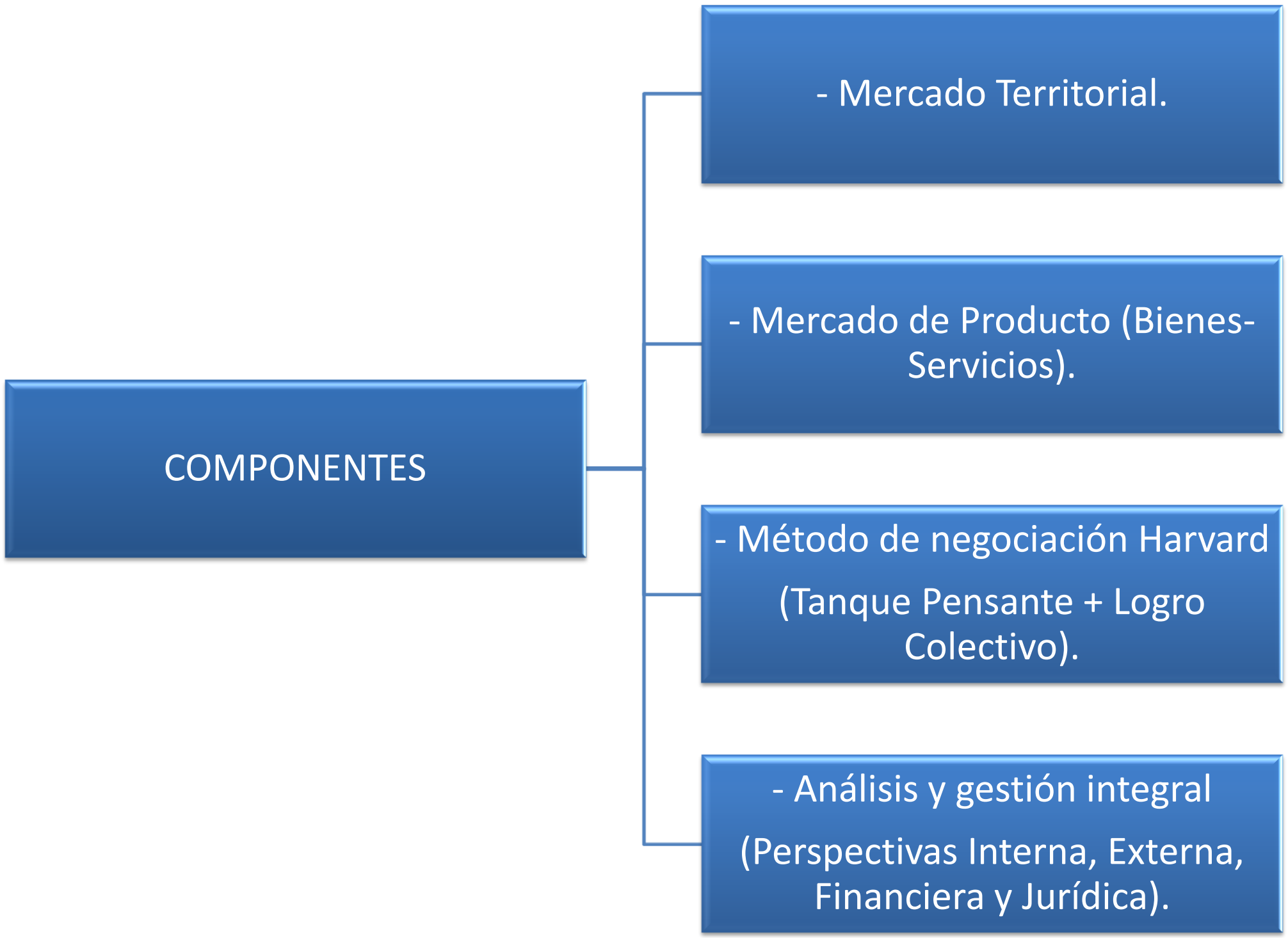
Logrando un balance entre libertad y control según las variables presentes en cada proyecto o gestión (tipo de modelo de negocio, modelo de operación, modelo de gestión, sector o sectores involucrados, perfiles de usuarios, contenidos, datos, información, normas generales y especiales aplicables, territorios penetrados, etc.)

ENTONCES ¿CÓMO SE APLICA EL DERECHO PREVENTIVO EN LA GESTIÓN DE DATOS PERSONALES DIGITALES?

DETECTANDO Y ATIENDO EL SEGMENTO DE CADA PROYECTO, Y SEGÚN LAS VARIABLES QUE SE DETECTEN SE SABRÁ CUÁL ES LA NORMATIVIDAD QUE LE APLICA Y SE DISEÑARÁN SOLUCIONES JURÍDICAS A LA MEDIDA.

- Mercado Territorial
- Mercado de Producto
- Clase de Modelo de Negocio o Gestión
- Perfil de los Usuarios

LA REGULACIÓN Y AUTORREGULACIÓN POR MERCADOS O CONTEXTOS RELEVANTES EN EL SECTOR TIC



LA SUPERACIÓN DEL DILEMA

Diseñando modelos de Derecho Preventivo que protegen y generan eficiencia tanto a la empresa o entidad como a los demás grupos de interés (consumidores, proveedores, aliados, comunidad, etc.)

GENERNANDO LOGRO COLECTIVO GANA-GANA

Video

COMO VE EL DERECHO PREVENTIVO BRINDA VALIDEZ Y EFICACIA JURÍDICA

El Derecho Preventivo no es un gasto, es una inversión que brinda múltiples beneficios tanto para el que produce y/o provee un proyecto digital como para quienes lo emplean ya que permite cumplir de forma integral, oportuna y creativa con los diferentes deberes y derechos que estén involucrados en un proyecto -es decir que creamos ecosistemas jurídicos donde se vive, se cumple y se disfruta el derecho en cada Proyecto-, generando un esquema **GANA-GANA**, dándole un atractivo y diferenciador excelente al Proyecto o Gestión, y facilitando su ejecución.

EL DERECHO PREVENTIVO REQUIERE ESFUERZO

“19. Nanpu Bridge. Es una más de las obras maestras de China. Se encuentra en Shanghai, uno de los puntos tecnológicos más importantes del mundo. Asómbrate con su compleja construcción”. Texto e Imagen disponibles en: http://www.taringa.net/post/imagenes/13703319/Los-20-Puentes-mas-Famosos-del-Mundo.html Último acceso: 24 de agosto de 2016 a las 4:00 p.m.

LA CONSTRUCCIÓN DE UNA BUENA OBRA ES COMPLEJA. EN EL DERECHO PREVENTIVO SE DEBEN ARMONIZAR TODAS LAS VARIABLES INVOLUCRADAS.

EL DERECHO PREVENTIVO CONSISTE EN HILAR FINO (DELGADO)

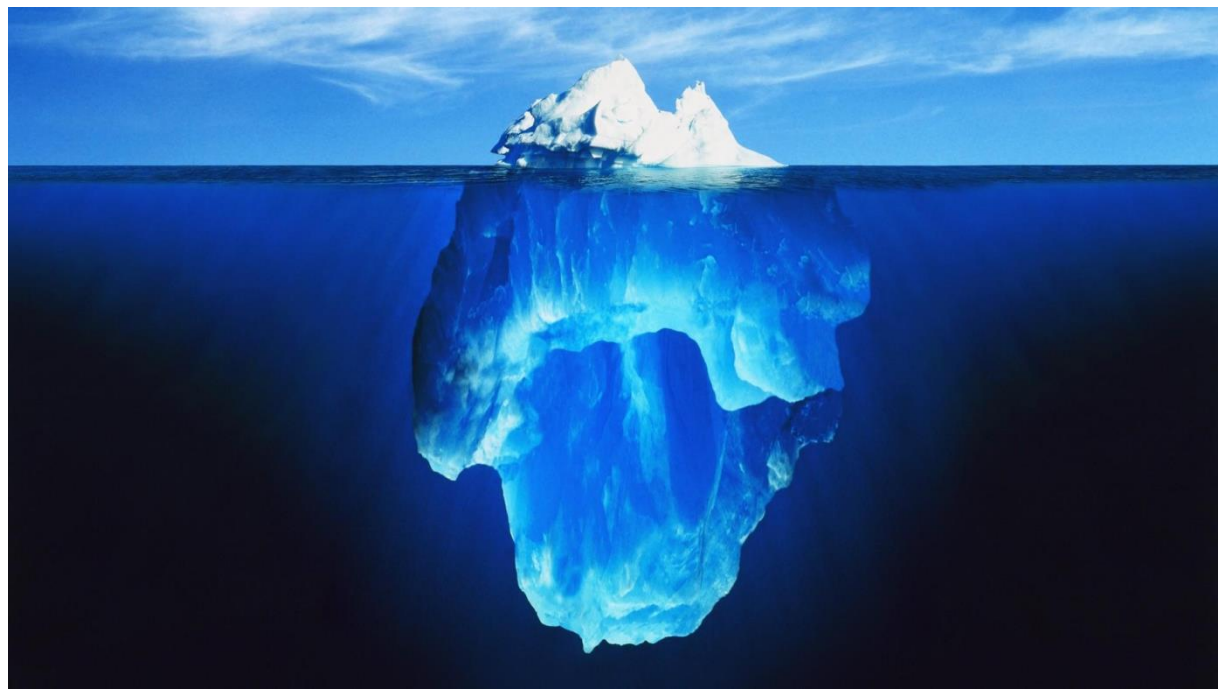
SE DEBE SER MINUCIOSO PARA PODER DETECTAR, ATENDER Y ARMONIZAR IDÓNEAMENTE -Y DE FORMA FLUÍDA Y COHERENTE CON EL CONTEXTO DIGITAL INVOLUCRADO- TODAS LAS VARIABLES INVOLUCRADAS EN CADA CASO CONCRETO. ASÍ SE LOGRA LA VALIDEZ Y LA EFICACIA JURÍDICA.

LO SIMPLE ES LO PROFUNDO

VÍDEO ILUSTRATIVO

EN EL DERECHO PREVENTIVO SE DEBEN PRESENTAR SOLUCIONES INTEGRALES Y SISTEMÁTICAS PERO MINIMALISTAS PUES DEBEN SER COHERENTES CON EL CONTEXTO DIGITAL.

SE DEBE TRANSMITIR LO RELEVANTE, ES DECIR LOS ELEMENTOS ESENCIALES, NATURALES Y ACCIDENTALES DE PROTECCIÓN DE DATOS PERSONALES EN CADA ACTO O NEGOCIO JURÍDICO INVOLUCRADO. SE DEBEN GENERAR ECOSISTEMAS SIMILARES A UN **ICEBERG** (SE OBSERVA LO SENCILLO PERO EXISTE UN TRASFONDO ROBUSTO):



EJEMPLOS DE ALGUNOS INSTRUMENTOS DE DERECHO PREVENTIVO PARA LA GESTIÓN DE LOS DATOS PERSONALES DIGITALES:

1. Códigos de ética (aprobados por mayorías para que sean vinculantes jurídicamente).
2. Términos y Condiciones de Uso (manual de usuario).
3. Políticas de Protección de Datos Personales.
4. Contratos a la medida de las Gestiones que se Desarrollen.
5. Documentos Jurídicos de Seguridad de la Información.
6. Manuales de Buenas Prácticas Jurídicas en diferentes temáticas.
7. Garantías y Acuerdos de Niveles del Servicio.

EJEMPLOS DE ALGUNOS INSTRUMENTOS DE DERECHO PREVENTIVO PARA LA GESTIÓN DE LOS DATOS PERSONALES DIGITALES:

1. Protección de la Propiedad Intelectual presente en los proyectos.

2. Marcas de certificación, sellos de confianza y en general mecanismos autorregulatorios.

3. Ecosistemas jurídicos preventivos para proyectos de Tecnologías de la Información (T.I.) y Telecomunicaciones.

4. Modelos Completos de Derecho Preventivo para todo un proyecto de TIC, o para atender puntos o temas específicos del proyecto.

5. Capacitación (generación de cultura de derecho preventivo).

6. ETC.

Recomendaciones de derecho preventivo

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN S.G.S.I. (Video ilustrativo I – Video ilustrativo II)

- INTRODUCCIÓN.
- NORMA ISO 27001 (información, actividad, y acceso + Planear, Hacer, Verificar, y Actuar).
- AUTORES (categoría general: Hackers y Bandabs).
- PRINCIPALES FORMAS DE ATAQUE (interrupción, interceptación, modificación, y fabricación).
- MODELOS DE PROTECCIÓN (host – network).
- NUEVOS INJUSTOS PENALES (Ley 1273 de 2009).
- OTRA NORMA DE REFERENCIA PARA LA DILIGENCIA: CONPES 3854 – POLITICA NACIONAL DE SEGURIDAD DIGITAL.

Ley 1273 de 2009, Artículo 269F: ***"Violación de datos personales.*** *El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".*

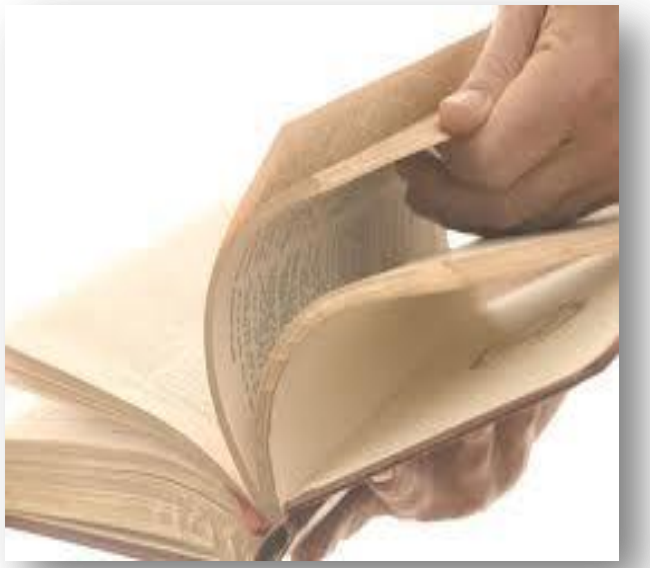
PRINCIPALES HERRAMIENTAS DE DERECHO PREVENTIVO EN LAS TIC

Desarrollo de instrumentos de derecho preventivo, tales como:

Herramientas de Derecho Preventivo

- Declaraciones de buenas prácticas
- Diseño de garantías sobre los bienes y/o servicios involucrados (ACUERDOS DE NIVELES DEL SERVICIO)
- Manual de gobierno societario (Ley 222 de 1995)
- Retroalimentación continua / Marcas de certificación
- Diseño e implementación de adecuadas medidas de seguridad y gestión (técnicas y jurídicas) a nivel electrónico y físico.

Manual de Gobierno Societario o Institucional: Deberá contener las políticas generales de la compañía en materia de:

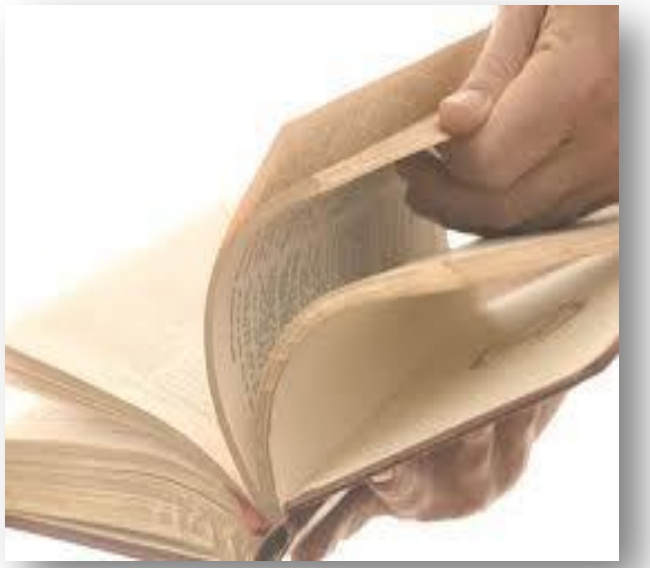


- Protección del interés de la compañía o entidad frente al de los socios o funcionarios.

- Protección al consumidor o usuario.

- Protección al medio ambiente.

Manual de Gobierno Societario o Institucional:



- Protección de la información (pública o restringida, bien sea gubernamental, empresarial o personal).

- Protección de los compromisos económicos de la compañía o entidad.

- Planes de crecimiento sostenible, creativo, rentable, competitivo, leal y prospectivo de la compañía o entidad.

Adecuados procesos de Selección y adecuado Contrato individual y/o colectivo -o convenio- de trabajo.

Establece los derechos, deberes y funciones a cargo de un miembro determinado a interior de la organización.

En seguridad de la información, protección al usuario y protección de datos personales se deberá brindar un claro soporte de las atribuciones y restricciones que posee un miembro de la compañía al interior de la misma en el ejercicio de sus funciones.

Acuerdo de confidencialidad

Documento que establece las restricciones en el uso de la información, bien sea en la fase de negociación, de ejecución, o de disolución y/o liquidación de un contrato, tanto a un miembro de la compañía o entidad como a un tercero con que se tenga una relación.

Protocolo de Seguridad de la Información

Documento que indica el conducto regular que se debe cumplir en los diversos contextos en que se trate información física y/o electrónica.

Manual de uso de Herramientas Informáticas

Señala los derechos y deberes a cargo de un miembro de la compañía o entidad en relación al uso de las herramientas informáticas que le brinden o pongan a su disposición.

Emplea el principio de neutralidad tecnológica incluyendo derechos y deberes genéricos aplicables a cualquier clase de herramienta informática (hardware, redes, contenidos y/o software).

Debe desarrollarse y vincularse en armonía con los códigos de ética de la compañía o entidad.

Términos y Condiciones de Uso

Documento macro que consagra el sistema jurídico general de las fuentes del derecho tanto públicas como autorreguladas, regirá la experiencia del usuario con el proyecto o entorno de TIC.

Acuerdo de niveles del servicio (GARANTÍA SOBRE PRODUCTOS, BIENES Y SERVICIOS, EN GENERAL).

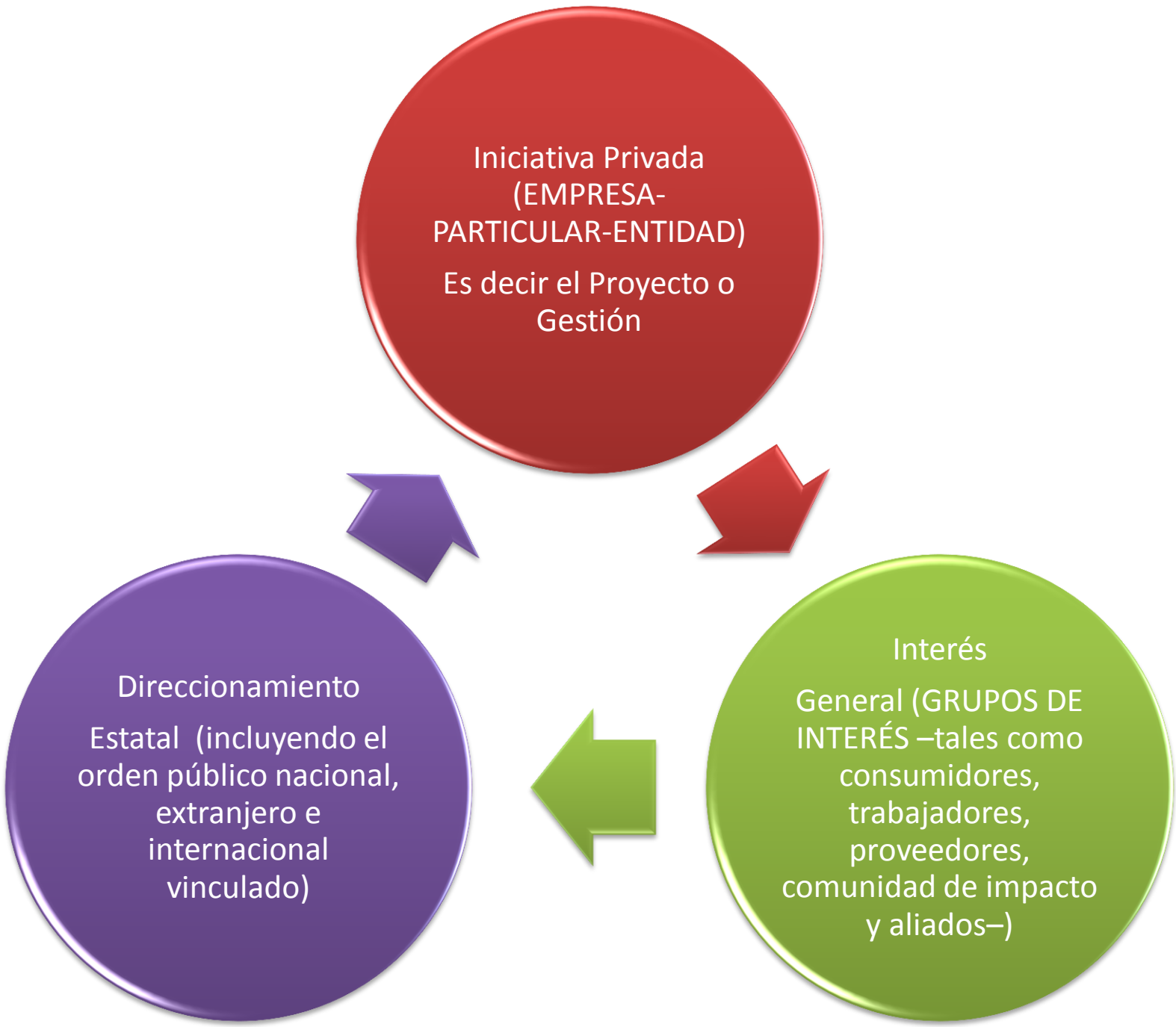
Se trata de un anexo que se sugiere incluir en todo contrato pues indica con claridad los niveles de calidad, seguridad y garantía que se brinda sobre el bien o servicio contratado o prestado por la compañía o entidad.

Contratos de colaboración empresarial, distribución y compensación comercial

Documentos que establecen relaciones comerciales con terceros cercanos a la compañía, en los cuales se deben precisar muy bien los deberes y derechos en las actuaciones digitales que se vayan a realizar o se puedan llegar a presentar.

CONCLUSIÓN

LA VALIDEZ Y LA EFICACIA JURÍDICA DE UN MODELO DE GESTIÓN DE DATOS PERSONALES DIGITALES SE OBTIENE SI SE LOGRA UNA ARMONÍA SISTEMÁTICA DE LOS DERECHOS Y DEBERES DE LA EMPRESA O ENTIDAD CON LOS DE LOS GRUPOS DE INTERÉS DE ORGANIZACIÓN, SITUACIÓN QUE DEBE TENER CONFORMIDAD CON EL ORDEN PÚBLICO QUE SE ENCUENTRE INVOLUCRADO EN CADA CASO DE TIC:



FORO DE PREGUNTAS
Y CONSTRUCCIÓN COLECTIVA DE CONOCIMIENTO

¡Gracias por su atención!

Camilo Alfonso Escobar Mora

Fundador de JURÍDIA®

gerencia@juridia.co

www.juridia.co

Cont@ctenos

Móvil: (57) 320 803 4090

Dirección: Calle 108 # 57-09, oficina 507

Bogotá D.C., Colombia, Suramérica.

Página web: www.juridia.co

Correo: comunicaciones@juridia.co