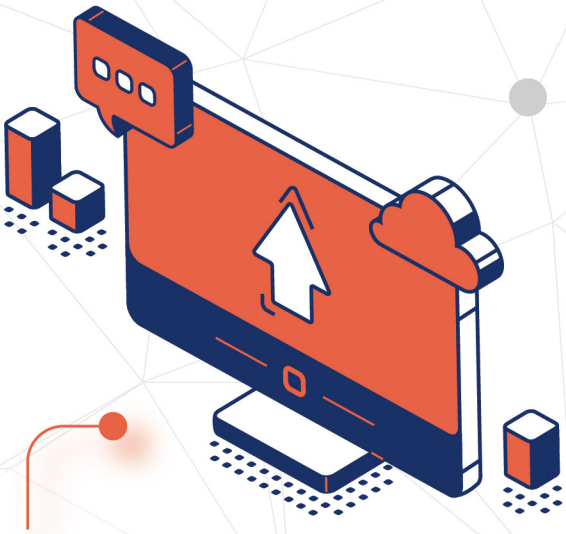


Guía para Navegar el Ecosistema Digital

anda
Asociación Nacional de Anunciantes de Colombia

ANDA COLOMBIA

La Asociación Nacional de Anunciantes ANDA, es el gremio que representa los intereses de los anunciantes en Colombia. Constituida en 1939, impulsa el desarrollo de la industria de la comunicación comercial, como motor de progreso para el país y como una actividad que estimula entre los anunciantes la generación de buenas practicas en beneficio de un consumidor informado.

Estamos comprometidos con el desarrollo, y el buen ejercicio de la industria generando puntos de encuentro y relaciones de confianza con actores relevantes para los anunciantes, que van desde la academia hasta el regulador.

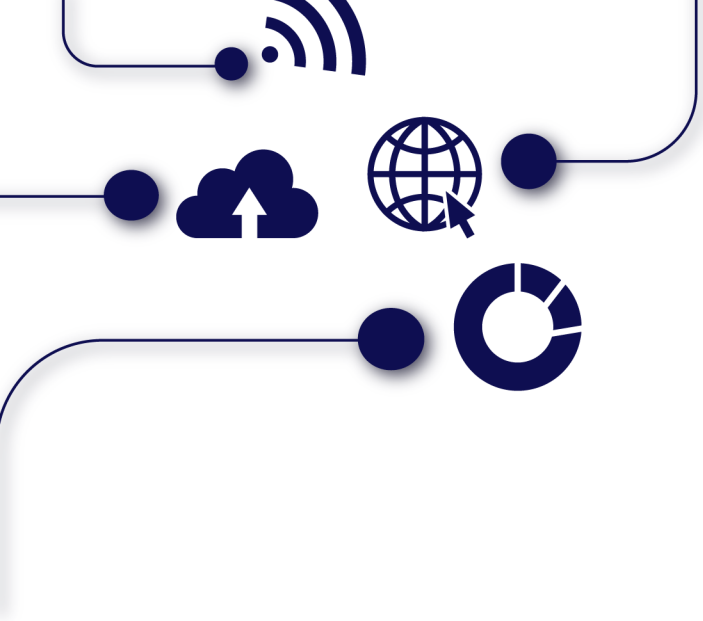
Nos regimos por los principios de autorregulación entendiendo esta como la manera más eficiente para garantizar el balance entre el derecho a la libre expresión comercial y la protección del consumidor.

Hacemos parte de la **Federación Mundial de Anunciantes (WFA)**, asociación cuyas publicaciones son la base para el desarrollo de nuestros documentos de autorregulación.

La WFA, reúne a los Mercados y anunciantes más grandes del mundo, y lidera el desarrollo de las Comunicaciones de mercadeo responsables y efectivas. Esta federación conecta a los anunciantes más grandes del mundo con asociaciones nacionales de anunciantes en más de 60 países, reuniendo miles de marcas a nivel local. Juntas crean una red global que ofrece liderazgo, experiencia e inspiración.

Desde el 2013, ANDA es responsable de la organización del programa **Effie Colombia®**, bajo licencia otorgada por Effie Worldwide Inc. La misión de Effie es liderar , inspirar y promover, la práctica y a quienes practican la efectividad en mercadeo. Desde 1968, Effie incentiva a la industria a ser cada vez más efectiva y a mostrar los mejores ejemplos de esta evolución, impactando a profesionales en todas las etapas de sus carreras a través de sus programas, **Effie College** y los **Effie Awards.** Hoy en día, Effie cuenta con 55 programas; tiene presencia en 50 países y 5 programas regionales.

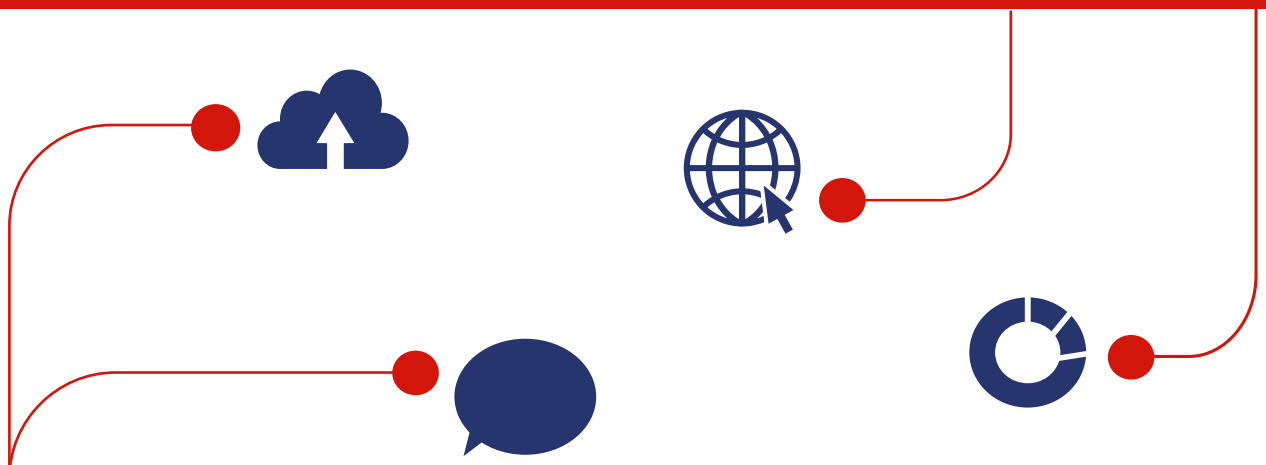
anda
Asociación Nacional de Anunciantes de **Colombia**



GUÍA PARA NAVEGAR EL ECOSISTEMA DIGITAL

Contenido

Presentación



En octubre de 2019 inicia un año de conmemoración de los cuarenta años de existencia de la Asociación Nacional de Anunciantes (ANDA), durante los cuales ha trabajado en impulsar las mejores prácticas en la comunicación comercial, convencidos de la capacidad de la publicidad para transformar social y culturalmente. Nuestros anunciantes son conscientes que la confianza del consumidor es su activo más valioso; por eso, desde la ANDA hemos impulsado el desarrollo de iniciativas de autorregulación con el fin de mitigar problemas que arriesguen la confianza y la seguridad del consumidor.

El auge de la era digital ha generado nuevos desafíos para la industria; estos retos afectan a las empresas, como en el caso de amenazas de brand safety o fraude publicitario, y a los consumidores, quienes son vulnerables a la falta de transparencia sobre la recolección, el manejo y el almacenamiento de datos. Con el fin de protegerlos, la autorregulación debe liderar la definición de estándares éticos que ayuden a delinear las mejores prácticas en la comunicación comercial digital, ya que el Ecosistema Digital no se rige por las fronteras nacionales que limitan la regulación.

Inspirados en esta coyuntura y en las guías y documentos de autorregulación de la WFA (World Federation of Advertisers), elaboramos la Guía para Navegar el Ecosistema Digital de la mano del Comité de Innovación y Mercadeo de la ANDA. Este documento, producto del compromiso de los anunciantes de la ANDA con una comunicación comercial ética y sostenible, recoge las buenas prácticas y tendencias globales y locales y ofrece recomendaciones para proteger al consumidor y evitar riesgos a la reputación de las marcas.

Esperamos que esta guía sea un referente para nuestros afiliados e inspire a todo el ecosistema de la comunicación comercial para que en un futuro sirva como un insumo para desarrollar compromisos voluntarios que sean adoptados y promovidos por todos los actores de la industria del mercadeo digital en Colombia.

Elizabeth Melo
Presidenta Ejecutiva
Asociación Nacional de Anunciantes, ANDA Colombia

En una era del manejo de Data, la transparencia y buen uso de los datos son una responsabilidad de las marcas y todos los actores del mercado publicitario.

Frente a este desafío se ha desarrollado este documento, el cual servirá de marco de referencia para las buenas prácticas digitales y hace parte de la búsqueda de procesos de autorregulación y de la responsabilidad por impulsar un ecosistema digital más transparente y de alta calidad en nuestro mercado.

Es un punto de partida para construir un compromiso común de colaboración continua de todos los actores de la industria para manejar con responsabilidad las plataformas y la influencia que ejercen en la sociedad. Buscamos actuar de forma responsable, de acuerdo con nuestros principios de negocios y con el consumidor para promover las buenas prácticas y modelos de transparencia en la cadena de valor digital; este debe ser un principio extendido y compartido por todos, contribuyendo a una mejor sociedad y a una relación positiva de las marcas con los consumidores

Liliana Pérez
CCM Director Unilever, Middle Americas
Coordinadora del Comité de Innovación y Mercadeo, ANDA Colombia

Hemos entrado en la etapa de las compañías disruptivas, diseñadas por el ecosistema tecnológico y digital; hoy vemos como la experiencia del consumidor pesa más que la publicidad tradicional, la tecnología y los datos hacen que los modelos tradicionales de mercadeo y publicidad hayan quedado obsoletos.

Las regulaciones a nivel internacional como GDPR, CCPA y el Privacy Sandbox Policy de Google obliga que marcas y agencias modifiquen el proceso para la recolección, manipulación, análisis y explotación de los datos, y que hoy más que nunca tenga un componente tecnológico mandatorio. Atrás quedaron las opciones de cookies, muy pronto se verá afectado los famosos IDs o SDKs de la publicidad y el mercadeo móvil, y las plataformas propias para homogeneizar el proceso de datos, cada vez tenga mayor relevancia.

Los medios no se quedan atrás, el COVID hizo que obligatoriamente se vean en la tarea de digitalizar su oferta de valor, el consumidor de hoy está inmerso en digital, sin importar si es un punto de contacto físico o no. Esta guía lo que pretende es ampliar el conocimiento sobre los datos, su estructura, sus diferentes fuentes y cómo procesarlos con base a las normativas actuales. Pero también es una invitación a transformarse, porque de lo contrario estamos a puertas de la 6a era de la extinción en términos económicos, donde aquellos que se atreven a ser disruptivos y se adaptan sobreviven...los que no, son cosa del pasado.

Andrés Felipe Gutiérrez Henao
Head of Data Dentsu Aegis, México
Experto en publicidad digital y big data

Capitulo 1: Privacidad de los datos y regulación

1. MARCO REGULATORIO.

COLOMBIA:
Ley 1581 de 2012 y Decreto 1074 de 2015.

El artículo 15 de la Constitución Política de Colombia consagra el derecho fundamental que tienen todas las personas 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. Lo anterior se refiere a que las personas, (nacionales o extranjeras), tienen la potestad de conocer y autorizar lo que hacen las empresas con su información personal, además de tener la autoridad para solicitar la eliminación de sus datos de cualquier base de datos, salvo algunas excepciones legales.

La Ley 1581 de 2012 o Ley de Datos Personales, desarrolla este derecho constitucional de protección de datos personales, también conocido como Habeas Data, y sus disposiciones son de obligatorio cumplimiento para todas las personas naturales y jurídicas, públicas o privadas, que realicen tratamiento, es decir recolección, almacenamiento, uso, circulación o supresión de datos personales.

La Superintendencia de Industria y Comercio (SIC), a través de la Delegatura para la Proteccion de Datos Personales, se encarga de la vigilancia y control del tratamiento de los datos personales en Colombia y cuenta con amplias facultades sancionatorias. De acuerdo con la Ley 1581 de 2012, la delegatura para la Proteccion de datos personales tiene, entre otras, las siguientes funciones:

- Adelantar investigaciones administrativas y ordenar medidas para la efectividad de los derechos de habeas data.

- Imponer sanciones:
  - Multa de carácter personal e institucional hasta por 2.000 smlmv.
  - Suspensión de actividades relacionadas con el tratamiento, hasta por 6 meses, con indicacíon de correctivos.
  - Cierre temporal de operaciones relacionadas con el tratamiento.
  - Cierre definitivo, por tratamiento de datos sensibles.

- Disponer bloqueo temporal de los datos, si existe riesgo de vulneración de derechos fundamentales.

- Administrar el Registro Nacional de Bases de Datos (RNBD).

La Ley de Datos Personales también establece importantes obligaciones para quienes realicen tratamiento de Datos Personales, entre ellas:

1. Contar con la autorización previa, expresa e informada de los titulares para captar datos personales semiprivados, privados y sensibles.

2. Conservar copias o evidencias de las autorizaciones otorgadas por los titulares.

3. Custodiar la información compilada.

4. Atender las consultas y los reclamos de corrección o actualización de información presentados por los titulares de los datos personales, conforme a los procedimientos y plazos establecidos en la Ley.

5. Adoptar un manual interno de políticas y procedimientos, en especial para atención de consultas y reclamos.

6. Informar a SIC sobre violaciones a códigos de seguridad y cuando identifique riesgos en la administración de la información de los titulares.

AUTORIZACIÓN O CONSENTIMIENTO.

Uno de los principios fundamentales que debe respetar todo tratamiento de datos personales es el principio de libertad, según el cual, el tratamiento sólo puede realizarse con el consentimiento previo, expreso e informado del titular del dato personal a tratar.

Cabe aclarar que los datos personales pueden ser de naturaleza pública, semiprivada o privada. Para el caso de los datos que se consideran públicos la ley ha indicado que su tratamiento puede realizarse sin que se requiera previa autorización del titular. Este es el caso, por ejemplo, de los datos relacionados con el estado civil de las personas, su profesión u oficio, su calidad de comerciante o de servidor público.

Por su parte, datos personales como el nombre, datos de contacto (el número de teléfono, la dirección física o el correo electrónico personal), datos financieros o crediticios se consideran como datos semiprivados, pues su conocimiento y divulgación pueden interesar a cierto grupo de personas o a la sociedad en general. Por otro lado, los datos personales privados, son los que tienen naturaleza íntima o reservada y sólo son relevantes para el titular.

Así las cosas, si se trata de datos personales privados o semiprivados, cualquier tipo de tratamiento requerirá el consentimiento previo, expreso e informado de su titular.

En desarrollo del mencionado principio de libertad, la Ley estableció que el responsable del tratamiento de datos personales, -entendiendo por este a quien por sí mismo o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos- , tiene la obligación de solicitar y conservar copia de la respectiva autorización otorgada por el titular y de informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

Esto tiene sentido, porque recordemos que la ley exige que el consentimiento sea previo, expreso e informado, por lo cual, no es suficiente pedir una autorización, sino que debe cumplirse con varias condiciones:

- La autorización debe solicitarse oportunamente, o, como lo dispone la norma reglamentaria: a más tardar en el momento de la recolección de los datos.

- Si la finalidad para la que se va realizar el tratamiento requiere conocer la identidad del interesado, el Responsable del Tratamiento debe establecer previamente la identidad de la persona natural cuyos datos serán recolectados y usados, es decir, tener certeza de la identificación del titular para así evitar posibles suplantaciones de identidad.

- Tomando en cuenta que se requiere que la autorización sea expresa, la Ley dispuso que esta puede manifestarse por escrito, de forma oral, o mediante una conducta inequívoca que permita, de forma razonable concluir que el titular otorgó su autorización previa, expresa e informada. La norma reglamentaria dispuso que el silencio no se puede considerar nunca como una conducta inequívoca.

- A más tardar al momento de solicitar la autorización, el responsable del tratamiento debe haber informado al titular sobre:

  I) El tipo de Tratamiento al que serán sometidos sus datos personales y la finalidad del Tratamiento.

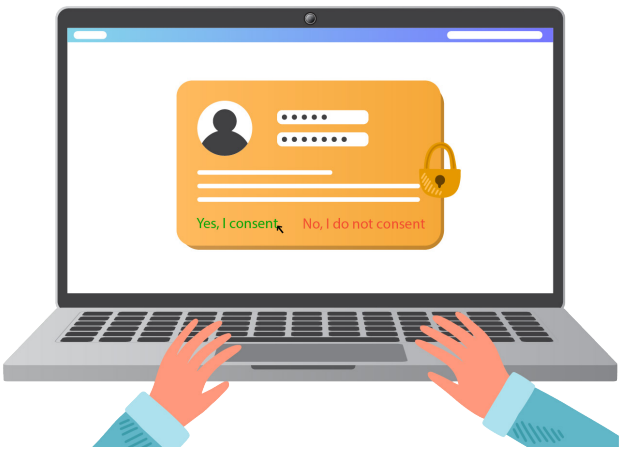
  II) Los derechos que le asisten como titular.

  III) La identificación y datos de contacto del responsable del tratamiento.

IV) Si se trata de datos sensibles o datos de niños, niñas y adolescentes, debe informarse sobre el carácter facultativo de las respuestas a las preguntas que se le formulen. Es muy importante conservar la prueba de haber cumplido con esta obligación de información.

- En relación con las formas a través de las cuales se puede obtener el consentimiento, la norma reglamentaria permitió expresamente la posibilidad de que los mecanismos para obtener la autorización sean predeterminados por el Responsable del Tratamiento, a través de medios técnicos que faciliten al titular su manifestación automatizada. No obstante, en este caso deberá poderse acreditar que el titular otorgó su autorización, y además, que lo hizo habiendo sido debidamente informado.

- Es muy importante tener en cuenta que la SIC ha manifestado que el hecho de que el titular registre voluntariamente sus datos en una plataforma digital, o que descargue o instale una aplicación, o que acepte los términos y condiciones de un servicio, por si solos no permiten inferir la obtención de la autorización, ni permiten deducir que el titular fue debidamente informado.



LA PROTECCIÓN DE DATOS PERSONALES Y LOS MECANISMOS PARA RECOLECTAR DATOS A TRAVÉS DEL ECOSISTEMA DE PUBLICIDAD DIGITAL.

En Colombia, a diferencia de lo que ha sucedido en otros países, el uso de tecnologías de almacenamiento de información, como el que se hace a través de las cookies, no ha sido objeto de una reglamentación especial. No obstante, cada vez son más evidentes las implicaciones que el uso de esas tecnologías puede tener en relación con la protección de los datos personales o incluso con otros derechos como la intimidad y la privacidad.

En particular, en relación con la protección de datos personales, se ha discutido si esta regulación es aplicable al uso de cookies, pues no resulta del todo claro si la información que se recopila a través de estas se puede considerar como un dato personal y si el uso de las cookies configura un tipo de tratamiento de datos personales.

No obstante la ausencia de regulación particular, la cuestión en nuestro país se resuelve de una forma relativamente simple.

> Por una parte, debe recordarse que la legislación colombiana define el Dato Personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". [1]

A su vez, la SIC, con base en la definición mencionada y en la jurisprudencia constitucional, agrega que los datos personales tienen las siguientes características:

(I) están referidos a aspectos exclusivos y propios de luna persona natural.

II) Permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos;

III) Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita.

IV) Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación[2].

Así las cosas, puede considerarse, como de hecho sucede en otros países, que la información que recopilan las cookies sobre los hábitos de navegación, las preferencias o acciones del usuario del sitio web o de la app, o sobre su equipo, como por ejemplo la dirección IP del usuario, son datos que, vistos en conjunto con otros datos, podrían asociarse con un usuario determinado.

Por lo anterior, la SIC ha indicado que las cookies eventualmente pueden conformar una base de datos, pues recolectan datos personales (conforme a la definición que ya citamos), y en consecuencia, el Responsable deberá cumplir las normas sobre protección de datos.

Por otra parte, las cookies son un mecanismo tecnológico que permite la recopilación de datos; si tomamos en cuenta que la recolección es una de las formas de hacer Tratamiento de datos personales de acuerdo con la Ley, debemos concluir que el uso de las cookies requiere, sin excepción, el consentimiento expreso y previo por parte del titular de los datos, quien deberá haber sido informado sobre el tipo de cookies que se van a utilizar y la finalidad de estos.

1. Literal c) del artículo 3 de la Ley 1581 de 2012.
2. Superintendencia de Industria y Comercio, Concepto Radicado No. 16-172268 del 9 de agosto de 2016.

REVOCATORIA DE LA AUTORIZACIÓN Y SUPRESIÓN DE LOS DATOS PERSONALES.

Los Responsables del Tratamiento deben garantizar en todo momento a los titulares de datos personales, el ejercicio pleno y efectivo de su derecho de Habeas Data, esto incluye, respetar la decisión del titular de revocar la autorización que había otorgado y proceder a suprimir los datos que había recolectado, si así lo solicita el titular.

El consentimiento entonces no es inamovible, puede ser revocado por el titular en cualquier momento, para todos o para algunos tipos de tratamiento y respecto de todas o de alguna de las finalidades para las que había dado su autorización, mediante la presentación de un reclamo ante el Responsable o el Encargado del Tratamiento, quienes, a su vez, tienen la obligación de establecer mecanismos gratuitos y de fácil acceso para que los titulares presenten sus solicitudes de supresión de los datos o las revocatorias de las autorizaciones.

En adición, la SIC ha indicado que estos mecanismos deben implementarse a través de los mismos medios o canales mediante los cuales los Responsables del Tratamiento se contactan o comunican con los Titulares de los datos, y que las consultas y reclamos que estos presenten deben responderse de manera oportuna y de fondo, eliminando cualquier barrera innecesaria para garantizar los derechos de los titulares.

Por último, es importante tener en cuenta que las solicitudes de revocatoria de la autorización y de supresión de los datos no proceden cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.

COLOMBIA:
REGISTRO NACIONAL DE BASES DE DATOS (RNBD).

El Registro Nacional de Bases de Datos (RNBD) fue creado por la Ley 1581 de 2012 que lo define como el directorio público de las bases de datos personales sujetas a Tratamiento que operan en el país, administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos.

La información mínima que debe contener este registro, así como los términos y condiciones en que se deben inscribir los responsables del tratamiento en el RNBD fueron objeto de reglamentación posterior por el Gobierno Nacional.

Es importante advertir que, la obligación de registrar las Bases de Datos en el RNBD que administra la SIC, únicamente existe para las sociedades y entidades sin ánimo de lucro que tengan más de 100.000 UVT´s de activos totales [3], independientemente del número de empleados que tengan, así como para todas las entidades públicas.

El último plazo para realizar la inscripción de las Bases de Datos en el RNBD por parte de personas jurídicas de naturaleza privada expiró el día 31 de enero de 2019. Adicionalmente, debe tenerse en cuenta que las Bases de Datos nuevas deberán inscribirse dentro de los dos (2) meses siguientes a su creación. El incumplimiento de la obligación de inscribir las Bases de Datos en el RNBD acarrea la imposición por parte de la SIC de las sanciones ya mencionadas.

3. Corresponde a $3.427.000.000,oo., tomando en cuenta el valor de la UVT fijado por la DIAN para el año 2019.

UNIÓN EUROPEA:
Reglamento General de Protección de Datos (RGPD) o General Data Protection Regulation (GDPR).

GDPR es un Reglamento destinado a reforzar y armonizar la protección de datos en la Unión Económica Europea, aplicable desde el 25 de mayo de 2018. Se aplica tanto a empresas de la UE como a empresas extranjeras que procesan datos de residentes de la UE. Por lo tanto, tiene un profundo impacto en ecosistema digital publicitario.

El GDPR requiere que cualquier procesamiento de datos sea legal (es decir, que cumpla al menos una de las condiciones especificadas). La mayoría de los datos publicitarios digitales deberán procesarse con base en el consentimiento explícito del interesado. Se debe conservar un registro del consentimiento, incluida la redacción exacta, la fecha y los medios para obtenerlo.

Las condiciones para obtener el consentimiento en el GDPR son relativamente estrictas, incluyendo:

- La solicitud de consentimiento debe ser prominente y fácil de entender.
- Debe haber una aceptación positiva (opt-in) que requiera acción (no hay recuadros predeterminados previamente).
- El consentimiento no puede ser una condición previa del servicio.
- El consentimiento debe ser fácil de retirar (opt-out).
- El propósito del procesamiento de datos debe ser declarado.
- Todas las organizaciones que dependen del consentimiento deben ser nombradas.

En cuanto al alcance, GDPR se aplica a los datos personales, cualquier información relacionada con una persona física identificada o identificable (PII). Los identificadores personales pueden incluir:

- Nombre
- Direcciones físicas
- Números de teléfono o celular
- Correo electrónico
- Información financiera (Tarjetas de crédito)
- Dirección IP
- IDs (por ejemplo, ID de cookie, ID de dispositivo)
- Datos de ubicación –location data -
- Fotos
- Información médica
- Huellas dactilares

Bajo GDPR, las personas tienen los siguientes derechos:

- A estar informado (es decir, recibir información de procesamiento de datos equitativa).
- A acceder a los datos (obtención de confirmación de procesamiento de datos personales y acceso a la misma).
- A la rectificación (si los datos son inexactos o incompletos).
- A ser borrado (particular si un individuo retira el consentimiento).
- A la restricción del procesamiento (los datos pueden almacenarse, pero no pueden procesarse).
- A la portabilidad de datos (es decir, obtener datos personales y usarlos en otro lugar).

- A la objeción al procesamiento de datos basado en intereses legítimos, para marketing directo o con fines de investigación.

- Derechos en relación con la toma de decisiones automatizadas y la creación de perfiles (es decir, protección contra el riesgo de decisiones automatizadas significativas, ejemplo: clusterizaciones).

El GDPR diferencia entre procesadores de datos y controladores de datos. Si bien el controlador determina los fines y los medios de procesamiento de los datos personales, los procesadores son responsables del procesamiento de los datos. Tanto los controladores como los procesadores deben cumplir con los principios de GDPR y deben garantizar (contractualmente donde corresponda) que los datos personales estén adecuadamente protegidos, por ejemplo, contra el procesamiento o la pérdida ilegal o no autorizada.

Antes de cualquier nueva actividad de procesamiento de datos (incluida la adopción de nueva tecnología, procesamiento de datos de riesgo o sensibles, o perfiles de usuario), los controladores de datos requieren llevar a cabo una evaluación de impacto.

Algunas organizaciones, como las que llevan a cabo un seguimiento del comportamiento a gran escala utilizado en publicidad digital (ejemplo: DMPs), también deben designar Oficiales de Protección de Datos (DPO). Los DPO son responsables del cumplimiento de GDPR y otras leyes de protección de datos.

Conforme al GDPR, la transferencia internacional de datos fuera de la UE está restringida para garantizar que el nivel adecuado de protección sea asequible para los datos de las personas. Las organizaciones deben informar infracciones de datos más riesgosas, ya sea a una autoridad supervisora, o también a las personas afectadas. Para garantizar el cumplimiento, GDPR faculta a las autoridades de protección de datos con el poder de imponer multas significativas: hasta 20 millones EUR o el 4% de la facturación anual global de la empresa (lo que sea mayor).

La reglamentación del GDPR, a pesar del costo y la carga administrativa que impone a las organizaciones que procesan datos, en general ha sido bien recibida por la industria. Mejora la conciencia y el control de la información de las personas, lo que aumenta su confianza en la industria de la publicidad digital y en los publishers y servicios a los que ayuda.

Esta regulación también aumenta la transparencia del flujo de datos, el procesamiento y la visibilidad de las organizaciones involucradas de la siguiente manera:

- **Prima el consentimiento expreso:** En términos generales, tanto en el Habeas Data como en el Reglamento GDPR ha primado el consentimiento expreso como base jurídica para el tratamiento de datos personales; es la norma general y lo demás excepciones. Frente al consentimiento tácito que ha venido funcionando hasta ahora, se exige una declaración o una clara acción afirmativa.

- **Solo se utilicen los datos estrictamente necesarios:** El GDPR mantiene la exigencia de que solo se utilicen los datos estrictamente necesarios, lo cual puede ser relevante en actividades como las de las redes sociales; e introduce un elemento novedoso: el de la responsabilidad proactiva. De hecho, la prevención es uno de los pilares del Reglamento, según el cual actuar una vez producida la infracción, que puede causar daños difíciles de reparar, es insuficiente como estrategia.

- **Mensajes comerciales y publicidad digital:** Cuando un mensaje comercial digital sea enviado a correos electrónicos, teléfonos móviles u otras cuentas o servicios similares, a través de los cuales cada destinatario del mensaje pueda ser contactado directa y personalmente, el encabezado y contexto del mensaje deben indicar claramente que el mensaje es de naturaleza comercial. El texto de los encabezados no debe provocar confusión al respecto. Solamente pueden enviarse mensajes comerciales no solicitados a través de medios digitales interactivos cuando, además de respetar las normas aplicables en materia de protección de datos personales:

  1. Existan bases razonables para considerar que el consumidor que los reciba pueda tener interés en el objeto de éstos o en la oferta.

  2. Incluyan un mecanismo claro y transparente que permita al consumidor expresar su deseo de no recibir otras comunicaciones en el futuro.

- **Más información al interesado:** El deber de información del responsable se configura ahora como un derecho del interesado, al que hay que facilitar una información considerablemente mayor: desde los datos de contacto, hasta la base jurídica del tratamiento, que no existía hasta el momento. Y si los datos no se recaban del interesado habrá también que dar cuenta de la categoría de los que se van a tratar y de la fuente de procedencia. La información sobre el tratamiento y procesamiento de los datos exige que esta información sea clara, sencilla y accesible. Existen algunos antecedentes en este sentido, como el caso de las cookies, donde se presenta una información breve cuando se accede al sitio web y luego enlaces a datos complementarios.

- **Portabilidad de los datos:** Se fomenta el ejercicio por vía electrónica de los derechos a la limitación del tratamiento y a la portabilidad, lo que implicará articular mecanismos para garantizar la identidad de quienes los ejerzan. Y surge un derecho nuevo, el de la limitación al tratamiento, por el que se bloquean los datos de carácter personal con el fin de evitar su tratamiento al menos durante un tiempo.

TENDENCIAS EN PROTECCIÓN DE DATOS

La Ley de privacidad del consumidor de California (CCPA). [4]

¿Qué es la CCPA?

Ley de Privacidad del Consumidor de California (CCPA) es la primera norma global de privacidad de Estados Unidos. Se sancionó a finales de junio de 2018 y establece una variedad de derechos de privacidad para los consumidores de California. Los negocios regulados por la CCPA tienen una serie de obligaciones hacia los consumidores, como divulgación de información, derechos de consumidores como los del RGPD, una "no participación" para determinadas transferencias de datos y un requisito de "consentimiento" para menores.

¿Quién necesita conocer la CCPA?

La CCPA solo se aplica a los negocios que operan en California y que satisfacen una o varias de las siguientes condiciones:

1. Tienen un beneficio bruto superior a 25 millones de USD
2. El 50 % o más de sus ingresos se originan en la venta de información personal de los consumidores, o
3. Compran, venden o comparten la información personal de más de 50 000 consumidores.

¿Cuándo entra en vigor la CCPA?

La CCPA entra en vigor el 1 de enero de 2020. Sin embargo, el Fiscal General no comenzará a aplicarla hasta el 1 de julio de 2020.

¿Cómo afectará la CCPA a mi empresa?

Muchos de los derechos que la CCPA otorga a los californianos son similares a los que proporciona el RGPD, incluidas las solicitudes de divulgación y del consumidor, similares a las solicitudes del interesado (DSR) del RGPD, como el acceso, la eliminación y la portabilidad de datos. Por lo tanto, los clientes pueden buscar nuestras soluciones de RGPD existentes para ayudarles con el cumplimiento normativo de la CCPA.

4. FAQ CCPA – Fuente: https://docs.microsoft.com/es-es/microsoft-365/compliance/ccpa-faq?view=o365-worldwide

Para comenzar con la CCPA, debe centrarse en cinco pasos clave:

1. **Descubrimiento:** identifique qué información personal tiene y dónde reside.
2. **Asignación:** determine cómo comparte información personal con terceros e identifique si el tercero está sujeto a una excepción de los requisitos de no participación de la CCPA.
3. **Administración:** controle cómo se usan los datos y cómo se obtiene acceso a ellos.
4. **Protección:** establezca controles de seguridad para evitar, detectar y responder a vulnerabilidades y filtraciones de datos.
5. **Documentación:** elabore un programa de respuesta a una filtración de datos y asegúrese de que sus contratos con terceros aplicables puedan hacer uso de las excepciones de no participación.

¿Qué derechos deben habilitar las empresas conforme a la CCPA?

La CCPA establece para los negocios regulados que recopilen, usen, transfieran y vendan información personal, entre otras, las siguientes obligaciones:

- Informar a los consumidores, antes de la recogida de datos, de las categorías y propósitos de la recogida.
- Dar información detallada en la política de privacidad de las fuentes de datos, los fines empresariales y las categorías de información personal recopilada, incluido cómo se venden estas categorías o se transfieren a otras entidades.
- Permitir el acceso, la eliminación y la transferencia de los elementos específicos de información personal que usted ha recopilado.
- Habilitar un control que permita que los consumidores puedan renunciar a las "ventas" de los datos de los consumidores. Sin embargo, se siguen aceptando determinadas transferencias, como las transferencias a proveedores de servicios.
- Para menores de 16 años, habilitar un proceso de consentimiento para que no se pueda producir ninguna venta de la información personal del menor sin un consentimiento activo para la venta.
- Asegurarse de que no se discrimina a los consumidores que ejerciten cualquiera de sus derechos otorgados por la CCPA.

¿Qué divulgaciones de información requiere la CCPA?

La CCPA obliga a estas divulgaciones de información:

- Categorías de la información personal del consumidor recopilada.
- Categorías de las fuentes usadas en la recopilación.
- Fines empresariales o comerciales para la recopilación.
- Las categorías de terceros con los que se "comparte" la información personal.
- Categorías de información personal "vendida" y categorías de "terceros" a los que se vendió cada categoría de información personal.
- Categorías de información personal que se han "divulgado por un motivo empresarial" (es decir, transferencia sin "venta") y categorías de "terceros" a los que se ha transferido cada categoría de información personal.
- Las partes específicas de la información personal que se han recopilado sobre el consumidor.

¿Cómo se "venden" los datos bajo la CCPA?

La definición de "vender" de la CCPA es muy amplia, incluida "poner la información personal a disposición" de terceros por consideraciones monetarias o de otro carácter oneroso. Cuando un consumidor decida "no participar", el negocio tendrá que desactivar el flujo de información personal a cualquier tercero.

La CCPA determina tres exenciones al control de no participación en la venta. Las tres principales son las transferencias

(I) a un Proveedor de servicios,
(II) a una "entidad exenta" o "contratista" y
(III) en la dirección del consumidor. Incluso si un consumidor ha optado por "no participar", su información personal puede transferirse a otras empresas que encajen en estas exenciones.

Para poder beneficiarse de las dos primeras exenciones, los negocios tendrán que asegurarse de que las transferencias se rijan por contratos escritos que contengan los términos específicos necesarios para la CCPA.

¿Qué significan *Negocios y Proveedores de Servicios* en el contexto de la CCPA?

En el contexto de la CCPA, los Negocios son individuos o entidades que determinan el propósito y el medio del procesamiento de los datos personales del consumidor y los Proveedores de Servicios son las personas o entidades que procesan información en nombre de un Negocio. Por lo general, son sinónimos de los términos Controladores y Procesadores utilizados en el GRPD.

¿A cuánto pueden ascender las multas a las empresas por incumplimiento?

El derecho privado de acción de la CCPA se limita a filtraciones de datos. Bajo el derecho privado de acción, los daños oscilan entre 100 y 750 dólares por incidente y consumidor. El Fiscal General de California también puede aplicar la CCPA en su totalidad para imponer una sanción civil que no supere los 2500 USD por infracción o los 7500 USD por infracción intencional.

¿Qué herramientas pueden ayudar a mi organización a empezar a prepararse para la CCPA?

- Empiece a aprovechar la evaluación de la GDPR en la puntuación de cumplimiento como parte de su programa de privacidad de la CCPA.
- Establezca un proceso de respuesta eficaz a las solicitudes de los clientes.
- Use las capacidades de cifrado de correo electrónico para controlar aún más la información confidencial.

¿Quiénes son los Procesadores y los Controladores?

Un controlador es una persona física o jurídica, una autoridad pública, una agencia u otro organismo que, solo o junto con otros, determina los medios de procesamiento de los datos personales y sus fines. Un procesador es una persona física o jurídica, una autoridad pública, una agencia u otro organismo que procesa datos personales en nombre del responsable.

¿Qué se considera específicamente información personal?

La información personal es cualquier información relacionada con una persona identificada o identificable. No hay distinción entre los roles privados, públicos o laborales de una persona. La definición de la CCPA de la "información personal" es a grandes rasgos similar a la que el GDPR hace de los "datos personales". Sin embargo, la CCPA también incluye datos domésticos y familiares.

Algunos ejemplos de datos personales incluyen:

Identidad

- Nombre
- Dirección del domicilio
- Dirección del trabajo
- Número de teléfono
- Número de celular
- Dirección de correo
- Número de pasaporte
- Documento de identificación nacional
- Número de la Seguridad Social (o equivalente)
- Licencia de conducir
- Información física, psicológica o genética
- Información médica
- Identidad cultural

Finanzas

- Información bancaria y números de cuentas
- Número de identificación fiscal
- Números de tarjetas de crédito y débito
- Publicaciones de las redes sociales

Artefactos en línea

- Publicaciones de las redes sociales
- Dirección IP (región de la UE)
- Datos de ubicación y GPS
- Cookies

¿Cómo se aplica la CCPA a los niños?

- La CCPA introduce obligaciones del consentimiento paterno compatibles con la Ley de Protección de la Privacidad en Línea de los Niños (COPPA) para menores de 13 años.
- En el caso de niños entre 13 y 16 años de edad, la CCPA impone una nueva obligación de obtener el consentimiento del niño a cualquier "venta" de su información personal.

¿Qué ocurre con los datos personales de mis empleados?

En octubre de 2019, se realizaron algunas enmiendas a la CCPA. Una de las enmiendas estableció que las obligaciones de la CCPA no se aplican a la información personal de los empleados de la empresa. Sin embargo, los legisladores han puesto una moratoria de un año a esta exención. Creemos que California elaborará una nueva legislación de protección de datos para empleados en el 2020.

¿Cuáles son las diferencias entre el GDPR y la CCPA?

Hay muchas diferencias. Es más fácil centrarse en las similitudes, entre las que se incluyen:

- Obligaciones de divulgación/transparencia.
- Derechos de consumidor para tener acceso, eliminar y recibir una copia de los datos.
- Definición de "Proveedores de servicio" similar a la definición del GDPR de los "procesadores" y con obligaciones contractuales similares.
- Definición de "negocios" que engloba la definición de "controladores" del GDPR.

La mayor diferencia con la CCPA es la exigencia troncal de permitir la "no participación" de las ventas de datos a terceros ("ventas" se define ampliamente para incluir el uso compartido de los datos con fines onerosos). Esta es una obligación más precisa y específica que la amplia definición que el RGPD hace de la renuncia al procesamiento. Esta engloba este tipo de "venta", pero no la trata de forma específica.

2. BUENAS PRÁCTICAS

- Identifique qué tipo de base de datos tiene en su empresa.
- Clasifique si los datos almacenados requieren o no de autorización del titular. En caso de requerir autorización por parte del titular, tenga en consideración lo indicado previamente en este documento sobre los requisitos y formas de obtener adecuadamente el consentimiento.
- Solicitar el permiso de uso de datos a quienes ya se tienen en la base: Si ya se cuenta con una base de datos, pero aún no se tiene el permiso para el uso de los datos personales que reposan en ella, se debe solicitar expresamente la autorización de los titulares de esos datos, por medio de un correo electrónico o cualquier medio de notificación.
- Los datos personales deben recopilarse para los fines previstos y legítimos, y utilizarse únicamente para dichos fines u otros usos compatibles con aquellos fines.
- Los datos personales deben ser adecuados, relevantes y no excesivos respecto al fin para el cual fueron recopilados y/o tratados posteriormente.
- Los datos personales deben ser correctos y mantenerse actualizados.
- Los datos personales deben ser preservados únicamente por el tiempo requerido para el fin por el que fueron recopilados o procesados posteriormente.
- En el Sitio Web deben publicarse no sólo los Términos y condiciones del sitio web, sino también un enlace visible a sus Políticas de privacidad y tratamiento de datos.
- Si se utilizan formularios para captación de datos de los usuarios, debe verificarse que en ellos se enlacen los Términos y condiciones del sitio web, y la Política de privacidad y tratamiento de datos.
- Activar la limitación para que el envío de mensajes únicamente se haga a los usuarios que han dado consentimiento para ello, por ejemplo, a los usuarios registrados a través de los formularios de registro.
- Activación de una ventana emergente (banner) donde se le informa al usuario que el sitio web utiliza cookies, así como la finalidad de ésta, por ejemplo, mejor experiencia de navegación, analisis de comportamiento, envío de mensajes de su interés, entre otros.

- Ajustar la función de eliminar el contacto para que, sin demora injustificada, se supriman por completo todos los datos almacenados en relación con un usuario, una vez este ha solicitado la eliminación de sus datos personales o, cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados (según GDPR)

- Verificación en los correos electrónicos de la opción para cancelar la suscripción.

- Para el caso de tratamiento de datos de ciudadanos de la UE con residencia permanente o temporal en Colombia y/o destino Colombia, debe aplicar lo descrito en el GDPR en cuanto al tratamiento de datos personales identificables y el debido proceso de notificación.

- Realice una evaluación del proceso de custodia de los datos. Si los datos se transfieren a terceros, se debe establecer que estos emplean al menos un nivel de medidas de seguridad equivalente.

- Identifique las empresas con las que contrata y a las que les permite acceder y tratar las diferentes bases de datos. Se debe tener en cuenta que de acuerdo a la Ley, estos terceros son Encargados del tratamiento de los datos y para su contratación siempre debe existir un documento donde aseguren que va a manejar la información conforme la autorización otorgada por el titular y que dejarán indemne en todo momento al Responsable del tratamiento.

Capitulo 2: Brand Safety

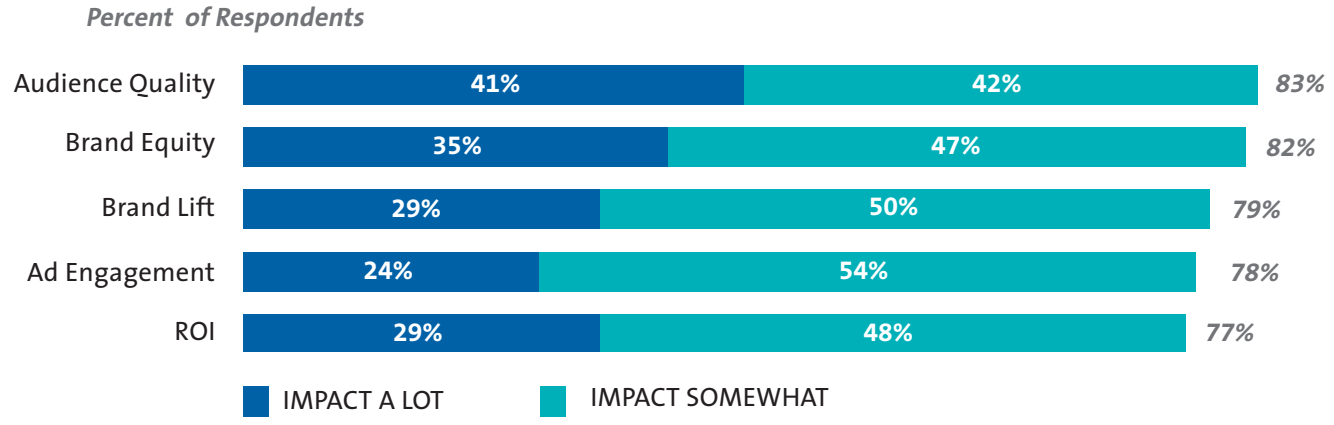
2.1 CONTEXTO ACTUAL

El Brand Safety/Seguridad de la marca, el Ad Fraud/ Fraude Publicitario y el Viewability /Visibilidad Digital, continúan desafiando a los anunciantes digitales y cada vez más los anunciantes demandan claridad, transparencia y confianza en el contenido y calidad de las plataformas en línea en las que están invirtiendo y sus anuncios se están sirviendo en pro de sus consumidores y marcas.

A continuación, presentamos un informe basado en el estudio de DoubleVerify* en 2017.

En la investigación llevada a cabo por "Trusted Media Brands en 2018" se encontró que +70% de los anunciantes encuestados creen que la seguridad de la marca impacta directamente en el ROI de la compañía. Los resultados de esta investigación ponen de relieve el hecho de que el contenido es importante y que colocar anuncios en entornos confiables y seguros para las marcas es determinante para la inversión digital, lo que se considera esencial para la efectividad de la publicidad. Se cree que la publicidad en entornos seguros para la marca tiene un impacto significativo en medidas clave como la calidad de la audiencia - Audience Quality (83%), el valor de la marca - Brand Equity (82%) y el aumento de marca – Brand Lift (79%). Más de tres cuartos de los comercializadores de marcas encuestados creen que la seguridad de la marca tiene un impacto en el ROI (77%).

AUDIENCE QUALITY IS IMPACTED MOST BY ADVERTISING IN A BRAND SAFE ENVIRONMENT AS WELL AS BRAND SUCCESS METRICS



Q. *In your opinion, to what degree are the following positively impacted by advertising in a brand safe environment?*
Base: Involved in Digital/Mobile Advertising

Otras cifras para tener en cuenta:

- Los incidentes de seguridad de marca aumentaron en un 25%.

- El fraude publicitario móvil aumentó en un 800% a medida que las aplicaciones se apropian del presupuesto de medios (el fraude en
aplicaciones es el problema de fraude publicitario de mayor crecimiento en 2018, incluyendo áreas nuevas como la suplantación de aplicaciones, anuncios ocultos y dispositivos móviles secuestrados.)

- La visibilidad mejora en display donde pasa del 52% al 56% y video del 59% al 63%.

- Los contenidos en publishers que transmiten violencia extrema y el discurso del odio casi se triplicaron en 2017.

- Las violaciones a la seguridad de la marca se disparan en un 50% luego de una cobertura noticiosa importante de violencia.

2.2 BUENAS PRÁCTICAS

Para establecer una metodología y principios fundamentales para salvaguardar a los anunciantes y a las marcas de servir anuncios publicitarios directa o indirectamente a través de agencias o trading desk y en portales y/o aplicaciones móviles que puedan afectar el buen nombre de sus productos o servicios y la experiencia de sus consumidores, se plantean los siguientes principios:

4 principios de autorregulación de los anunciantes afiliados a la Asociación Nacional de Anunciantes a poner en práctica en el ecosistema digital:

1. Bloquear el anuncio publicitario publicidad en las páginas que contengan en su HTML concretamente en su descripción, tags, meta tags palabras que considere el anunciante inadecuadas.

2. Bloquear un publisher que no cuente con la certificación Ads.txt (IAB) = Authorized Digital Sellers o cualquier otra certificación técnica para publishers.

3. Bloquear el anuncio publicitario en los dominios y subdominios, considerado inapropiado por el anunciante. Una cadena de texto apropiado en el nombre de dominio o subdominio como: https://www.inapropiado.com o http://www.apropiado.com/inapropiado.

4. En lo posible que se sirva en sitios con certificados de seguridad https://.

2.2.1. Toolkit para la verificación del contenido para la ejecución de la pauta (anunciantes, publishers, agencias).

Si una marca está junto a contenido ofensivo o inapropiado, los consumidores pueden establecer una conexión negativa con la marca. Los compradores de medios deben confiar en la tecnología y buscar garantías de seguridad de la marca con herramientas de verificación de contenido.

Sin embargo, si bien las herramientas apuntan a reducir el riesgo de una ubicación inadecuada, todas trabajan de diferentes maneras para lograrlo y no son infalibles, pero es responsabilidad de todos los actores del ecosistema digital propender por espacios seguros para sus audiencias.

Las herramientas de verificación de contenido juegan un papel determinante en este objetivo. Su tecnología está diseñada para rastrear a través de cientos de páginas web, clasificar el contenido y tomar decisiones sobre si el contenido es apropiado para la campaña publicitaria. Si se considera inapropiado, el anuncio será bloqueado, rescatando a la marca de un entorno potencialmente dañino y desestimulando la generación de contenidos que no construyan sociedad. Las siguientes son las principales herramientas:

vCE – ComScore: Es una solución para validar la entrega de anuncios y audiencia que provee información en tiempo real para mejorar el resultado de las campañas publicitarias, ya sean de display, video o móviles. vCE ofrece un conteo de duplicado de impresiones en una variedad de dimensiones, tales como anuncios vistos, en la geografía correcta, en un entorno seguro para la marca y sin tráfico no humano. También evalúa el grado en el que las impresiones validadas alcanzan la audiencia objetivo de la campaña.

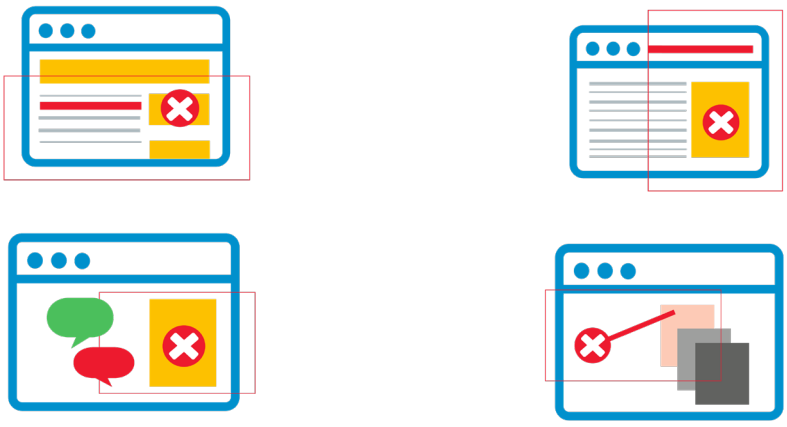
AdSafe firewall – IAS: La tecnología de IAS incorpora una gama de capacidades para la seguridad proactiva de la marca y el bloqueo preventivo de avisos publicitarios. Esta acreditación, junto con la nueva acreditación SIVT de IAS, valida la capacidad de la compañía para detectar y filtrar el tráfico no válido y el contenido inapropiado a lo largo de todo el proceso, desde la detección hasta el bloqueo.

RESULTADOS DE LA PRUEBA			ComScore vCE Validation by comScore		The AdSafe Firewall by Integral Ad Science IAS		DV - Digital IQ Real Time Ad Blocking by	
PRINCIPIO	LA HERRAMIENTA DEBE	PRUEBA	RESULTADO	CONTROL	RESULTADO	CONTROL	RESULTADO	CONTROL
1. BLOQUEO DEL ANUNCIO PUBLICITARIO BASADO EN EL CONTENIDO DEL SITIO								
1	Bloquear la publicación de anuncios publicitarios en páginas que contienen contenido que el anunciante considera inapropiado en el código fuente HTML?	A) ¿Cuando hay palabras inapropiadas identificadas previo a la servida del anuncio?	SI	SI	SI	SI	SI	SI
		B) ¿Cuando hay palabras inapropiadas identificadas después de que el anuncio se sirve?	SI	SI	SI	SI	SI	SI
		C) ¿Cuando existen palabras inapropiadas en los meta tags?	SI	SI	SI	SI	SI	SI
		D) ¿Cuando existen palabras inapropiadas en los alt tags?	SI	SI	SI	SI	SI	SI
		E) ¿Cuando las palabras inapropiadas están en la línea del javascript?	NO	SI	SI	SI	SI	SI
2	Bloquear el anuncio de publicidad en las páginas que contienen palabras en el contenido a través de un archivo vinculado que el anunciante considere inapropiado?	A) ¿Cuando contenido inapropiado es cargado en el publisher a través de linked script?	NO	SI	SI	SI	SI	SI
		B) ¿Cuando se entrega contenido inapropiado en un frame diferente al del anuncio servido?	NO	SI	SI	SI	SI	SI

2. BLOQUEO DEL ANUNCIO PUBLICITARIO BASADO EN URL DEL SITIO								
4	Bloquear el anuncio publicitario en dominios y subdominios considerados inapropiados por el anunciante?	A) ¿Cuando un dominio inapropiado es visitado?	SI	SI	SI	SI	SI	SI
		B) ¿Cuando un sub-dominio inapropiado es visitado?	SI	SI	SI	SI	SI	SI
5	Bloquear el anuncio cuando la URL contiene palabras inapropiadas para el anunciante?	A) ¿Cuando el dominio contiene palabras inapropiadas?	SI	SI	SI	SI	SI	SI
		B) ¿Cuando el sub-dominio contiene palabras inapropiadas?	NO	SI	SI	SI	SI	SI
		C) ¿Cuando el path de la URL contiene palabras inapropiadas?	NO	SI	SI	SI	SI	SI
		D) ¿Cuando el query contiene palabras inapropiadas?	NO	SI	SI	SI	SI	SI
6	¿Bloquear el anuncio publicitario en los alias de la URL o dominio considerado inapropiado por el anunciante?		SI	SI	SI	SI	SI	SI

RealTime AdBlocking: Double Verify (DV): El principal proveedor independiente de software de medición de marketing, datos y análisis que autentica la calidad y efectividad de los medios digitales para las principales marcas y plataformas de medios del mundo. DV proporciona transparencia y responsabilidad de los medios para ofrecer el más alto nivel de calidad de impresión para el máximo rendimiento publicitario.

4 áreas clave para los principios de autorregulación:



Como guía, a continuación se relaciona el comparativo de las principales herramientas en las 4 áreas:

3. BLOQUEO DEL ANUNCIO PUBLICITARIO SI SE REGISTRAN CAMBIOS EN EL CONTENIDO DEL SITIO, URL o INSTRUCCIONES DE CAMPAÑA								
3	Registrar cambios en el contenido de la página y se bloquea el anuncio publicitario en tiempo real?	A) Cuando el contenido agregado recientemente al sitio/página es considerado inapropiado?	NO	N/A	NO	N/A	NO	N/A
		B) Cuando el contenido inapropiado es removido del sitio/página?	NO	N/A	NO	N/A	NO	N/A
9	Tener la capacidad de agregar una lista de palabras claves, URLs, y detectar el tono de sitios/páginas considerados inapropiados por el anunciante previo (2 días hábiles) a que el anuncio se sirva?		SI	N/A	SI	N/A	SI	N/A
10	Tener la capacidad de bloquear la publicación del anuncio en cualquier URL no verificada como "segura" hasta que se conozca su estado, si la identificación del contenido no se realiza en tiempo real?		SI	N/A	SI	N/A	SI	N/A

4. BLOQUEO DEL ANUNCIO PUBLICITARIO SI SE REGISTRAN CAMBIOS EN EL CONTENIDO DEL SITIO, URL o INSTRUCCIONES DE CAMPAÑA								
7	Consultar los iframes del sitio/página y bloquea los anuncios publicitarios si encuentran URL o palabras claves inapropiadas oara el anunciante?	A) Cuando contenido inapropiado es servido dentro del iframe?	SI	SI	SI	SI	SI	SI
		B) Cuando otro anuncio considerado inapropiado por el anunciante es servido a tráves de iframes en la misma página del sitio?	SI	SI	SI	SI	SI	SI
		C) Cuando contenido inapropiado es entregado como objeto?	NO	SI	SI	SI	SI	SI
		D) Cuando se sirve el anuncio como un objeto, en un sitio/página inapropiada?	SI	SI	SI	SI	SI	SI
		E) Cuando contenido inapropiado es servido en la página bajo tags embebidos?	NO	SI	SI	SI	SI	SI
		F) Cuando se sirve un anuncio publicitario vía tag, dentro de un sitio/página considerada inapropiada por su contenido?	SI	SI	SI	SI	SI	SI
		G) Cuando el anuncio publicitario se entrega en 3 iframes anidados, en una página que contiene contenido inapropiado?	NO	SI	SI	SI	SI	SI
		H) Cuando el anuncio publicitario se entrega en 5 iframes anidados, en una página que contiene contenido inapropiado?	NO	SI	SI	SI	SI	SI
8	Operar de manera consistente al permitir o bloquear anuncios cuando el javascript esta deshabilitado?		SI	N/A	SI	N/A	SI	N/A

Capitulo 3: Fuentes de Data dentro del ecosistema digital

Hemos visto que a medida que aumenta la participación de la inversión digital en el mix de medios por parte de los anunciantes y agencias de publicidad, todo un ecosistema paralelo basado en data ha emergido, impulsado por el desarrollo en la recopilación de datos, el uso y las posibilidades de monetización. Los anunciantes y las agencias crean la mayor parte de la demanda de datos, mientras que los editores, las plataformas de publicidad independientes (standalone) y los proveedores de terceros proporcionan suministro de ellos.

Existe una gran cantidad de soluciones, servicios y herramientas relacionadas con los datos para ayudar con las distintas etapas del flujo de ellos. Los DMPs a menudo sirven como centros de datos, ayudados en la recopilación por analítica de sitios web/apps, proveedores de incorporación y soluciones de administración de etiquetas (Tag Managers). La activación de datos, especialmente para la orientación de anuncios, es el dominio de tecnologías que incluyen DSP y proveedores especializados de redireccionamiento, respaldados por servidores de anuncios dedicados (AdServers) y soluciones de medición de anuncios publicitarios.

Finalmente, debido a su naturaleza sensible, el ecosistema de datos está regulado no solo por los organismos de la industria, sino cada vez más a través de agremiaciones, gobiernos nacionales y/o inclusive, supranacionales. Está claro que el ecosistema de datos continuará envolviéndose para cumplir con nuevas oportunidades y restricciones, a través de la consolidación y la apertura de nichos de nuevas tecnologías.

Los datos usados en el marketing y la publicidad digital provienen de diferentes fuentes. Los datos de los sitios web, quizás son la fuente la más relevante, pero en un ecosistema que ha migrado al entorno móvil, estos son ahora quienes marcan la pauta en la ingesta de datos. Cada entorno participante tiene acceso a diferentes tipos de datos. 1st, 2nd y 3rd party data, como se explica a continuación:

SITIOS WEB: Una gran cantidad de la data empleada en la publicidad digital es obtenida de los sitios web ya que la recopilación de datos es relativamente fácil de implementar a escala y ofrece información valiosa sobre el interés, la intención y las características del usuario a menudo, estos datos se recopilan de las propiedades web propias (de una de las partes) o se compran a terceros. Los datos del sitio web se pueden agrupar en tres segmentos: a) Contenido/comportamiento. b) Declarada. c) Data técnica.

Cuando un usuario ingresa a un sitio web, deja una huella que indica el contenido consumido y el comportamiento en su navegador. Por ejemplo, los publishers pueden usar el análisis semántico para producir señales personalizadas de alta calidad relacionadas con el contenido de la página (como un proxy para el interés del usuario).

Los datos declarados se recopilan comúnmente en sitios web a través de formularios de registro, sorteos, cuestionarios, aplicaciones web, compras o configuraciones de preferencias. Estos datos declarados se pueden vincular fácilmente a un usuario y sus dispositivos y ser almacenados durante largos períodos de tiempo.

Los datos técnicos se refieren a los dispositivos utilizados para visitar un sitio web. Las señales incluyen cosas como navegadores, sistema operativo, tipo de dispositivo, idioma o ubicación geográfica.

MOBILE: Cuando los datos vienen del entorno móvil, existen varias fuentes, aplicaciones móviles y sitios web mobile. En particular, hay un tesoro de datos comportamentales y declarados, ya que prácticamente cualquier cosa que un usuario haga con una aplicación puede rastrearse y combinarse con su ID de publicidad exclusiva (IDFA o identificador de publicidad en iOS, AAID / GAID o Google Advertising ID en Android). Esto incluye puntos de datos de comportamiento como ID de la aplicación, duración de la sesión, días desde el último uso, hora del día en que se lanzó la aplicación, resolución del dispositivo, operador, ubicación geográfica, acciones / eventos dentro de la aplicación.

Los sitios web móviles ofrecen datos similares a los sitios web de escritorio, sin embargo, son mucho más difíciles de rastrear, ya que el uso de cookies de terceros e incluso de 1st party está restringido en dispositivos móviles (especialmente en Safari / iOS, que recientemente introdujo la llamada ITP Inteligente de Prevención de Seguimiento).

CAMPAÑAS PUBLICITARIAS: Son grandes fuentes de datos tanto para anunciantes, como cualquier otro jugador dentro del ecosistema que tenga acceso a ellas. Algunos de los datos que se recogen son: impresiones, clics, conversiones, (como leads, y compras), e interacciones. Cuando las campañas publicitarias van acompañadas de un tag correctamente implementado y formulado, pueden entregar datos como: ID de campaña, ID de creatividad e ID de anunciantes entre otros.

HERRAMIENTAS DE ANALÍTICA: Estas herramientas permiten obtener datos que pueden mostrar la granularidad de la visita del usuario, inclusive las plataformas "standalone" a través de pixeles propios instalados en sitios web y aplicaciones móviles, que configurados por eventos o no, generan valiosa información del usuario respecto a los intereses y comportamientos dentro de los sitios web o mobile, generando incluso información no solo descriptiva sino que tienen la posibilidad que tecnológicamente y por algoritmos genere predicciones de comportamiento e intenciones.

CRM: Independientemente de si la base de datos de CRM está online u offline, los datos contenidos dentro pueden ser llevados al entorno digital (a través de una plataforma de datos incorporados) y utilizados para aplicaciones en línea, como análisis de segmentación.

EMAIL DATA: Los datos generados por este canal o plataformas especializadas permiten conocer comportamientos de un usuario basado en el entorno (estatus de suscripción, tasas de apertura, CTR etc..) Hay casos en que la data compartida entre una campaña publicitaria y la plataforma utilizada para envío de correos, permite hacer retargeting permitiendo juntar datos de un entorno outbound a otro inbound.

OTRAS FUENTES DE DATOS: Existen muchas otras fuentes de datos que pueden ser usadas en campañas de pauta y marketing digital. Estos abarcan desde fuentes establecidas con orígenes offline, a través de varios paneles y sistemas POS, hasta flujos de datos modernos y de última generación (wearables, beacons, IoT). Siempre que pueda coincidir con un perfil de usuario digital, la identificación digital, el dispositivo, la huella digital o cualquier punto de datos pueden ser útiles para la orientación de anuncios u otras aplicaciones.

EXTERNAL DATA: Desde la perspectiva de un jugador individual dentro del ecosistema digital, la data externa debe ser vista como un protagonista diferente; esto incluye cualquier proveedor de 2nd o 3rd party, como también los datos disponibles en plataformas standalone/walled-gardens.

MÉTODOS DE CREACIÓN DE DATA

Data declarada: Es aquella entregada por el usuario. Lo valioso de los datos declarados es que usualmente son los más cercanos a la realidad.

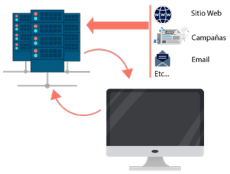
Data Inferida: Los datos inferidos no son entregados directamente por el propio usuario, pero son deducidos, usualmente basados en su comportamiento basado en cookies e IDs.

Data Modelada: Estos datos requieren de un amplio conjunto de datos (data sets) y a través de métodos de encriptación para el traspaso de información (API S2S, Batch o Cookie Sync) o basados en algoritmos de clusterización (k-Means, DBSCAN) y así poder hacer el "match" de un usuario con un perfil deseado.

Propiedad de la Data

La categorización más común sobre el uso de los datos en la industria de la publicidad digital, tiene como base la propiedad/control de los datos, y para ellos podemos distinguir datos de 3 tipos: 1st, 2nd y 3rd party. Esta distinción es desde la perspectiva singular del participante dentro del ecosistema. Puede ser o un anunciante, publisher o agencias.

Cada categoría tiene sus pros y contras, por lo que es común confiar en las 3 cuando se ejecutan campañas publicitarias, analítica u otras aplicaciones.



First Party Data: Esta categoría de datos es recolectada o controlada por los anunciantes o publishers. Esta es la categoría más transparente, valorada y exclusiva de todo el ecosistema. Este tipo de datos pueden ser utilizados para personalizar sitios o aplicaciones móviles para cada usuario de manera que se le enseñe contenido relevante y que genere mayor engagement. El publisher o anunciante podría vender esta data para casos concretos como segmentaciones, retargeting de campañas publicitarias o modelos de negocio como revenue stream. Pero al mismo tiempo esta categoría presenta limitaciones para el uso y la explotación debido a temas legales y de privacidad. A la luz de la normatividad vigente en Colombia, así como del GDPR y otras regulaciones mundiales, la recolección, procesamiento, control y explotación de ella debe hacerse con mucho cuidado y siempre debe contar con el explícito consentimiento del usuario

Second Party Data: Este tipo de datos se obtienen básicamente a través de alianzas (data sharing agreement-DSA) con proveedores de fuentes de datos (publishers / anunciantes) y en esencia es juntar dos fuentes bajo un solo acuerdo; para cada quien el otro participante hace parte de la categoría 2nd party. Una de las ventajas es que se conoce la fuente y la calidad de los datos compartidos, y de esta manera se amplía la escala de la categoría 1st party del interesado. Desde la óptica de las regulaciones, también podría decirse que es una de sus grandes limitantes, ya que el consentimiento del usuario debe ser requerido.

Third Party Data: Estos datos son obtenidos de proveedores externos, quienes no poseen relación directa con el comprador. En el mercado existen muchos proveedores de este tipo de datos que van desde jugadores globales, con una amplia selección de segmentos de audiencia o datos en bruto, hasta un nicho de proveedores locales. Este tipo de categoría de datos se encuentra por todo el ecosistema y sus proveedores se encuentran principalmente integrados a los DMPs, DSPs, Ad Servers y otras plataformas de tecnología para la compra y activación. Las ventajas de esta categoría de datos incluyen: alcance, fácil acceso, y aumentan el ROI de las campañas publicitarias siempre y cuando sean buenos proveedores.

Un excelente caso de 3rd party son las plataformas standalone/walled-gardens como Facebook, Google, Twitter o Amazon. Estas plataformas tienen gran riqueza de datos para segmentación de campañas publicitarias, pero en general restringen su uso solo a la explotación dentro de ellas.

MÉTODOS DE RECOLECCIÓN Y TRANSFERENCIA DE DATOS

Para recopilar y transferir datos a través del ecosistema de publicidad digital, se pueden emplear varios métodos comunes. Para los entornos de sitios web, ya sean de escritorio o móviles, las etiquetas y los píxeles se suelen utilizar para capturar datos y enviarlos a todas las partes relevantes. Data Onboarding es el procedimiento estándar para llevar datos de CRM u otra base de datos offline al entorno online. Los desarrolladores de aplicaciones a menudo implementan un SDK especial para monitorear el comportamiento de los usuarios dentro de la aplicación y reenviarlo a un DMP o proveedor de datos. Para transferir datos entre dos servidores web, se usa comúnmente la integración de servidor directo a servidor directo (S2S) basado en API o el procesamiento por lotes (batch data processing) o la sincronización de cookies (cookie sync) como una tecnología subyacente que permite la transferencia de datos entre S2S.

- **Recolección de datos basada en tags:** Los tags (piezas de código en JavaScript y HTML) es el método estándar de recolectar y transferir web data, un sitio web se carga, el tag contenido en él se carga y se ejecuta (fired).

- **Recolección de datos basada en pixeles:** Un pixel es esencialmente una etiqueta más simple: una pieza de código incrustada en una página web, utilizada para rastrear la actividad del usuario o la transferencia de datos. Por lo general, se implementa como una imagen pequeña invisible (1x1 o un píxel, de ahí el nombre), referenciado a través de una sola línea de código HTML. Los píxeles de seguimiento a menudo son utilizados por terceros para controlar la actividad del usuario en un sitio en particular o en muchos sitios. Otro caso de uso común es la captura de datos de campaña publicitaria (como impresiones, clics, visibilidad, etc.) mediante el pixel de la creatividad. La solicitud disparada por píxeles llega a un servidor web de terceros, lo que le permite enviar estas cookies. Para los editores, es extremadamente importante saber qué píxeles de seguimiento están permitidos en sus sitios web, para proteger sus valiosos datos y la privacidad del usuario.

- **Recolección de datos basada en onboarders:** Plataformas de tecnología que facilita a los anunciantes y ATD incluir data del ecosistema offline (ejemplo: Bases de datos CRM o sistemas POS) en el ecosistema online. Algunos ejemplos de estos son LiveRamp, Neustar y algunos DMP proveen este servicio.

- **Recolección de datos basada en SDK:** Los SDK se utilizan para recoger datos directamente de aplicaciones móviles (entornos nativos) y usualmente ofrecidos por terceros como DMPs o Data Vendors. La data recogida por los SDK usualmente identifica acciones de los usuarios en todo el contexto de la navegación dentro de ella ejemplo (recurrencia, compras, formularios diligenciados, tiempos de permanencia, entre otros).

- **Recolección de datos basada en APIs:** Las API, además de otros usos, facilitan la integración de servidor a servidor [S2S]) y son una forma común de ingerir datos en un DMP/CDP, por ejemplo. En esencia, una API especifica cómo se debe comunicar un servidor (en la forma de métodos aceptados con instrucciones de implementación). Las API se pueden aprovechar para transferir datos en tiempo real o en intervalos regulares.

- **Recolección de datos basada en lotes – Batch data processing:** Con el procesamiento por lotes, los datos se transfieren a intervalos establecidos (por ejemplo, cada hora o una vez al día) entre los servidores web (uno de ellos suele ser un servidor DMP). Los archivos correctamente formateados y nombrados se usan para este propósito, y deben seguir la convención de la plataforma receptora en términos de requerir contenido y sintaxis. El procesamiento de datos por lotes generalmente se implementa cuando la conexión S2S en tiempo real no es posible, o cuando el tiempo no es un factor crítico. Los casos de uso común son: Transferencia de datos de bases de datos offline y personalizadas, ejemplos CRM, así como la ingestión de servidores de anuncios en un DMP.

- **Cookies & Sincronización de cookies:** En el actual ecosistema de datos en publicidad digital, las cookies juegan un rol preponderante para la identificación de un usuario. Mucha información sobre el usuario está atada a las cookies y estas deben ser sincronizadas con un partner de cookies para que los datos se transfieran con éxito. En pocas palabras, las cookies son pequeñas piezas de datos enviados desde un servidor web y almacenadas como archivos de texto en un navegador web. Cada vez que el navegador web realiza una solicitud a un servidor, estos datos se envían al servidor junto con la solicitud.

  A medida que se completa la solicitud, el servidor web también puede actualizar su cookie en el navegador. Las cookies en cada navegador son independientes (es decir, los usuarios con múltiples navegadores utilizados para acceder al mismo servidor web tendrán múltiples cookies del servidor), y solo pueden ser leídos por el dominio del servidor que los configuró. La sincronización de cookies, también llamada coincidencia de cookies, es un proceso de vinculación de cookies relacionadas con el mismo navegador / usuario desde una plataforma de tecnología publicitaria con las de otra plataforma. Esto es necesario porque, como se indicó anteriormente, las cookies solo se pueden leer por el dominio del servidor (es decir, la plataforma) que las configuró y nadie más.

  Plataformas separadas (como DMP y DSP), cada una ha establecido su propia cookie, la sincronización de cookies requerida para saber que las cookies están relacionadas con el mismo usuario y, por lo tanto, es posible la transferencia de datos.

ESTUDIO DE CASO: NUEVO PROTOCOLO DE GOOGLE PRIVACY SANDBOX Y LA ELIMINACIÓN DE LAS COOKIES [5]

PRIVACY SANDBOX

En esencia, se trata de un conjunto de estándares web diseñados para proteger la privacidad de los usuarios que permitirá seguir garantizando a los anunciantes su capacidad para orientar y medir campañas.

Privacy sandbox [6] es un conjunto de estándares web diseñados para proteger la privacidad de los usuarios. Dicho de otra forma, el horizonte que Google vislumbra pasa porque la segmentación de anuncios, la medición y la prevención del fraude se rijan de acuerdo con los estándares establecidos por Privacy sandbox. En base a éste, las cookies se reemplazarán por una serie de interfaces de programación de aplicaciones –APIs–.

Los anunciantes utilizarán cada API en particular para recibir datos agregados sobre problemas como la conversión o la atribución. De esta forma, Privacy Sandbox representa una solución técnica alternativa que Google abre gratuitamente a la industria publicitaria, basándose en nuevos formatos –que no son cookies– para extraer información a través de Chrome en base a los hábitos de navegación de cada usuario. Y ahí es donde surge el primer gran obstáculo: Chrome será el núcleo de la solución.

¿ES PRIVACY SANDBOX LA SOLUCIÓN DEFINITIVA O UN MOVIMIENTO ESTRATÉGICO DE GOOGLE?

La primera respuesta del sector publicitario, del resto de la competencia y de buena parte de los especialistas en marketing y publicidad online ha sido escéptica. Y lo ha sido por dos buenas razones.

Por una parte, el movimiento de Google ha resultado controvertido en lo que a sus competidores directos se refiere.

---

5. Google propone privacy sandbox para sustituir las cookies. - Disponible en https://www.mediasal.es/blog/noticias/google-propone-privacy-sandbox-sustituir-cookies/.
6. Google privacy Sandbox – Chromium: https://www.chromium.org/Home/chromium-privacy/privacy-sandbox.

La propuesta de regirse por el Privacy Sandbox parece una buena solución, pero muchos sospechan que detrás de este movimiento reside la clave que puede asentar las bases de una nueva hegemonía de la empresa americana.

La solución de Google aún está en sus primera fases: no hay herramientas tangibles dentro de Privacy Sandbox, al menos no todavía.

UNA PROPUESTA ABIERTA: PRIVACY SANDBOX EN CHROMIUN

De hecho, y por el momento, Privacy sandbox no puede ser entendido más que como un punto de partida. El inicio de una conversación técnica entre los diferentes actores de la industria del marketing y la comunicación en la que se debe dar forma al futuro de la publicidad digital.

Para favorecer esta dinámica, en la que todas las partes puedan participar, Google ha puesto a disposición del público sus propuestas a través de un apartado en Chromium. Este enfoque trata de evitar las suspicacias ya mencionadas y, sobre todo, dejar de lado las últimas sanciones que han afectado a la compañía por prácticas monopolísticas.

Google ha abierto al público sus propuestas a través de un apartado en Chromium, eso sí, la mayoría de APIs recogidas en la carpeta compartida por Google, como hemos apuntado anteriormente, están aún en sus primeras fases. Lo que sí queda claro es que, ante soluciones más drásticas como el ITP 2.1. las APIs basadas en el navegador son el futuro. Sólo hay un inconveniente: todo está por definir.

Hay una agenda clara. Los dos primeros problemas que el gigante americano intentará abordar a través de sandbox son la medición de la conversión y la publicidad basada en intereses. De hecho, ya se ha anunciado que los ensayos para la medición de conversión basada en clics sin cookies de terceros comenzarán a finales de año 2020.

PRINCIPALES APIS DE PRIVACY SANDBOX

Por el momento, estas son las aplicaciones más llamativas que Google ha abierto a la comunidad de Internet:

1.CONVERSION MEASUREMENT –MEDIDAS DE CONVERSIÓN–

Una propuesta de API de medición de conversiones permitiría a los anunciantes medir e informar sobre las conversiones de clics y el rendimiento de los anuncios sin usar rastreadores de sitios cruzados.

2.FLOC

El aprendizaje federado de cohortes –FLoC–, según la traducción literal del inglés, tendría como objetivo habilitar la publicidad basada en intereses. Esta solución pasaría por evitar rastrear el comportamiento individualizado de cada usuario en la red, fijando una serie de "grupos comportamentales" sobre los que poder extraer conclusiones. Cada uno de estos grupos estaría compuesto por más de mil usuarios con historiales de navegación similares y referidos por un nombre alfanumérico corto.

3.PIGIN

Esta propuesta se encuentra estrechamente relacionada con la anterior. PIGIN es el acrónimo referido a los grupos de interés privados. Estos permitirían al navegador –en lugar de al anunciante– rastrear lo que les interesa a los usuarios para ubicarlos en distintos grupos de interés que podrían servir de orientación. En este sentido, existiría un número mínimo de usuarios dentro de cada PIGIN a fin de evitar mecanismos que pudieran generar un efecto similar al microtargeting convencional.

4.INFORMES AGREGADOS

Una API de informes agregados reuniría la información en un informe único de "preservación de la privacidad» que permitiría la medición de anuncios sin depender de identificadores entre sitios. La API del navegador podría medir el alcance de una campaña o administrar la limitación de frecuencia, y los datos solo se comunicarían si fueran realmente "efectivos".

5.PRESUPUESTO DE PRIVACIDAD

El objetivo de esta propuesta es limitar las huellas digitales. Teóricamente, los sitios web recibirán un presupuesto de privacidad. De esta forma, se limitará la cantidad de información sobre un individuo a la que podrán acceder. Los sitios que excedan ese presupuesto asignado perderían el acceso a las API.

6.MODELO DE PRIVACIDAD PARA LA WEB

Se trata de un modelo de privacidad potencial para la web que plantea una fragmentación de la información de los usuarios. La idea es que se pueda crear un perfil en base a la información recabada a partir de varios usuarios.

Este modelo tiene dos objetivos primordiales. Primero, definir en qué circunstancias debe un navegador permitir que los sitios web traten a una persona como si tuviera una identidad única. Y segundo, dilucidar cómo se puede "jugar" con esos límites de identidad para no poner en peligro la fragmentación de los datos.

En concreto, el navegador debería ser capaz de tratar a terceras parte como primeras, dependiendo de las circunstancias. Si un usuario no identificado visita un sitio, por ejemplo, ciertas terceras partes verificadas tendrían derecho a reconocer al usuario, mientras que otras no.

7.TOKEN DE CONFIANZA

Uno de los puntos más interesantes para los anunciantes. La puesta en marcha de este sistema supondría una ayuda determinante para detectar y prevenir el fraude en este nuevo entorno. El token serviría para discriminar a los usuarios que son de confianza de aquellos que no lo son. Los tokens no se distinguirían entre sí para que los sitios no tuvieran un referente de seguimiento.

8.CONJUNTOS FIRST PARTY

Por último, esta API propone aglutinar en conjuntos todos aquellos dominios relacionados propiedad de una única empresa. De esta manera, como ejemplo, Zara podría aglutinar Zara.de y Zara.es, sus páginas online de Alemania y España, como la misma primera parte. Es decir, aunque la información sobre hábitos de navegación procediese de dos localizaciones distintas, los hábitos de navegación sobre los que trabajar conformarían un único bloque sobre el que extraer conclusiones.

LAS PREOCUPACIONES DE LA INDUSTRIA PUBLICITARIA

Dejando los aspectos técnicos a un lado, Google ya ha dejado claro que está abierto a trabajar con anunciantes y usuarios de Chrome para configurar Privacy sandbox de forma satisfactoria. Por lo pronto, la mayor parte de especialistas rompen una lanza a su favor, en contraposición con un ITP 2.1. que se ha caracterizado por ser mucho más difícil de asumir por parte de la industria publicitaria.

Aún así, cabe preguntarse: ¿Contentará el resultado a todas las partes? ¿Será un movimiento estratégico para afianzar su posición en el futuro? ¿Podría ser el punto de partida que culmine en un identificador universal? De momento, la propuesta está abierta y al alcance de todos. Además, cuenta con el visto bueno del World Wide Web Consortium, lo que supone un apoyo de peso y permite pensar en una estandarización real en el futuro.

El apoyo del World Wide Web Consortium supone un buen punto de partida y permite pensar en una estandarización futura.

Lo que está claro es que tanto Google como la competencia, así como los anunciantes y todas aquellas empresas cuya actividad dependen del ecosistema de internet, tendrán que ponerse de acuerdo.

Las empresas centradas en el marketing one-to-one y la hipersegmentación, haciendo retargeting en base a las cookies, el third party data o utilizando métodos de trackeo sospechosos, se encontrarán un entorno cada vez más complicado. Aquellas otras que confían todo su trabajo en la tecnología para encontrar atajos en el sistema, verán cómo muchas de sus herramientas quedan obsoletas.

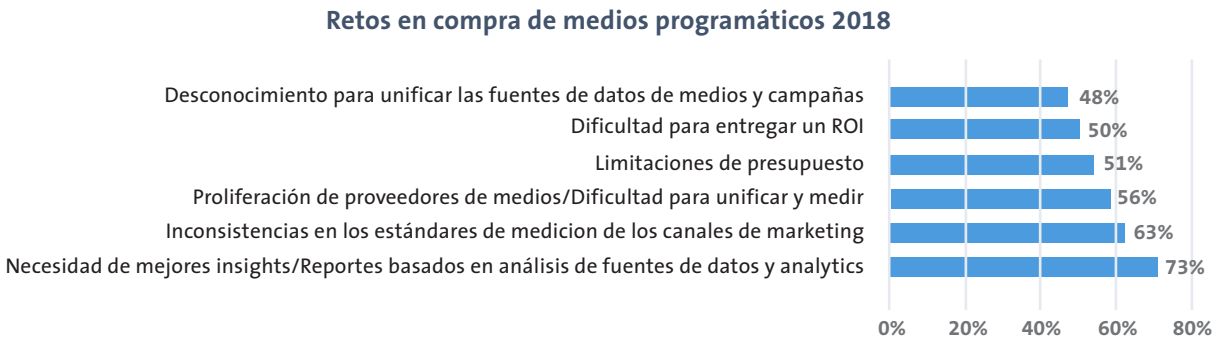
Capitulo 4: Operaciones de compra de pauta programática

4.1 CONTEXTO ACTUAL

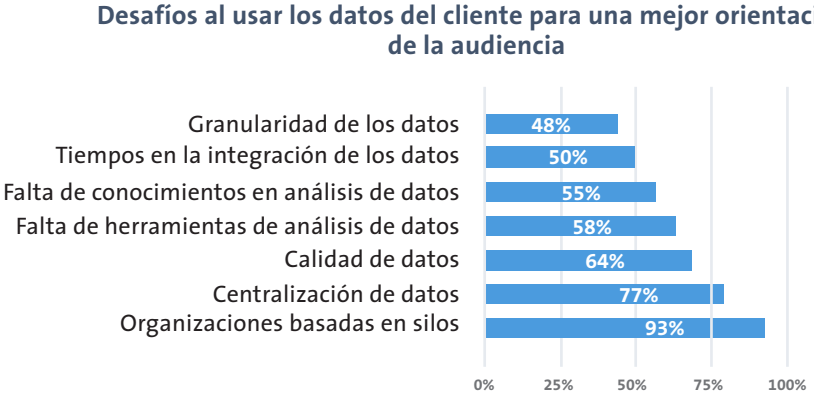
Hoy en día solo el 18%[7] de las marcas/anunciantes en el mundo han tomado el control de las funciones de la agencia de manera *in-house*. Mientras tanto, el 47%[8] se ha dedicado a llevar partes de la compra programática, como medios y estrategia de datos *in-house*, al tiempo que confía en las agencias para funciones especializadas como publicidad, ciencia de datos y codificación, según el informe.

Si bien las marcas quieren llevar la optimización y los análisis *in-house*, a menudo aún no tienen la experiencia y el *know how* para hacerlo, por esto, las agencias están ayudando a las marcas a en sus operaciones programáticas internas.

Según el último estudio de Centro y Advertiser Perceptions 2018 los retos en la compra programática son:



Uno de los retos que se han evidenciado en la compra programática es la proliferación de planeación en pro de formatos y no de audiencias, haciendo que el mercado se inunde de proveedores de tecnología que ofrecen ventajas sobre creatividad y dejan un vacío en la planeación y ejecución orientada a las audiencias. Esto conlleva a un portafolio amplio de medios, pero un vacío en la integración de datos y audiencias; lo que hace más difícil evidenciar un canal de atribución de marketing, pocas veces desarrollado en la industria.



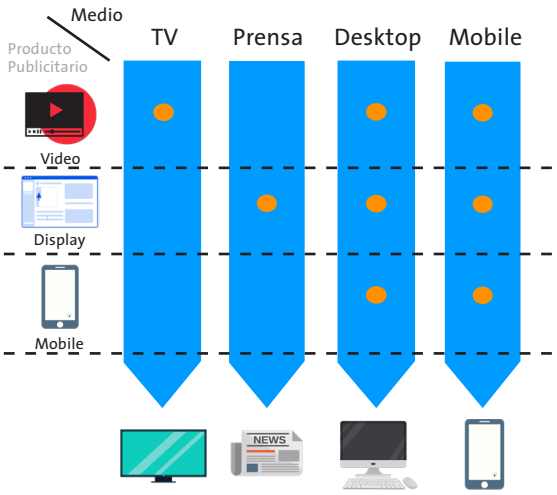
Fuente: Accenture – El futuro de la compra programática 2018-2020

7. IAB 2018 – Artículo " Las agencias caen en roles de especialistas a medida que las marcas llevan a casa la compra programática"
8. Ibid

Las marcas y sus agencias deberán desglosar los silos organizacionales que impactan la publicidad tradicional y digital. La capacitación y la contratación de personal se encuentran entre las principales áreas en las que las marcas y agencias deben planear e invertir en los próximos dos años; perfiles más técnicos en datos y habilidades de integración de datos son fundamentales para construir un modelo efectivo, pero sobre todo escalable en el tiempo. Tales esfuerzos son cruciales para infundir las habilidades digitales, especialmente: analíticas de marketing, analíticas de clientes y analíticas web, tratamientos de datos, formulación de modelos estadísticos, económicos, y aprendizaje automático que son necesarias para sobresalir en la publicidad digital.

Modelo Actual

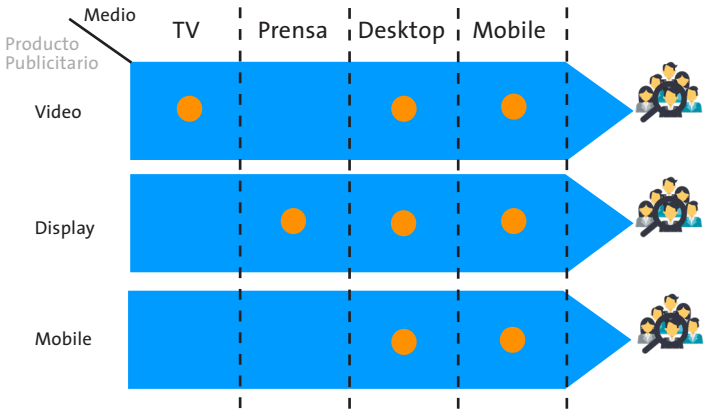
Planeación de medios vertical



- Campaña publicitaria enfocada a los medio (posición).
- Fuerza de ventas organizada por medios.
- Video digital a menudo se vende en paquete con pantalla a bajo precio.

Modelo Ideal

Planeación de medios basado en audiencias



- Campaña publicitaria enfocada en audiencias.
- Fuerza de ventas organizada cross-media por producto.
- Video digital vendido en paquete con TV para mejorar Target y alcance.
- Alcance y monetización del inventario.

El uso creciente de la tecnología y la automatización no cambiará el hecho de que la publicidad siempre será un negocio de personas. Al menos en el futuro previsible, los individuos seguirán siendo responsables de tomar decisiones comerciales y servir a las audiencias y clientes.

La utilización de datos en compra programática genera de forma inmediata, de acuerdo a su implementación, nuevas oportunidades de negocio principalmente en estas áreas:

- Extensión y aumento de inventario para nuevas audiencias.
- Optimización del inventario actual.
- Incremento en los precios de venta del inventario.

- Mejoramiento del proceso.
- Nuevos modelos de negocio basados en datos.
- Procesos de vigilancia y control sobre la pauta de acuerdo con el core de negocio.
- Modelos de planeación acertados por resultados
- Modelos de atribución única digital

La implementación de un modelo basado en datos centralizado en un CoE hace que las marcas y agencias deban afrontar diferente tipos de decisiones:

- Las marcas que deseen tomar total o parcialmente el control de la compra programática *in-house* deben saber que no es tan simple como conectar una pieza de tecnología.
- El modelo de las operaciones de compra programática y medios digitales debería ser compartido por marcas y agencias, y centralizado en una metodología de Centros de Excelencia,CoE, aprobado por la C-Suite bajo estándares de tecnología y gobernabilidad de datos. A través de un correcto análisis, integración y activación de datos inmersas en un CoE se apunta a un objetivo común corporativo, pero más allá, se activan en pro de audiencias determinando cual(es) plataformas son las que mejor desempeño tienen.
- El objetivo de tener la totalidad y/o parte de la compra de medios en el CoE es la propiedad de los datos.
- Datos centralizados, llevan a la integridad de los datos.
- La visión centralizada de datos permite tener el control de la totalidad de la estrategia.
- Una vez aprobado, los comercializadores de medios/agencias deben centralizar y/o crear métodos de transferencia desde o hacia su infraestructura de datos con base a la visión estratégica de la marca o el cliente; coordinar contratos y contratar expertos en análisis de datos, infraestructura y compra de medios para dirigir el CoE
- Una marca debe trasladar la estrategia de datos hacia sus agencias e imponer la medición de un ROMI (Return On Marketing Investment) y ROAS.
- La planificación y ejecución debe ser orientada hacia las audiencias definiendo modelos de atribución medibles y ejecutables.
- Optimizar con base a aprendizajes. Con una visión estratégica basada en datos, con KPIs medibles en tiempo real, plataformas y recursos que pueden comenzar a generar alto rendimiento y nuevos formatos sin el temor de haber pasado por alto cualquier agujero en sus datos.

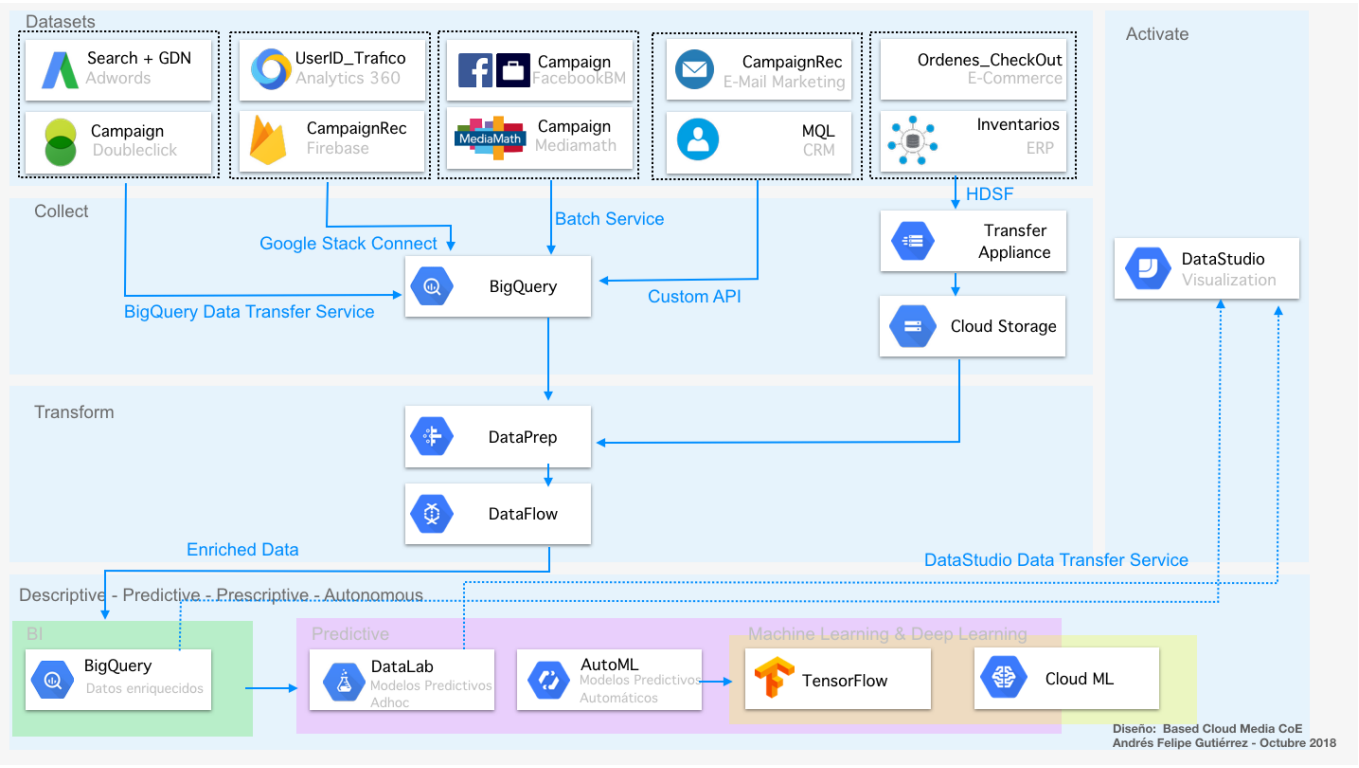


Imagen 1: Arquitectura CoE Digital – Fuente: "From data silos, to end 2 end predictive cloud based solution - Andrés Gutiérrez WebCongress 2018

House Hub / Campaign Overview

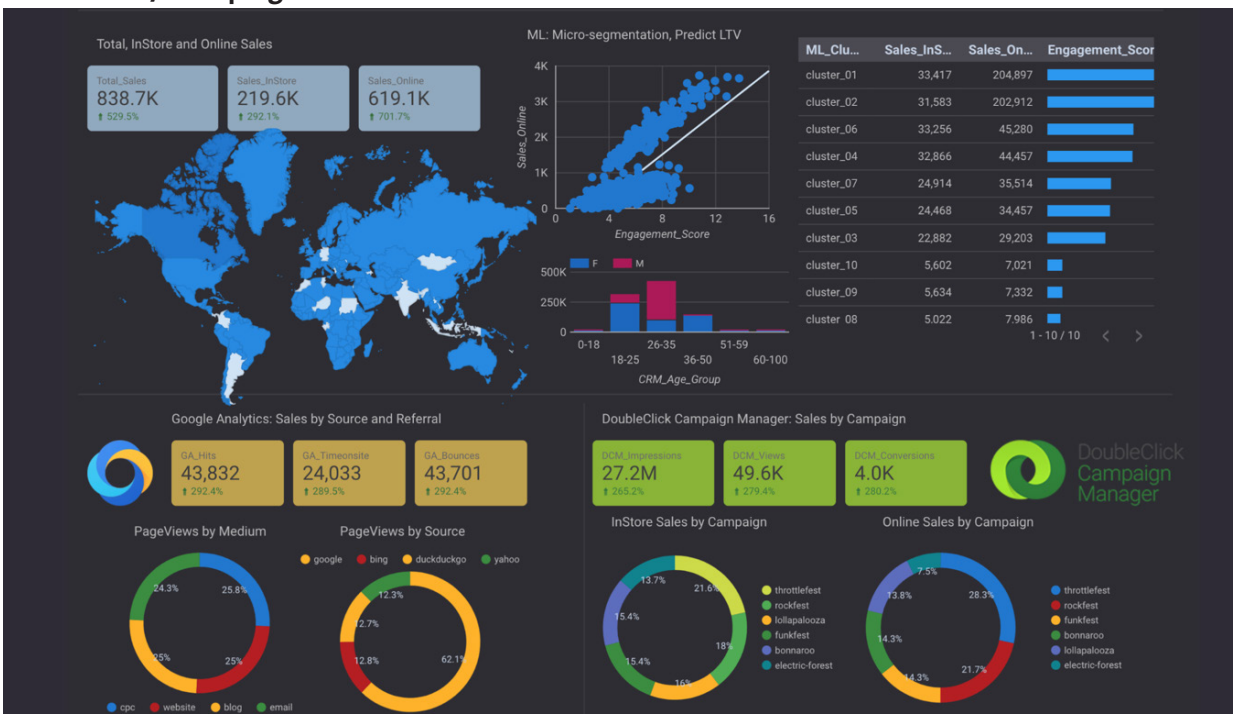


Imagen 2: Dashboard del CoE Digital – Fuente: "From data silos, to end 2 end predictive cloud based solution - Andrés Gutiérrez WebCongress 2018

4.2 PRINCIPIOS

4.2.1. Los datos centralizados, llevan a la integridad de los mismos: El objetivo de generar campañas a través de los diferentes medios, no es más que la recolección de datos a través de una gran cantidad de formatos publicitarios, publishers y canales para distribuir su mensaje junto con todas las plataformas y tecnología publicitaria que facilitan ese proceso. Pero con cada opción de anuncio viene un nuevo origen de datos, y rápidamente se vuelve difícil administrar todos los diferentes flujos de datos en juego. Es por eso que la centralización de los datos es de suma importancia. Tener un lugar para organizar, procesar, analizar sus datos encaminará a los anunciantes y agencias para extraer la mayor información a partir de ellos de manera efectiva, identificando cualquier inconsistencia o error y ganando confianza en su estrategia de publicidad.

Para lograr una sólida integridad de los datos, deberá tener esto en cuenta y liderar una iniciativa, comúnmente conocida como CoE (Center Of Excellence).

4.2.2 Tener la capacidad de poseer su estrategia: Una vez que haya creado una vista completa de todos sus datos, puede comenzar a examinar su estrategia ampliamente. Realice un seguimiento del rendimiento de diferentes canales desde un punto de vista holístico: compras directas frente a programáticas, anuncios de video frente a anuncios de display, anuncios de dispositivo móvil frente a anuncios de escritorio, etc. Dentro de las mismas vistas, comience a investigar cómo sus creatividades están rindiendo con segmentos de audiencia específicos, cómo diferentes canales con los que interactúa o cuál es su retorno de la inversión (ROMI), revise periódicamente el desempeño de las campañas de acuerdo a sus estrategias y hágalo sistemáticamente con el fin de evidenciar buenas prácticas.

Solo una advertencia: Los anunciantes y las agencias deben establecer un marco adecuado con indicadores clave de rendimiento (KPI) antes de comenzar a profundizar en su estrategia de centralización de los datos, dada la complejidad en la cantidad de datos y el riesgo de llegar a conclusiones incorrectas.

4.2.3. Optimice en base a sus aprendizajes: Finalmente, una vez que tenga una comprensión profunda de sus datos, puede comenzar a reinvertir en alto rendimiento y nuevas audiencias. Los anunciantes ya no necesitan depender de terceros para que tomen decisiones por ellos; tienen lo mejor de ambos mundos, ya que poseen recursos, ya sean internos o externos, que pueden ayudar a ejecutar estrategias y cambios efectivos basados en una comprensión sólida de los datos.

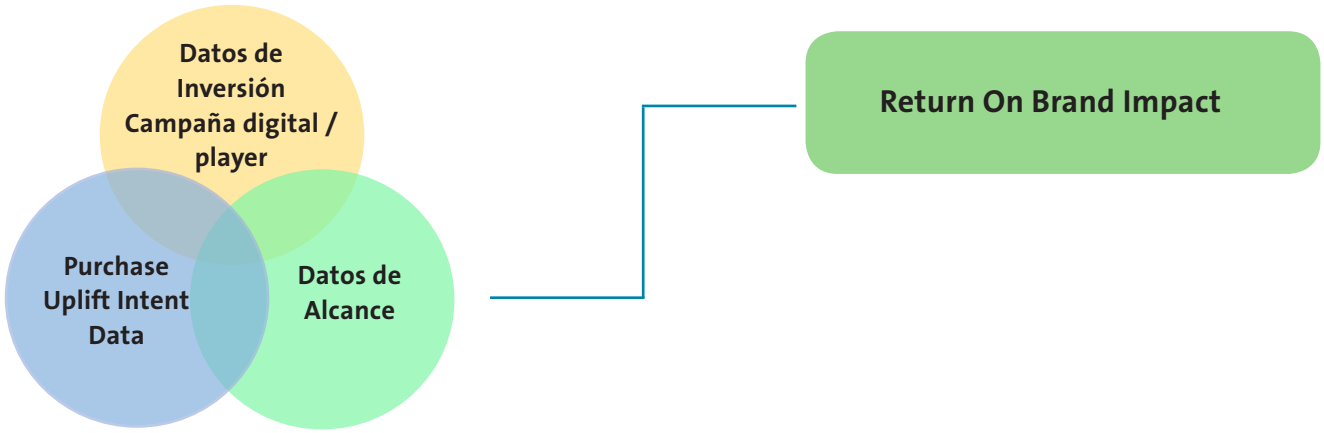
Además, si su compañía ha tardado en reaccionar para convertirse en una organización basada en datos, entonces probablemente debería considerar implementar proceso de cambio y generar un compromiso en todos los niveles del negocio.

Evidencie y genere una bibliografía de reglas y betas, con el fin de identificar en tiempo las buenas prácticas en pro de las marcas con los aprendizajes necesarios para que la agencia y la marca persigan el objetivo de manera mas óptima y rápida.

Lo más importante de migrar a un modelo de medios basado en audiencia es que se optimiza la compra, los formatos, el presupuesto; pero sobretodo, permite diseñar el marketing media mix óptimo ya que a partir de una planificación y ejecución de campañas, recolección, análisis y procesamiento de datos identificando los puntos de contacto de su audiencia.

4.2.5. Cálculo del ROMI (Return On Marketing Investment): Con la adecuada planeación, la visión y el control holístico de su estrategia y la centralidad de sus datos, logrará a que el cálculo del retorno de la inversión en medios sea más sencillo. Si el anunciante decide tener o no el control interno, si debe exigir a sus aliados quienes ejecuten su estrategia que se debe tener un ROMI.

Cuando abordamos el tema de seguridad de la marca, debemos preguntar, ¿cuántos de nosotros tenemos objetivos medibles en nuestras campañas digitales que impacten directamente la marca?. De acuerdo con On-Device Research, solo el 50% de los responsables de mercadeo usan métricas de marca en sus campañas digitales para medir una parte importante de su inversión en mercadeo. El Retorno del Impacto de Marca (ROBI-Return On Brand Impact) a diferencia de métricas, es un KPI que le permite a las marcas comprender el costo incremental por intensión de compra (CIPI), por medios, por formato y la frecuencia de las creatividades, y de esta forma mejorar el ROI mediante el aprendizaje de cada campaña. A través de esta métrica las marcas podrían comprender el costo incremental por intensión de compra (CIPI), por medios, por formato y la frecuencia de las creatividades, y de esta forma mejorar el ROI mediante el aprendizaje de cada campaña.



Variables del ROBI – Fuente: OnDevice Research 2018

1) El Retorno sobre el impacto de la marca (ROBI) implementa el cálculo del Retorno de la inversión en publicidad (ROAS) en las métricas de la marca.

2) ROBI = Valor del comprador incremental / Costo del incremento comprador.

3) Los mismos cálculos se pueden utilizar para otras métricas de marca, como el conocimiento y la consideración según los objetivos de la campaña.

4) Análisis de ROBI por media partner, DSP, creativo y plataforma permite un campo de juego nivelado al evaluar el impacto de la marca en los diferentes partners de tecnología.

	Impressions	Unique Users Reach	FreqCap	Cost USD	Purchase Intent Uplift	Incremental Purchase Intenders	Cost Per Incremental Purchase Intender - CPIP
Campaña sin optimización	3.000.000	1.000.000	3	$30.000	12,5%	125.000	$0,24
Creatividad 1	3.000.000	500.000	3	$15.000	8,0%	40.000	$0,38
Creatividad 2	3.000.000	500.000	3	$15.000	17,0%	85.000	$0,18
Campaña Optimizada							
Creatividad 2	3.000.000	1.000.000	3	$30.000	17%	17.000	$0,18
Purchase Intenders						45.000	
% Purchase Intenders						36,0%	

METRIC	VALUE
Value of incremental purchaser (unit cost of Brand X)	$1,50
ROBI Creative 1 (Value of Incremental Purchaser/CPIP)	$4,0
ROBI Optimized	8,5

Glosario

Para comprender la importancia de crear principios y compromisos de autorregulación en los ecosistemas digitales, es necesario conocer quiénes son los integrantes de la cadena de valor de la compra en medios. A continuación, encontrará un glosario para identificar su rol, el de sus pares y los actores que debe tener en cuenta en los procesos de pauta publicitaria.

- **ANUNCIANTE:** Individuo u organización que contrata un espacio publicitario para anunciar sus productos y servicios.

- **AGENCIA:** Empresa de comunicaciones dedicada principalmente al desarrollo de estrategias creativas de difusión, branding y posicionamiento en los diferentes canales de comunicación.

- **AGENCY TRADING DESK (ATD):** Equipo dentro de una agencia de publicidad que ejecuta la compra de medios en línea como un servicio administrado. Utilizan tecnología patentada o una plataforma de demanda (DSP) para comprar y optimizar campañas de medios en intercambios publicitarios (AdExchange), redes publicitarias y otras fuentes de inventario disponibles con las que están conectadas con diferentes fuentes de información de audiencias propias o de terceros, resultantes de la captura sistemática de cookies y/o devices ID, con el fin de unificar y optimizar la compra en un único alcance multiplataforma.

- **AD EXCHANGES:** Es el punto de encuentro online en el que oferta y demanda se unen para llevar a cabo las transacciones de compra y venta de espacios publicitarios. Permite que medios y anunciantes lleven a cabo el proceso comercial, generalmente en formato Real Time Branding, obteniendo el mejor rendimiento para todas las partes.
  El Ad Exchange es el motor principal de la subasta en tiempo real, reúne los espacios publicitarios proporcionados por las plataformas SSP, encargadas de reunir a los oferentes de espacios (Publishers), y elabora la puja enviada a las plataformas DSP, encargadas de llevar a cabo el acuerdo en nombre de las firmas anunciantes.

- **AD SERVERS:** Es un almacenamiento para contenido publicitario utilizado en Marketing Digital para toma de decisiones automáticas sobre qué anuncios mostrar en un sitio web disponible y publican los anuncios en los mismos de acuerdo con los criterios de configuración. También recopilan e informan datos (como impresiones, clics, etc.) para que los anunciantes y/o agencias obtengan información y controlen el rendimiento de sus anuncios.

- **SUPPLY SIDE PLATFORMS (SSP):** es una plataforma tecnológica de gestión comercial automatizada que permite a los Publishers administrar su inventario de espacio publicitario y recibir ingresos.

- **BRANDSAFETY:** La implementación de un aviso publicitario en formatos de display, video y nativos que no estén adyacentes a contenido online que sea ilegal (en contra de la ley), ilegítimo (temas controversiales y poco aceptados por el público) o inadecuado para la imagen de la marca.

- **PROVEEDORES DE MEDICION PUBLICITARIA:** Tecnología que permite a los anunciantes evaluar la calidad de las impresiones individuales del publisher e influir en la toma de decisiones antes de pujar. La calidad se evalúa en gran medida contra la visibilidad, el contenido, la seguridad de la marca y / o el fraude. La tecnología a menudo ofrece la opción de bloquear el anuncio según la medición.

- **COMPRA PROGRAMÁTICA:** La compra masiva y automatizada de espacios publicitarios en medios digitales (sitios web y/o aplicaciones nativas descargadas en dispositivos móviles a través de plataformas conocidas como DSPs.) de acuerdo a criterios de segmentaciones avanzadas como comportamientos de audiencias, criterios identificados o predictivos de las cookies o device ID que se alimenta sistemáticamente de diferentes fuentes proveedoras de dichos comportamientos.

- **DATA MANAGEMENT PLATFORMS (DMP):** Es una plataforma de gestión de datos centralizada que permite a los anunciantes crear audiencias basándose en una combinación de datos de diferentes fuentes. Por tanto, lo que caracteriza a las DMP es que son plataformas tecnológicas que ayudan a recolectar, integrar y gestionar enormes cantidades de datos, estructurados o no.

  Estos datos pueden ser de distintos tipos:
  - La propia web del anunciante.
  - Campañas de email marketing.
  - Dispositivos móviles.
  - Espacios propios en redes sociales.
  - Acciones de display.
  - Datos proporcionados por los clientes y agrupados en la herramienta CRM.

- **DEMAND SIDE PLATFORMS (DSP):** Plataforma tecnológica de gestión comercial automatizada que permite gestionar el acceso a los diversos inventarios publicitarios (AdExchanges), para maximizar la inversión en medios digitales.

- **GDPR-General Data Protection Regulation:** Es un reglamento destinado a reforzar y armonizar la protección de datos en la Unión Económica Europea, aplicable desde el 25 de mayo de 2018. Se aplica tanto a empresas de la UE como a empresas extranjeras que procesan datos de residentes de la UE.

- **PUBLISHERS:** Son los propietarios de portales web y aplicaciones, y las principales fuentes de data en el ecosistema de pauta digital. Cuando un usuario interactúa con alguno de ellos, su comportamiento puede ser identificado y rastreado por ellos mismos o terceros.

- **PLATAFORMAS DE PUBLICIDAD STANDALONE – "WALLED GARDENS":** Facebook, Google, Twitter son algunos de los ejemplos más claros de este tipo de plataformas que prosperan en data. Con millones de usuarios activos, tienen acceso a data de calidad como intereses, intensiones, sociodemográfica. Estas plataformas ofrecen de manera eficiente no solo inventario, sino una segmentación. Se conocen como walled gardens por que controlan y restringen el flujo de data para plataformas por fuera de su ecosistema (stack).

- **RETARGETERS:** Son vendedores especializados que se enfocan en maximizar el rendimiento de la data propia (1st Party Data). Como objetivo de negocio, retargeting es impactar usuarios que ya han estado en algún Publisher y que han mostrado interés por un producto o servicio. Algunos de los más populares en el mercado son: Criteo, AdRoll, ReTargeter y RTB House.

- **ROMI - RETURN ON MARKETING INVESTMENTS:** Es el retorno que obtiene un anunciante sobre los esfuerzos/costos asociados en publicidad y mercadeo también se puede llamar ROI (Este incluye otro long tail de costos).

Nuestros Afiliados

anda

Asociación Nacional de Anunciantes de **Colombia**

www.andacol.com

AndaCol
ANDA Asociación Nacional de Anunciantes de Colombia
ANDA Colombia