

---

## LA EDUCACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES<sup>DR©1</sup> PLANEANDO LA SOLUCIÓN DEL PROBLEMA

Noé Adolfo RIANDE JUÁREZ<sup>2</sup>

### SUMARIO

I. *Introducción.* II. *El estado del arte.* III. *Nuestras observaciones.* IV. *Conclusiones.*  
V. *Fuentes de información.*

### I. INTRODUCCIÓN

Las formas más comunes de afectar a quienes realizan actividades en el mundo virtual están señaladas –entre otros–, en la “*Tipología de riesgos en línea para niños*”, desarrollada dentro de las recomendaciones del Consejo de la OCDE<sup>3</sup>:

- Los riesgos de contenido
- Los riesgos de contacto
- Los riesgos de los consumidores
- Los riesgos de seguridad de la información y de privacidad

---

<sup>1</sup> Copyright 2015-16 por Noé A. Riande Juárez. Todos los Derechos Reservados. Ninguna parte de este documento puede ser reproducida para fines comerciales en ninguna forma o mecanismo, incluyendo el fotocopiado, grabación, o almacenamiento en algún sistema de información, sin la autorización por escrito del dueño del copyright. Copias de este documento pueden ser distribuidas, en papel y en formato electrónico, siempre y cuando se realice sin alteraciones, con fines científicos o académicos, citando al autor (disponible en noeriane@gmail.com) y la fuente.

<sup>2</sup> Abogado por la Universidad Veracruzana. Maestro en Filosofía del Derecho por la Università degli Studi di Roma “La Sapienza”. Especializado en Informática Jurídica y Derecho Informático por el Centro di Documentazione Elettronica della Corte Suprema di Cassazione Italiana 1985, y por el Centro Interdisciplinario di Ricerca in Filosofia del Diritto e Informatica e Diritto de la Universidad de Bolonia 1991. Presidente fundador de la Asociación Nacional de Investigadores en Informática Jurídica, A.C. 1993. Catedrático de la División de Estudios de Posgrado de la Facultad de Derecho desde 1994 y Catedrático por invitación de la Maestría en Derecho del Instituto de Investigaciones Jurídicas, ambas de la Universidad Nacional Autónoma de México (UNAM). Exdirector de Investigaciones del Centro de Estudios Superiores en Materia de Derecho Fiscal y Administrativo del entonces Tribunal Federal de Justicia Fiscal y Administrativa. Productor de “Dicere Iure Automatione”, programa del “Proyecto Grado Cero” de la Facultad de Derecho de la UNAM. Consultor Senior en Riande y Assoc. desde 1997. Actualmente es Director de Facilitación al Sector Público en la Secretaría de Protección de Datos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

<sup>3</sup> Cfr. *Las recomendaciones del Consejo de la OCDE para la protección on-line de los niños*, p. 25, disponible en: [https://www.oecd.org/sti/ieconomy/childrenonline\\_with\\_cover.pdf](https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf).

### 1. *Los riesgos de contenido*

La visita a sitios con contenidos riesgosos, por tener contenidos ilegales, inducir a hábitos o dar consejos dañinos.

### 2. *Los riesgos de contacto*

El establecimiento de contactos y amistades en línea sin considerar los riesgos del *cyber-grooming*, del *cyberbullying* (hostigamiento, acoso, burla, persecución) del *cyberstalking* (acoso deshonoroso, con difusión de mensajes o imágenes ofensivas), del *sexting* (acoso sexual, porno venganza) o los riesgos de establecer relaciones en la red para violar la ley, o para compartir materiales indebidos.

Las conversaciones en línea que exponen la privacidad de los usuarios, como en el caso de la interrogación excesiva o disimulada a adultos o menores y la consecuente entrega excesiva de datos, o como sucede cuando se realizan la obtención de datos personales mediante técnicas de ingeniería social con consecuencias imprevistas a corto o largo plazo, a la integridad física, económica y material del usuario o de sus familiares o de personas cercanas.

### 3. *Los riesgos de los consumidores*

Las actividades de consumo en línea que proponen desde la obtención de productos inapropiados o inadecuados, hasta la obtención de productos ilegales con restricciones de edad, la obtención de alimentos y/o bebidas dañinas; o bien, las actividades de consumo en línea que exponen a operaciones engañosas, tales como, el fraude en línea, las estafas y el robo de identidad.

### 4. *Los riesgos de seguridad de la información y de privacidad*

Las actividades que ponen en riesgo la seguridad de la información conservada por el usuario, a través de un código malicioso, de un software espía, o de actividades que al revelar información permiten la realización de estafas en línea y/o robo de identidad.

## **II. EL ESTADO DEL ARTE**

### 1. *Situación actual*

Generalmente se considera que esta educación debe desarrollarse acorde con los principios de la "Educación digital"<sup>4</sup>: "Se entiende por esta, a la educación ya sea presencial o

---

<sup>4</sup> Véase la definición de *educación digital*, en Núñez Álvarez, Andrés. "La educación digital", disponible en: [http://webcache.googleusercontent.com/search?q=cache:1UQyr-utQaMJ:gte2.uib.es/edutec/sites/default/files/congresos/edutec01/edutec/comunic/tse16.html+&cd=1&hl=es&ct=clnk&gl=mx&lr=lang\\_es%7Clang\\_it](http://webcache.googleusercontent.com/search?q=cache:1UQyr-utQaMJ:gte2.uib.es/edutec/sites/default/files/congresos/edutec01/edutec/comunic/tse16.html+&cd=1&hl=es&ct=clnk&gl=mx&lr=lang_es%7Clang_it).

a distancia que hace uso de tecnologías digitales y que tiene como objetivo la adquisición de competencias y habilidades para aprender a aprender, tanto de profesores como de estudiantes en un proceso de formación permanente”

Educación que debe dirigirse a:

- Docentes;
- Alumnos; y
- Familia.

Enfatizándose que:

- Con los docentes el trabajo debe darse desde su formación inicial, y debe involucrarse en un constante proceso de “reciclaje formativo”;
- Con los alumnos el trabajo debe darse con una orientación hacia el disfrute y aprovechamiento del mundo digital, en un ambiente amigable y seguro (... si va acompañada de la entrega de equipos, que nunca se entreguen sin antes capacitar en materia de privacidad y/o protección de datos); y
- Con las familias el trabajo debe empezar por la construcción de espacios de relación con los hijos con diferentes canales de información donde la fuente puede estar tanto en los hijos como en cualquier miembro de la familia.

Cuando se pretende el desarrollo de una acción educativa más amplia<sup>5</sup>, se dice que:

- El Estado... Debe incluir esta educación como una “asignatura obligatoria” y que cuando se entreguen recursos digitales a la ciudadanía (equipos, dispositivos, aplicaciones, etc. para romper la brecha digital), necesariamente sea acompañado de una formación en materia de privacidad y protección de datos.
- A nivel internacional... En ciertos ámbitos ya se habla de intercambios de programas y experiencias.
- La iniciativa privada... También se ha llegado a pensar que la iniciativa privada debe participar desarrollando equipos y aplicaciones que favorezcan la protección de la privacidad.

---

<sup>5</sup> Cfr. “La Declaración de Buenos Aires, hacia la unificación de criterios educativos para la protección de la privacidad en Iberoamérica”, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, disponible en <http://oiprodat.com/declaracion-de-buenos-aires/>.

Otra arista de la problemática que aquí se aborda es la de los “Nativos” y los “Inmigrantes Digitales”:



Los Nativos Digitales, que saben usar las TIC, las usan sin sacarles todo el provecho disponible (y en muchos casos, sin la formación en materia de privacidad y protección de datos que les asegure disfrutar del mundo digital en un ambiente amigable y seguro).

Los Inmigrantes Digitales, que no saben usar las TIC o las usan para lo más indispensable (y en el mejor de los casos también para jugar y socializar).

¿Qué solución se ha planteado para la problemática de la diversa percepción de los “Nativos” y los “Inmigrantes Digitales”?

La respuesta la ofrece el mismo concepto de “*Educación digital*”. Por una parte: No se les debe educar (a Nativos e Inmigrantes Digitales) colocándolos solo como receptores pasivos del conocimiento, hay que volverlos generadores de experiencias y conocimientos. Por otra parte: debe educárseles para que “*Aprendan a aprender*”.

Finalmente, en el marco de la 38ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, (Marruecos, octubre de 2016), se adoptó el “Marco Internacional de Competencias para estudiantes en Materia de Protección de Datos” (dirigido a ayudar a los Educadores), impulsado por el Grupo de Educación Digital de dicha Conferencia coordinado por la Comisión Nacional de Informática y Libertades (CNIL) de Francia<sup>6</sup>.

Este marco presenta nueve (9) principios o temas fundamentales y plantea la obtención un bloque de competencias independientes para cada principio. En total de 42 competencias resultantes del conocimiento y 27 resultados de nuevas habilidades y destrezas.

<sup>6</sup> Véase documento original en: [https://edps.europa.eu/sites/edp/files/publication/16-10-18\\_resolution-competency-framework\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/16-10-18_resolution-competency-framework_en.pdf).

Principios	Resultados del Conocimiento	Habilidades y Destrezas
1. Datos personales		
2. <i>Privacidad, libertades civiles y protección de datos personales</i>		
3. Comprender el entorno digital-aspectos técnicos		
4. <i>Entender el entorno digital-aspectos económicos</i>		
5. Entender los reglamentos y la legislación en materia de datos personales		
6. <i>Entender las normas sobre datos personales: Controlar el uso de la información personal</i>		
7. Gestionar mis datos: Aprender a ejercer mis derechos		
8. <i>Gestión de mis datos: Aprender a protegerme en línea</i>		
9. El mundo digital: Convertirse en un ciudadano digital		

Las 42 competencias resultantes del conocimiento y los 27 resultados de nuevas habilidades y destrezas se distribuyen en grupos de 3 a 5 para cada principio.

Aquí se muestra las competencias específicas para el primer principio (Datos Personales):

Resultados del Conocimiento	Habilidades y Destrezas
<ul style="list-style-type: none"> <li>• Entiendo lo que implica el concepto de <i>datos personales</i>, definido como cualquier dato –sin importar si se hizo público o no– acerca de un individuo identificable;</li> </ul>	<ul style="list-style-type: none"> <li>♦ Puedo dar ejemplos de datos personales que puedan identificar directamente a individuos (estado civil, fotos de un estudiante en la clase, etc.) y datos técnicos que pueden monitorear las actividades de una persona e identificarlas (cookies, datos de geolocalización, etc.).</li> </ul>
<ul style="list-style-type: none"> <li>• Conozco y entiendo el concepto de <i>seudónimo y enmascaramiento de identidad</i>;</li> </ul>	
<ul style="list-style-type: none"> <li>• Sé que, <i>dependiendo de cómo se procese</i>, los datos pueden permitir la identificación del individuo;</li> </ul>	
<ul style="list-style-type: none"> <li>• Sé que ciertos datos técnicos pueden facilitar la identificación de individuos; que los documentos e imágenes escaneadas tienen <i>metadatos</i> internos que describen su contenido y que la actividad en línea puede dejar <i>huellas</i> (cookies, historial de navegación, etc.) que puede contener datos personales;</li> </ul>	
<ul style="list-style-type: none"> <li>• Sé que hay datos que <i>pueden ser considerados como particularmente sensibles, según el país</i> y que, por ejemplo, contienen información sobre <i>menores, orígenes de las personas, opiniones o afiliaciones políticas y/o religiosas, perfil biométrico o genético, salud y/o vida sexual</i>.</li> </ul>	<ul style="list-style-type: none"> <li>♦ Puedo dar ejemplos de datos personales sensibles (por ejemplo, salud, perfil genético, vida sexual).</li> </ul>

### III. NUESTRAS OBSERVACIONES

#### 1. *Consideraciones previas*

Sin dejar de apreciar el valor de las aportaciones previas respecto de las acciones que ahí se proponen, sucedió que desde los primeros abordajes al problema:

Educar: ¿Sobre qué? ¿A quién? ¿Para qué? ¿Qué se debe enseñar? ¿Educar cómo?  
¿Con qué?

Encontramos estas respuestas:

- ¿Sobre qué educar? En materia de protección de datos.
- ¿A quién educar? Al titular de los datos y al responsable del tratamiento.
- ¿Qué se debe enseñar?
  - a) El titular debe conocer los principios de la protección;
  - b) Debe de conocer las condiciones de privacidad;
  - c) Debe exigir el aviso de privacidad;
  - d) Debe saber cómo, cuándo, dónde ejercer sus derechos ARCO;
  - e) Saber cómo, cuándo, dónde presentar una denuncia, y
  - f) Saber cómo obtener un resarcimiento del daño, etc.

Por su parte, el responsable debe conocer cómo elaborar el Aviso de Privacidad, cómo implementar medidas de seguridad... ¿Cuáles medidas?

- a) Evaluar el impacto en la privacidad;
- b) Establecer encargados;
- c) Contratar servicios de “nube”;
- d) Dar respuesta a ejercicios de derechos ARCO;
- e) Responder a denuncias, etc.

No obstante, al buscar respuestas claras ¿Para qué? ¿A partir de dónde? ¿Cuál es el “universo” de atención? ¿A que darle prioridad? ¿Cuáles son las causas? ¿Cuáles son los efectos? Nos encontramos que se tenía que responder también a otras interrogantes que representan nuevos problemas.

#### 2. *Enfrentando problemas*

- ¿Cómo comprender mejor la situación?
- ¿Cuáles herramientas emplear para resolver problemas y tomar decisiones?

- ¿Cuál herramienta para el desarrollo de proyectos orientada a objetivos?
- ¿Cuál herramienta *analítica* para la planificación de proyectos de Política Pública?

La respuesta fue: La metodología del Marco Lógico. El Manual 68 de la CEPAL (Comisión Económica para América Latina y el Caribe), "Formulación de programas con la metodología del Marco Lógico"<sup>7</sup>, nos la ofrecía con gran claridad.

El Marco Lógico se desarrolla en dos fases: la primera fase consiste en el desarrollo de un análisis de la situación que implica:

- Un análisis de los involucrados;
- Un análisis de los problemas;
- Un análisis de los objetivos;
- Un análisis de las alternativas.

La segunda fase consiste en el desarrollo de la llamada Matriz del Marco Lógico de acción, misma que se consigue con el desarrollo de:

- El objetivo del desarrollo;
- El o los objetivos específicos;
- Las actividades que deben realizarse;
- Los resultados que deben esperarse;
- Los indicadores y medios de verificación;
- Los supuestos iniciales; y
- Los insumos y los costos.

Y todo lo anterior se hace partiendo de que los proyectos se diseñan porque existe un obstáculo al desarrollo; y que ese obstáculo se genera porque existe una situación actual insatisfactoria.

Situación insatisfactoria que implica la existencia de una situación futura deseada, esto es, del análisis de la situación actual es posible determinar los términos en que debe trabajarse.

---

<sup>7</sup> Cfr. [https://www.cepal.org/ilpes/publicaciones/xml/0/43220/SM\\_N68\\_Formulacion\\_prog\\_metodologia\\_ML.pdf](https://www.cepal.org/ilpes/publicaciones/xml/0/43220/SM_N68_Formulacion_prog_metodologia_ML.pdf).

### 3. Metodología del marco lógico

Esta metodología puede describirse de manera muy rápida de la siguiente manera:

- El análisis de involucrados; y
- El análisis de problemas.

Alcanzamos *la identificación del problema*, así como también:

- El análisis de objetivos; y
- El análisis de alternativas.

Alcanzamos *la identificación de un proyecto*:

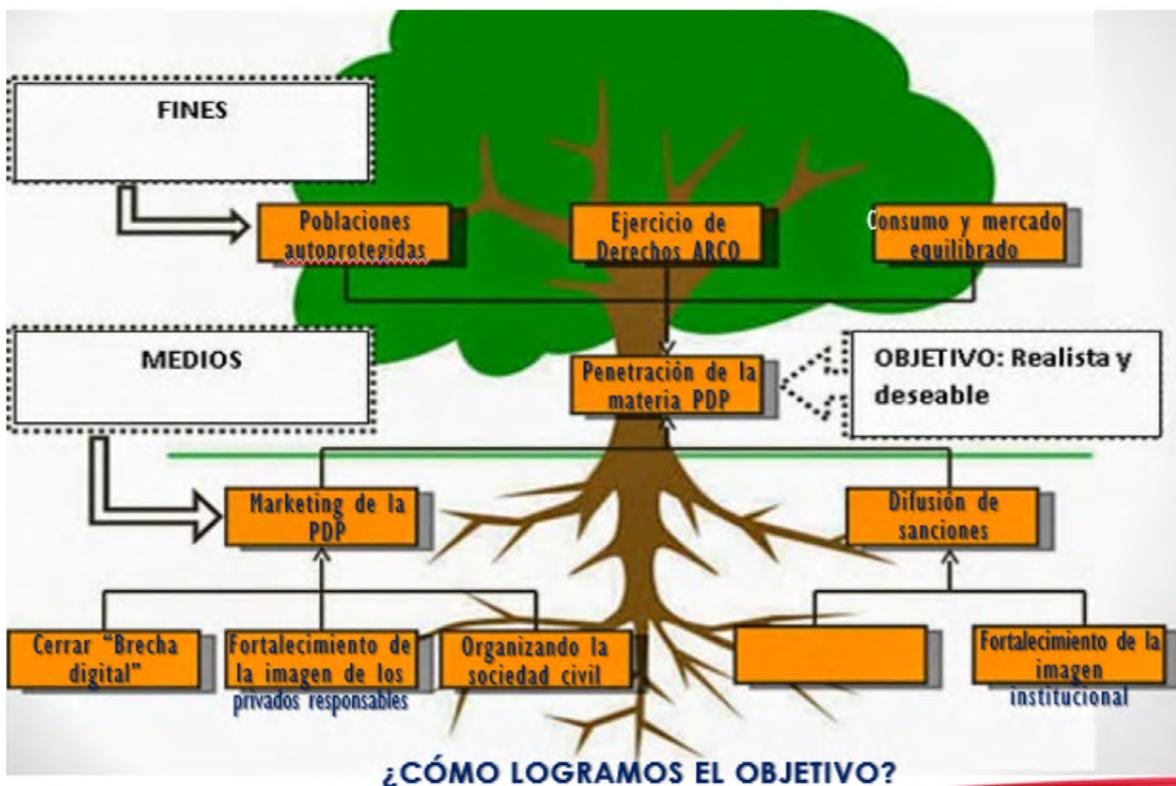
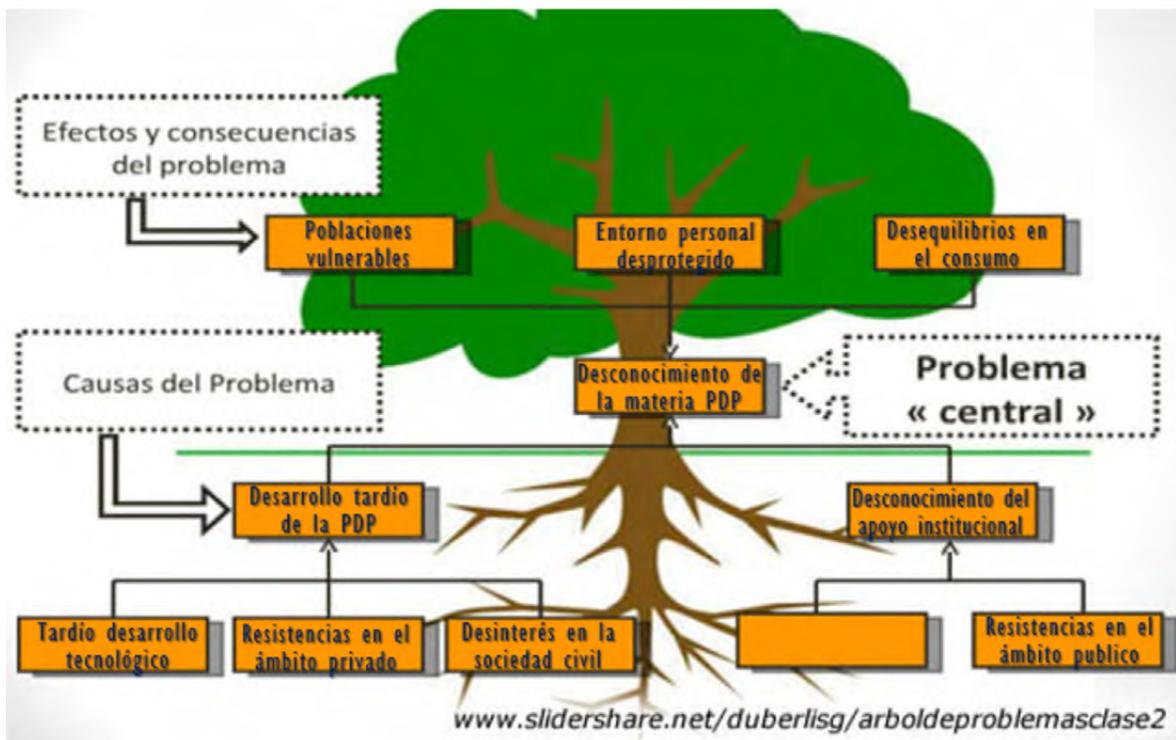
- Esto es, se resume todo lo discutido en los cuatro pasos anteriores;
- Se agrega información sobre lo que se va a monitorear;
- Información sobre lo que se va a evaluar (indicadores); y
- El alcance de la responsabilidad del gerente del proyecto.

En términos de dicha metodología se construye el Árbol del Problema y el Árbol de la Solución.

El Árbol del Problema, tiene un tronco que es el problema previamente identificado, tiene unas raíces que son las que se determinaron como causas de problema; y tiene unas ramas que son las que previamente se determinaron como efectos y consecuencias del problema.

Por otra parte, el Árbol de la Solución consta de igual modo con un tronco constituido por el objetivo realista y deseable, con raíces conformadas con los medios identificados como los deseables para alcanzar el objetivo, y asimismo, con ramas conformadas por los fines que se esperan conseguir como consecuencia de haber alcanzado el objetivo.

Véanse las figuras a continuación:



Al momento de aplicar esta metodología encontrarán que:

- Simultáneamente se deben atender más de un problema y que se tendrán que analizar más situaciones;
- Que más de una causa producen un problema;
- Las raíces o las ramas de un árbol pueden profundizarse demasiado;
- Hay causas y/o efectos que van más allá de su ámbito de control o de interés; y
- El énfasis se centra en encontrar objetivos fáciles de medir o cuantificar.

Pero también apreciarán que esta metodología:

- Proporciona una guía al análisis sistemático;
- Mejora la capacidad de planeación de un proyecto;
- Asegura que las preguntas fundamentales que se hagan, analicen, realicen e identifiquen las debilidades del proyecto;
- Facilita la comunicación y uniformidad de las ideas; y
- Facilita el análisis sectorial y los estudios comparativos, al tener la mayoría de los proyectos en formatos similares.

#### **IV. CONCLUSIONES**

La *Metodología del Marco Lógico* es solo una de las herramientas de formulación y diseño de proyectos, que no reemplaza a herramientas como el análisis de grupos, la planeación de tiempo, el análisis de efecto e impacto y otras que aseguran un proyecto socialmente ubicado.

Por lo anterior, es de esperarse su empleo de manera casi obligada pero sin dejar de considerar otras herramientas de planeación, así como:

- Los acertados aportes del *Observatorio Iberoamericano de Protección de Datos*;
- Las recomendaciones provenientes de la corriente pedagógica de la "*Educación Digital*";
- "*El Marco internacional de competencias para estudiantes en materia de Protección de Datos*" producido por el Grupo internacional de Educación Digital de la 38° Conferencia internacional de autoridades de Protección de Datos y Privacidad; y
- Que la tarea no es solo con los "*titulares*" sino también con los "*responsables*".

## V. FUENTES DE INFORMACIÓN

*Formulación de programas con la metodología del Marco Lógico*, Manual 68 CEPAL, [https://www.cepal.org/ilpes/publicaciones/xml/0/43220/SM\\_N68\\_Formulacion\\_prog\\_metodologia\\_ML.pdf](https://www.cepal.org/ilpes/publicaciones/xml/0/43220/SM_N68_Formulacion_prog_metodologia_ML.pdf).

*La Declaración de Buenos Aires, hacia la unificación de criterios educativos para la protección de la privacidad en Iberoamérica*, Observatorio Iberoamericano de Protección de Datos, <http://oiprodat.com/declaracion-de-buenos-aires/>.

*Las recomendaciones del Consejo de la OCDE para la Protección on-line de los niños*, [https://www.oecd.org/sti/ieconomy/childrenonline\\_with\\_cover.pdf](https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf).

*Marco Internacional de Competencias para estudiantes en Materia de Protección de Datos*, Comisión Nacional de Informática y Libertades (CNIL) de Francia, [https://edps.europa.eu/sites/edp/files/publication/16-10-18\\_resolution-competency-framework\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/16-10-18_resolution-competency-framework_en.pdf).

NÚÑEZ ÁLVAREZ, Andrés, *La educación digital*, [http://moodle2.unid.edu.mx/dts\\_cursos\\_md/pos/ED/AN/AM/08/Congreso\\_internacional\\_de\\_tecnologia.pdf](http://moodle2.unid.edu.mx/dts_cursos_md/pos/ED/AN/AM/08/Congreso_internacional_de_tecnologia.pdf).