CONFI*MOS EN LOS D*TOS

Guía para conseguir la confianza del cliente a través de la privacidad

TEALIUM®

Prólogo

La privacidad se ha convertido en uno de los principales aspectos que las organizaciones tienen en cuenta y al que prestan especial atención. Cualquier negocio que se base en los datos y tenga que procesar datos personales debe dar prioridad a la privacidad de los datos y tener una perspectiva reflexiva en cuanto al modo de recopilar y usar esos datos.

La privacidad de los datos varía de unos países a otros, y por eso es importante comprender las distintas normativas. Europa tiene el Reglamento General de Protección de Datos (RGPD) y Estados Unidos tiene la Ley de Privacidad del Consumidor de California (CCPA), que pronto pasará a ser la Ley de Derechos de Privacidad de California (CPRA). Japón y Australia también cuentan con sus propias normativas federales. Todas las normativas sobre privacidad evolucionan continuamente, ya que los organismos reguladores comparten información sobre casos en los que deben aplicarse, además de directrices para explicar cómo lograr su cumplimiento. Por este motivo, estar preparados y responder adecuadamente puede suponer todo un reto para una empresa.

Todas las principales normativas sobre privacidad ponen al cliente al mando, es decir, le permiten decidir qué datos desea compartir. Así pues, los consumidores pueden proporcionar menos datos personales, pero, al mismo tiempo, esperan que una organización les ofrezca experiencias relevantes y personalizadas.

Esto supone un reto para todas las empresas: tener una conversación con los clientes que se base en las ventajas, con la privacidad al frente de todas.

Un enfoque que las organizaciones modernas están adoptando incluye contar con una estrategia de datos donde se dé prioridad a la privacidad. Un componente tecnológico clave de esa estrategia es una Plataforma de Datos de Cliente. Con un CDP es más fácil tener la seguridad de que se recopilan los datos correctos y se activan en los canales respectivos y, lo más importante, que se respetan las preferencias de privacidad durante todo el proceso. Anteriormente, los datos de un cliente incluían el historial de compras y las acciones que llevaba a cabo en una página web. Ahora hay muchos más datos disponibles para recopilar, lo que significa que las empresas deben identificar datos de calidad y respetar las preferencias de privacidad del usuario final. Los CDP ayudan a las empresas a ofrecer al comprador el tipo de contenido, la oferta y la información oportunas en el momento justo. Esto facilita la creación de una relación de confianza con el comprador, algo fundamental en la actualidad.

Los CDP se están convirtiendo en un componente básico para la mayoría de las empresas, porque permiten a los equipos organizar las preferencias de privacidad necesarias, añadir o quitar activaciones de proveedores, cambiar la implementación y modificar los eventos que se comparten.

Incluso a pesar de que las normativas sobre privacidad cambian continuamente y son necesarias nuevas formas de gestionar los datos de los clientes, las empresas pueden ofrecer experiencias y momentos extraordinarios que deleiten a sus clientes. En este libro se tratan los aspectos fundamentales de un modo conciso y práctico. Puede parecer desalentador, pero estamos aquí para ayudarle. Nuestro objetivo es extraer la complejidad, de modo que los equipos puedan empezar ya con la tecnología adecuada para sustentar una estrategia de datos que dé prioridad a la privacidad.

– Julián Llorente Perdigones, Director of Data Privacy en Tealium

Introducción

En el mundo actual basado en los datos y la privacidad, es imperativo para las empresas ofrecer claridad a sus clientes sobre por qué, cómo y qué información personal desean procesar y compartir con terceros. Esto no solo es necesario para cumplir las normativas sobre privacidad, que cambian constantemente, como el Reglamento General de Protección de Datos (RGPD) y la Ley de Privacidad del Consumidor de California (CCPA), sino que también es una necesidad para establecer una relación de confianza con el cliente. Cuando se proporciona a los clientes una experiencia relevante y útil a cambio de sus datos, se refuerza la confianza de esos clientes en su negocio y la fidelidad a su marca. Por eso, aunque obtener el consentimiento y cumplir la legislación en materia de privacidad es un gran comienzo, es aún más importante que utilice los datos de sus clientes para beneficiarlos, ofreciéndoles experiencias increíbles y de confianza.

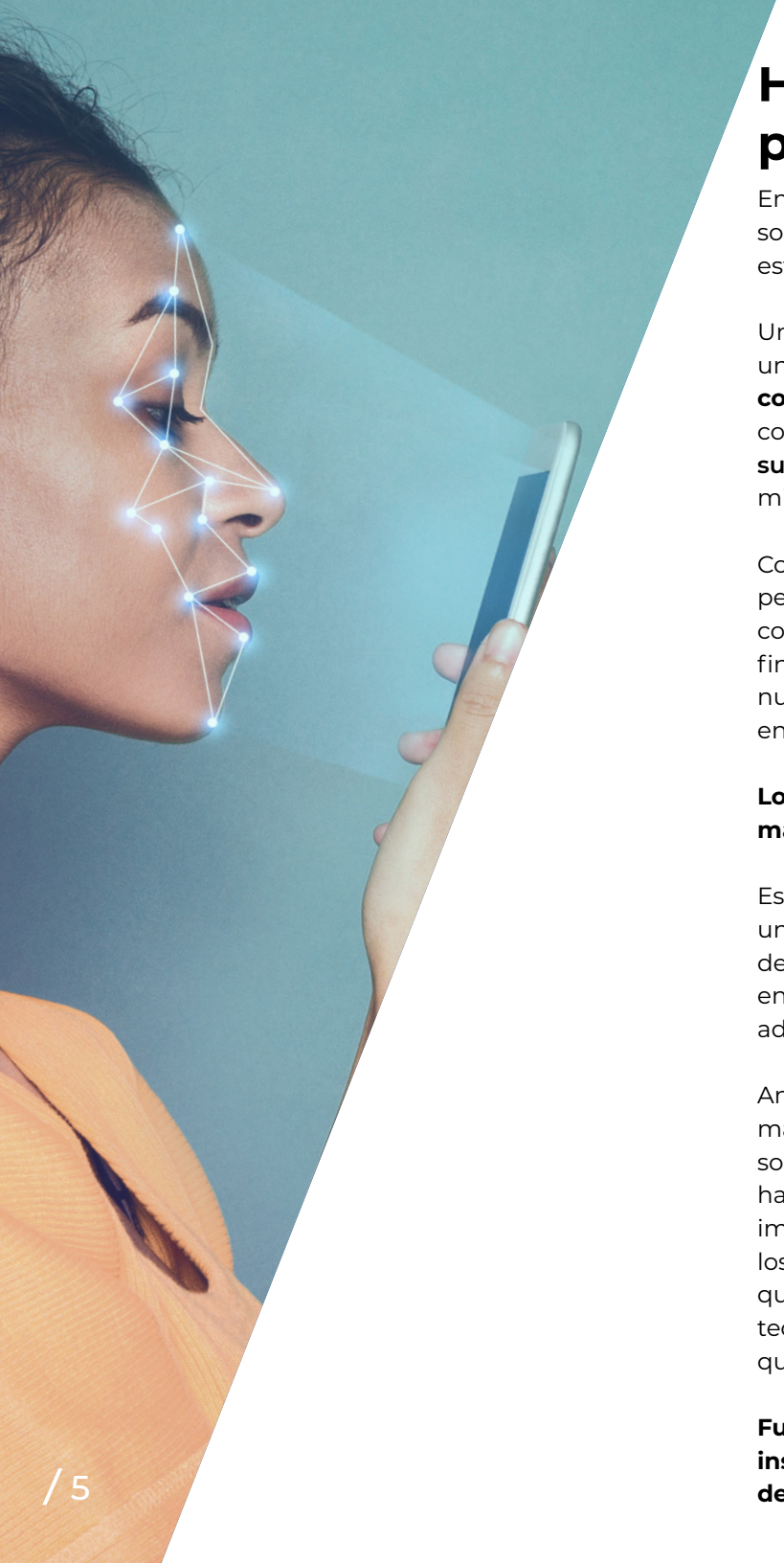
Los consumidores valoran la confianza digital
Los consumidores afirman que la confianza digital es realmente importante y muchos se irán a otra parte cuando las empresas no la proporcionen.

Las empresas deben generar confianza ahora

Al igual que en cualquier otra relación, una persona debe generar credibilidad para que otra persona confíe en ti. Lo mismo ocurre con las relaciones entre empresas y consumidores. Hoy en día, muchas empresas utilizan modelos de intercambio de valor donde ofrecen algún beneficio a cambio de los datos del cliente; por ejemplo, una dirección de correo electrónico a cambio de un descuento del 50 % en un artículo. Los clientes son conscientes de que se está recopilando y rastreando su información, pero esperan tener una experiencia de confianza con la marca. Para hacer esto posible, las empresas necesitan un socio de confianza y tecnología con la que sentar las bases para recopilar, transformar, orquestar y activar los datos de los clientes basándose en la privacidad.

No establecer y mantener la confianza conlleva un coste

Las marcas se benefician cuando mantienen la confianza de los clientes, pero también pueden incurrir en costes importantes cuando pierden esa confianza. Cuando los clientes gastan dinero en una marca, confían en que el servicio o producto que han adquirido cumplirá ciertas expectativas de calidad. De igual modo, cuando un cliente proporciona datos a una marca, espera que la marca los use de forma responsable. En ambos casos, el resultado es un precio muy elevado: **el 71 % de los encuestados con los que PwC elaboró un estudio rafirmó que compraría menos a una empresa en la que ya no confíe.** De ese grupo, **el 73 % dijo que gastaría mucho menos.** Los clientes quieren confiar en las marcas que les gustan y, como revela nuestro estudio, una vez que se pierde la confianza, es casi imposible recuperarla. **El 85 % de los clientes no perdonará los errores de una empresa, aunque antes haya confiado en ella.**



Historia de las normativas sobre la privacidad de los datos

En la era digital compartimos más información personal que nunca. Ya sea a través de los medios sociales, las citas online o incluso con una simple búsqueda en Google, nuestros datos privados están ahí, en el mundo.

Uno de los socios de Tealium, Sailthru, una plataforma de marketing multicanal, llevó a cabo una encuesta recientemente en la que **«el 81 % de los encuestados manifestó su voluntad de compartir datos personales para conseguir las ventajas que ofrecen los programas de fidelidad** con un comerciante minorista o una marca de confianza, y **el 70 % estaba dispuesto a compartir sus datos para obtener ofertas y descuentos especiales** con una marca o un comerciante minorista de confianza».

Compartir información personal con las empresas con las que interactuamos permite una personalización importante que influye en nuestra vida cotidiana, como la exposición a conocimientos médicos basados en un análisis de la salud en tiempo real, el asesoramiento financiero basado en el estilo de vida y los hábitos de consumo, ofertas de productos que reflejen nuestra individualidad única y experiencias personalizadas que mejoren aún más los viajes y el entretenimiento, por nombrar solo algunos ejemplos.

Los dos factores más importantes para una relación digital de confianza entre un cliente y una marca son la transparencia y el valor.

Esto supone explicar qué tratamiento se dará a los datos de los clientes y con qué fin, utilizando un lenguaje claro que todos los clientes entiendan. Las empresas que se basan en los datos deben establecer una estrategia de datos eficaz que aborde este reto, cuyos objetivos se centran en comprender el valor de los datos de los clientes y las responsabilidades inherentes a una administración efectiva.

Antes de la entrada en vigor del RGPD en 2018, las empresas recopilaban datos con fines de marketing, pero sin el consentimiento de los clientes. Sin duda, ya se conocían bien los avisos sobre el uso de cookies y las políticas de privacidad, pero los marcos eran todos diferentes y no había normas jurídicas ni sectoriales que pudieran ayudar a los clientes a comprender por qué era importante un intercambio de valor. En esos años, para poder rechazar la aparición de publicidad, los clientes tenían que seguir vínculos a sistemas externos de terceros que presuntamente los quitaban de una publicidad dirigida a una audiencia incipiente con cientos de proveedores de tecnología diferentes, cuyos nombres no conocía la mayoría de la gente y tampoco entendía qué hacían.

Fue este ambiente de perplejidad el que dio lugar al primer paso, y el más importante, hacia la institucionalización de las normativas sobre privacidad: la obtención y gestión del consentimiento.

Cronología de la privacidad de los datos en el marketing digital

2009
Se propone no rastrear el encabezado HTML

2016
Entra en vigor el Escudo de la privacidad (Privacy Shield)

2017
Apple introduce Intelligent Tracking Protection (ITP)

2018
Entra en vigor el Reglamento General de Protección de Datos (RGPD)

2019
Firefox bloquea las cookies de terceros
Google anuncia Privacy Sandbox y el atributo «SameSite» para las cookies

2020
Se invalida el Escudo de la privacidad (Privacy Shield), entran en vigor la Ley de Privacidad del Consumidor de California (CCPA) y la Ley de Derechos de Privacidad de California (CPRA)
Safari bloquea las cookies de terceros
Facebook implementa la API de conversiones (CAPI)

2021
Se implementa App Tracking Transparency (ATT), la UE investiga Google Privacy Sandbox
Apple implementa la opción para aceptar o no el acceso al IDFA
Android anuncia la implementación de la opción para aceptar o rechazar el uso del AAID

2022
Se elabora el borrador de la Ley Federal de Privacidad y Protección de Datos de Estados Unidos (ADDPA)
La FTC comienza a estudiar normas para proteger con firmeza la seguridad de los datos

2024
Chrome bloquea todas las cookies de terceros

El requisito de obtener el consentimiento ha obligado a las empresas a detallar qué datos desean procesar, con qué fin y con quién los van a compartir, dando la opción al cliente de decidir si acepta o no tales actividades. Esto significa que el cliente ahora tiene el poder legítimo de decidir cuándo y cómo se usan sus datos.

> Esta transparencia en cuanto al modo en el que se utilizarán los datos de los clientes crea una base de confianza y las empresas que adopten esta estrategia desarrollarán relaciones de confianza con sus clientes y, en definitiva, disfrutarán de una ventaja competitiva ahora y en el futuro.

A medida que la industria avanza con la innovación en las tecnologías de inteligencia artificial, el marketing digital y las técnicas de engagement de clientes, los datos de los clientes se han convertido en el elemento fundamental que determina el nivel de éxito que se puede alcanzar. El consentimiento es la clave para aprovechar todo el potencial de nuestras inversiones en innovación, ya que permite a las empresas utilizar la información de los clientes para impulsar experiencias y servicios modernos a lo largo del recorrido del usuario, lo que implica un omnicanal de dispositivos y sistemas, todos ellos con necesidades diferentes en cuanto a la protección de los datos personales y el marketing de marca.

En las secciones siguientes veremos con más detenimiento cómo las Plataformas de Datos de Cliente (CDP), y en concreto el CDP de Tealium, convierten la privacidad y la confianza de los clientes en una ventaja estratégica. Ofrecemos consejos reales proporcionados por expertos en privacidad y profesionales del marketing sobre cómo impulsar la transparencia necesaria para establecer la privacidad por diseño. Aclaramos quién es ahora responsable de recopilar y proteger los datos de clientes, y damos una idea general de cómo es el equipo de privacidad ideal y del enfoque necesario para abordar la complejidad de las normativas sobre privacidad de todo el mundo.

Las complejas necesidades de los clientes en relación con sus datos requieren soluciones sencillas y flexibles

Los clientes esperan que las marcas con las que interactúan los comprendan, sepan quiénes son y, en definitiva, les ofrezcan una experiencia de usuario óptima. Por otro lado, también esperan que las marcas respeten sus derechos de privacidad de los datos, que ahora están oficialmente documentados y se han impuesto en todo el mundo. A esto se le denomina con frecuencia la «paradoja de la privacidad».

Paradoja de la privacidad
Gartner ha acuñado el término «paradoja de la privacidad» para referirse a la incoherencia entre la preocupación de los clientes por la privacidad y su comportamiento y sus deseos reales online.

Por un lado, según una encuesta llevada a cabo por nuestro partner Merkle, **«un 88 % de los consumidores consideran que los productos de una marca son de más calidad** si sienten que la marca presta atención a sus necesidades. El 91 % de los consumidores es ligeramente más propenso o muy propenso a repetir una compra si sienten que les han escuchado». Por otro lado, según un estudio realizado por Pew Research Center, **«el 81 % del público afirma que el riesgo potencial al que se enfrentan por la recopilación de datos** que llevan a cabo las empresas supera a las ventajas». Y **«a un 79 % de los consumidores les preocupa** la forma en la que las empresas utilizan los datos recopilados».

Para recopilar, enriquecer y activar los datos de clientes de un modo que cumpla las normativas sobre privacidad y a la vez ofrezca experiencias increíbles, las empresas necesitan una solución flexible y neutra respecto al proveedor que se integre con todo su stack tecnológico de marketing, y esa solución es una Plataforma de Datos de Cliente (CDP).

Un CDP puede estar en el centro de la cadena de suministro de datos y facilitar la gestión de los datos de clientes y la privacidad de los datos al mismo tiempo. Ofrecer una gran experiencia y satisfacer las preferencias de privacidad es posible.

La paradoja de la privacidad en números

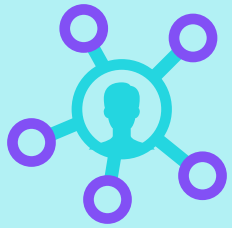
El 91 % de los consumidores es ligeramente más propenso o muy propenso a repetir una compra si sienten que han escuchado sus necesidades

El 81 % del público afirma que el riesgo potencial al que se enfrentan por la recopilación de datos que llevan a cabo las empresas supera a las ventajas.

Cinco formas en las que un CDP genera la confianza de los clientes en los datos

1 Reducir el riesgo de los datos en silos

Los silos de datos dan lugar a procesos costosos y a un aumento del riesgo en diferentes áreas, como duplicación, conjuntos de datos obsoletos y un concepto erróneo o fracturado de los perfiles de los clientes, lo que lleva a malgastar el presupuesto de marketing y a elaborar estrategias equivocadas. Estos silos impiden que su organización maximice la experiencia del cliente y pueden llevarla a correr el riesgo de cometer infracciones en materia de privacidad. Si un departamento gestiona los datos de clientes de una forma diferente a como lo hace otro departamento, significa que sus equipos están hablando un idioma diferente y no están atendiendo la petición de una gestión constante de la privacidad de los datos. Un CDP que comience con la recopilación de datos ayudará a su organización a eliminar estos silos y a reducir el riesgo de incumplimiento normativo.

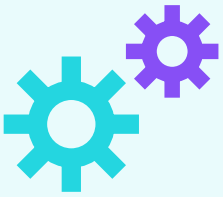


2 Propagar las preferencias de privacidad

Si los datos sobre el consentimiento no se gestionan en tiempo real, pone a su organización en riesgo e incluso puede incumplir las normativas sobre privacidad sin saberlo mientras las preferencias de consentimiento esperan quizá a ser actualizadas. Por ejemplo, si alguien solicita que se eliminen sus datos y la organización tarda más de lo que dicta la ley en satisfacer esa petición, puede enfrentarse a importantes sanciones por no cumplir la solicitud de acceso del interesado. Así pues, es fundamental propagar la privacidad a todo el recorrido del usuario, en todos los canales, y mantenerla desde la perspectiva del cliente. El cumplimiento de la privacidad por canal no es realmente una práctica conforme con la normativa y conlleva el riesgo de cometer infracciones.

3 Facilitar la eficiencia operativa y la agilidad empresarial

Para ser una organización que se basa en la privacidad, las empresas deben eliminar los silos de datos y de comunicación para comprender qué datos se procesan y por qué. El CDP de Tealium aplica una nomenclatura común para los datos que permite a las empresas y a los departamentos de informática hablar un mismo idioma de forma coherente. Este esquema de datos universal elimina cualquier riesgo de que un departamento se quede atrás respecto a otro cuando cambien los requisitos de privacidad o cuando nuevas inversiones en tecnología exijan nuevas integraciones.



Cinco formas en las que un CDP genera la confianza de los clientes en los datos

4 Ofrecer transparencia a los clientes y entregarles el control de sus datos

Sus clientes cuentan con el respaldo de las normativas sobre privacidad internacionales para gestionar cuándo se recopilan, almacenan y utilizan sus datos. Un CDP se convierte en un repositorio de confianza para los datos de clientes y en la cadena de suministro controlada que conecta los dispositivos de los clientes a las plataformas que ofrecen valor. Como administrador de confianza de sus datos, sus clientes tendrán acceso al conjunto más preciso y significativo de sus datos personales cuando lo soliciten, y sistemas auxiliares, como las plataformas de gestión del consentimiento, ayudan a complementar el CDP al supervisar la recopilación y orquestación de esos datos.

5 La mejor experiencia del cliente

Un CDP puede ayudar a las organizaciones a comprender mejor el comportamiento y las preferencias de los clientes con una visión única del cliente. Los clientes quieren que se les conozca y comprenda con independencia del dispositivo que usen o de si están interactuando online o en persona. Hoy en día es frecuente que las empresas mantengan los datos de clientes en diferentes sistemas, como plataformas sociales y de correo electrónico. Además, un cliente puede tener una configuración de la privacidad diferente para cada una de esas plataformas, lo que puede dar lugar a que no se respeten sus preferencias. Con un CDP se pueden recopilar datos de confianza de los clientes en todos los puntos de contacto para producir una única visión completa de cada cliente, que será la base para todo lo relacionado con la privacidad. Esto permite un engagement en tiempo real en cualquier canal basado en las preferencias del cliente. Y este nivel de personalización se puede hacer a gran escala con un CDP neutro respecto al proveedor y en tiempo real, como el de Tealium.

¿Cómo pueden las organizaciones establecer la privacidad de los datos por diseño a gran escala?

La privacidad por diseño es el método de diseñar la privacidad de los datos en todos los procesos y operaciones empresariales, de modo que la información de identificación personal (IIP) esté protegida de manera predeterminada. La gobernanza de los datos es la política formal documentada para administrar la disponibilidad, la capacidad de uso, la integridad y la seguridad de los datos en los sistemas empresariales, de acuerdo con normas y políticas de datos internas que se definen con la privacidad por diseño. Para lograr una gestión adecuada de la privacidad y la personalización a gran escala, una organización debe incorporar un conjunto de soluciones tecnológicas que estén en línea con los parámetros de la privacidad por diseño y los procesos definidos en la gobernanza de los datos. Una plataforma de datos de cliente es ideal para este enfoque unificado

Los siguientes son algunos de los principales sistemas que son necesarios para la implementación de la privacidad por diseño y la gobernanza de los datos:

- **Plataforma de gestión del consentimiento (CMP):** recopile datos de consentimiento e implemente procesos para respetar la privacidad, como las solicitudes de acceso de los interesados.
- **Herramienta de marketing multicanal:** conéctese con sus clientes en todas las plataformas con los principios de privacidad incorporados en las integraciones de los canales elegidos.
- **Análisis del comportamiento y la experiencia:** comprenda y elabore experiencias digitales de más calidad teniendo en cuenta las preferencias de privacidad a lo largo de todo el engagement con el cliente y ajustando la experiencia al nivel óptimo que permita el cliente.
- **Plataformas de Datos de Cliente (CDP):** cree una foundation del dato independiente en la que se puedan basar sus tecnologías facilitadoras para satisfacer sus necesidades de datos y organizar la entrega de datos con fiabilidad.

«Al poner el CDP en el centro de la estrategia de privacidad, disponemos de un lugar para controlar los datos de los que nuestra organización se hace responsable y nos permite comprender de un modo coherente el linaje de los datos que debemos administrar».

- Ted Sfikas

Senior Director of Value Engineering & Digital Strategy en Tealium

Anatomía de una plataforma de datos de clientes

Estas tecnologías también ayudan a proporcionar una forma para que las empresas controlen los datos a gran escala. Es crucial controlar los datos desde el momento en el que se recopilan hasta el momento en el que se activan en todo el stack tecnológico, sin que afecte a la arquitectura actual ni requiera una inversión económica excesiva.

El CDP de Tealium está diseñado con una filosofía que da prioridad a los datos, es decir, que comienza en el momento en el que se recopilan esos datos. En concreto, Tealium proporciona tecnologías que automatizan la gobernanza necesaria con la automatización de la recopilación de datos (Tealium Data Connect, Tealium iQ Tag Management, y Tealium EventStream API Hub), la creación y el enriquecimiento de los perfiles de clientes (Tealium AudienceStream CDP), y el análisis y los informes de datos de los clientes (Tealium DataAccess y Tealium Data Insights).

De qué forma ayudan la oferta de productos de Tealium a gestionar la privacidad y personalizar la experiencia del cliente, desde la gestión de etiquetas hasta el CDP:

Tealium Data Connect

Cuando los datos de clientes residen en sistemas empresariales clave, como almacenes de datos, data lakes, MDM y otros repositorios importantes que forman parte de la cadena de suministro de datos, es fundamental unificar y validar estos conjuntos de datos antes de incorporarlos al CDP para poder usarlos. Data Connect proporciona una interfaz visual para lograr este objetivo de un modo eficaz y permite una gobernanza coherente automatizada.

Tealium Event Data Framework

La gobernanza se optimiza en gran medida cuando los datos de los clientes se recopilan en tiempo real en forma de eventos, es decir, cualquier interacción de un cliente con su marca, ya sea online o en persona, que cuenta como un punto de datos único que debe incorporarse al perfil del cliente. Los eventos son una unidad de medida de la interacción de un cliente que ofrecen una vista detallada del comportamiento del cliente y garantizan que se detecten y recopilen los datos adecuados de la forma correcta para que puedan usarse de inmediato en todos los sistemas. Los eventos representan información significativa para los sistemas empresariales que se usan como base para tomar medidas, ofrecer experiencias del cliente modernas respetando la privacidad y permitir a las empresas obtener fácilmente un conocimiento más profundo con capacidades intuitivas de elaboración de informes. Tealium recopila y activa estos eventos en tiempo real, en cualquier dispositivo que los muestre, con Event Data Framework, un paquete de tecnología de recopilación de datos que satisface estas necesidades de un modo rápido y efectivo:

- **Tealium iQ Tag Management (TiQ):** Los sistemas de gestión de etiquetas son el estándar del sector para diseñar y activar datos de eventos en sitios web. TiQ es un enfoque basado en el dispositivo para controlar y automatizar los datos de eventos en sitios web, aprovechando etiquetas de Javascript precompiladas para aplicar las preferencias de consentimiento y la consiguiente activación cuando sea necesario. La automatización de TiQ tiene lugar directamente en los dispositivos de los clientes, como teléfonos móviles y navegadores.

- **Tealium EventStream API Hub:** Tealium EventStream se utiliza con el fin de abordar las restricciones actuales de los navegadores, cuya finalidad es atender los mandatos de privacidad, para proporcionar la misma capacidad de gobernanza y automatización que TiQ, pero usando un enfoque basado en la nube para recopilar y controlar los datos de eventos. EventStream pone primero los datos recopilados en un entorno en la nube para validarlos y enriquecerlos. Después, activa esos datos de forma segura en cualquier destino por medio de API.

  Ambos enfoques para el data management de los clientes en tiempo real satisfacen las necesidades que plantean la privacidad y el marketing de controlar los datos de los clientes de una forma segura, con un modelo probado basado en eventos que se ha convertido en el estándar actual del sector.

Tealium DataAccess and Data Insights

La medición y la información se han convertido en algo fundamental para la mejora continua de los equipos de marketing y las iniciativas del departamento de informática. Con DataAccess y Data Insights se proporcionan a los departamentos de inteligencia empresarial actuales las estrategias modernas de incrementalidad y experimentación que serán necesarias para competir, sin necesidad de invertir en nuevas soluciones. Tealium ayuda a las herramientas de Business Intelligence que la empresa haya elegido a proporcionar paneles, informes y servicios de segmentación que serán necesarios para optimizar las innovaciones, como las Data Clean Rooms, que se pueden incluir para futuras estrategias de medios y el modelado de combinación de medios.

La confianza del cliente debe ir más allá del marketing

Durante mucho tiempo se ha pensado que el marketing tiene un rol principal para atraer y conseguir clientes y mantener una relación de confianza con ellos. Al haber más datos disponibles y haber aumentado las expectativas de los compradores, los equipos de marketing han invertido en el CDP como una forma de conseguir experiencias del cliente más completas. **Los CDP hacen posibles muchos casos de uso de marketing, ya que simplifican el rastreo de los datos, estandarizan los datos de diferentes fuentes y se integran en tiempo real con soluciones de partners designados,** como Meta, Google, etc., para ofrecer experiencias del cliente vanguardistas y significativas.

Sin embargo, con la entrada en vigor del RGPD y la proliferación de normativas sobre privacidad en todo el mundo, la responsabilidad de generar la confianza de los clientes a través de los datos ha establecido un nuevo incentivo para todos los equipos, no solo el de marketing. Las empresas que se basan en datos tienen motivos de sobra para hacer fuertes inversiones en la claridad de los datos (saber qué datos se procesan, quién los procesa y con qué fin), ya que esto genera nuevas fuentes de ingresos y mejora los costosos procesos operativos. Este incentivo no solo se valora en marketing, sino también en los departamentos de Data Science, Productos, Business Intelligence, Ventas y Customer Success, lo que lo convierte en un componente clave de toda la estrategia de clientes de la organización.

¿Cómo afecta entonces a la organización la consiguiente reasignación de responsabilidades para esta estrategia unificada? **Si bien todos los empleados de la organización deben comprender las políticas y los procedimientos relacionados con los datos de clientes, hay algunos departamentos y roles que trabajan directamente con ellos de forma independiente**. El enfoque se convierte entonces en un enfoque probado donde se utiliza un centro de excelencia.

Roles y departamentos clave para la nueva estrategia de datos de clientes

Profesionales de la privacidad de los datos

Cumplimiento normativo en el tratamiento de los datos

Con todas las normativas sobre privacidad de los datos que hay en el mundo, los expertos en privacidad de los datos desempeñan ahora un papel crucial en la incorporación de un CDP. Esto incluye a **directores de seguridad de la información (CISO), directores de privacidad (CPO), directores de privacidad de los datos, analistas, etc.**, que serán responsables de desarrollar e implementar programas de privacidad en toda la organización. También son responsables de trabajar con el resto del equipo de datos para establecer las políticas y los procedimientos internos de gobernanza de los datos adecuados para eliminar los silos internos y garantizar que se recopilen y gestionen los datos correctos desde un punto de vista analítico y de la privacidad. Estas personas deben colaborar estrechamente con los equipos de tecnología y marketing para aplicar las preferencias de privacidad de los clientes y cumplir las normativas al respecto, con el fin de asegurar que la organización cumpla y gestione sus obligaciones normativas y contractuales de un modo que tenga en cuenta la privacidad.

Profesionales del marketing

Experiencia del cliente basada en datos

Los profesionales del marketing están en la primera línea de la privacidad de los datos y del establecimiento de una relación de confianza con los clientes. Este equipo de personas, que incluye al **director de marketing (CMO), los directores de canales de marketing, el equipo de operaciones de marketing, etc.**, lleva a cabo el engagement con los clientes, facilita la recopilación de datos y los activa. Son los encargados de cumplir la responsabilidad de obtener el consentimiento de los clientes. Por tanto, el equipo de marketing desempeña un rol muy activo con el equipo de privacidad y los desarrolladores para determinar cómo se van a recopilar los datos y cómo se van a respetar las preferencias de privacidad.

Debe trabajar con los equipos de tecnología que administran el stack tecnológico de marketing y con los equipos de datos para asegurarse de que sigan las políticas de gobernanza establecidas, que los análisis sustenten su actividad de marketing y que se cumplan y actualicen cuando sea necesario los requisitos de privacidad de forma constante en las campañas de marketing.

Roles híbridos

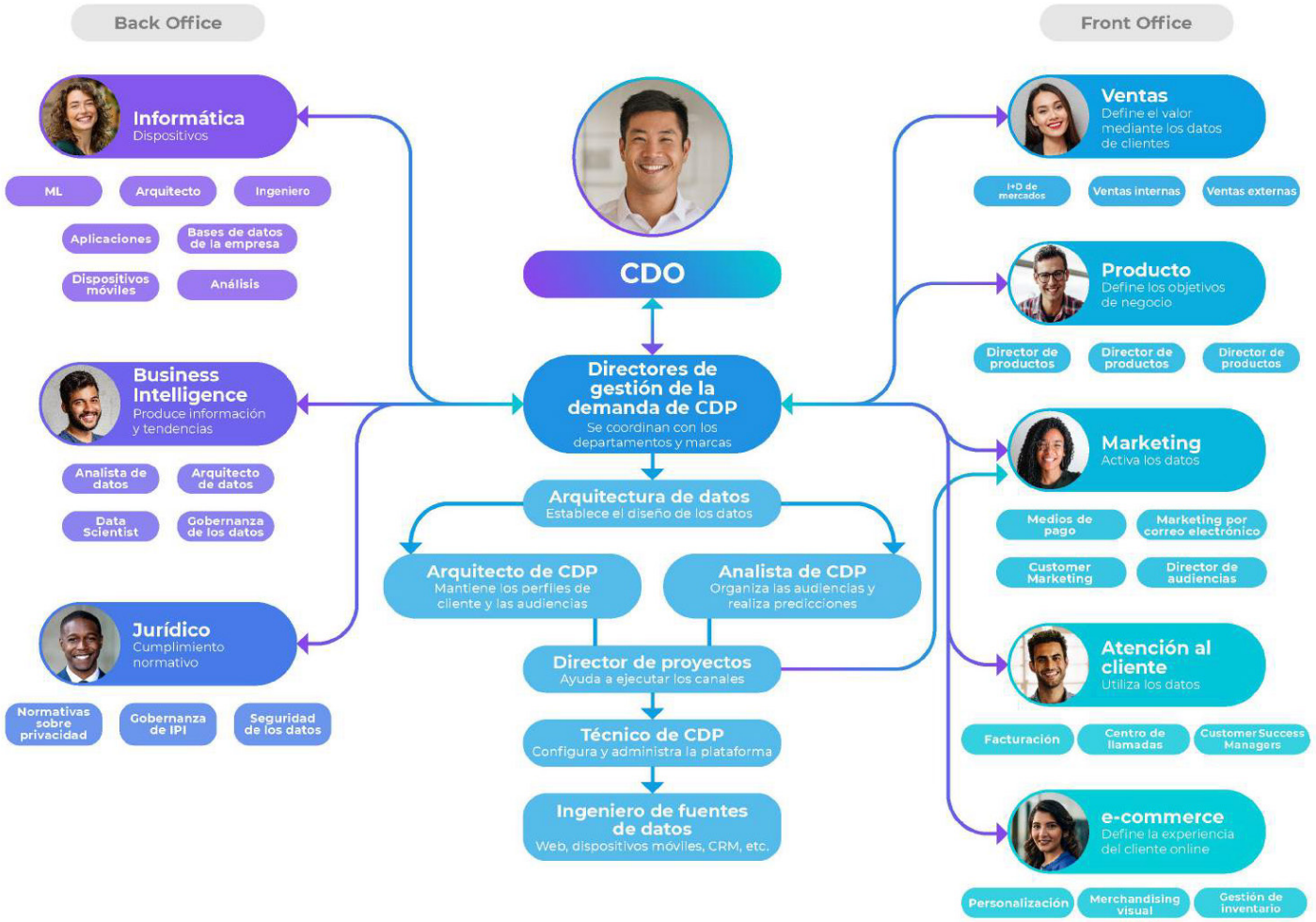
Unión de las responsabilidades relacionadas con los datos

En nuestro reciente ebook «La organización del futuro» explicamos cómo han cambiado los roles en la empresa debido a la creciente importancia de la gestión de los datos de clientes y la adopción de un CDP. Han surgido también nuevos roles ejecutivos, como el de director de datos, que está en línea con las partes interesadas de seguridad e InfoSec, para asumir la responsabilidad de administrar los datos de acuerdo con los roles más tradicionales que siempre han controlado los datos en un sentido amplio.

Debido a la evolución constante de la privacidad de los datos y a su rol en toda la organización, están surgiendo nuevos roles híbridos que gestionan la naturaleza interdisciplinar de la privacidad y la personalización. Algunos de estos roles son:

- **Profesional del marketing para la privacidad**
- **Directores de marketing de productos para la privacidad**
- **Ingenieros de la privacidad que establecen la privacidad por diseño**
- **Personas que sirven de puente porque hablan ambos idiomas y pueden lograr la claridad necesaria**

El Data Center of Excellence



El Data Center of Excellence (DCoE) es un departamento centralizado que está especializado en la estrategia, el diseño, la dotación de personal y la prestación de servicios que la organización necesita a gran escala. El equipo ayuda a simplificar el acceso a datos de clientes unificados para aumentar la velocidad a la que pueden actuar los equipos interdepartamentales. Es responsable de definir y responder a preguntas críticas que afectan a toda la empresa. Por ejemplo, cómo crear un data layer que normalice las convenciones de nomenclatura y la gobernanza, cómo integrar la infraestructura de datos, cómo mantener la seguridad y el cumplimiento normativo de los datos y, después, diseñar una solución y un modelo de entrega que ayude a crear casos de uso para los datos en toda la organización. El Data Center of Excellence reestructura la organización introduciendo un nuevo equipo que colabora con varios departamentos a fin de recopilar, organizar y activar datos de clientes de todas las formas posibles.

Organizaciones altamente reguladas

Las empresas de sectores altamente regulados, como la asistencia sanitaria y los servicios financieros, tienen un nivel más de complejidad a la hora de organizar sus equipos de CDP, debido al tipo de datos con los que trabajan y a las normativas. Los equipos de gobernanza de los datos y cumplimiento en materia de privacidad deben incluirse en cualquier caso de uso desde el principio, y después de forma continua y periódica, para asegurar el correcto cumplimiento de las leyes y los estándares de todo el mundo. Aunque puede parecer abrumador, los sectores muy regulados están obteniendo también importantes ventajas con la implementación de un CDP.

Tres recomendaciones clave para generar la confianza de los clientes a través de los datos

1.ª recomendación: Dar sentido a la privacidad

> *«Uno de los aspectos del cumplimiento de la gobernanza de los datos es saber qué datos se procesan, dónde se procesan y quién tiene acceso a ellos. Tener una buena gobernanza de los datos es fundamental para el cumplimiento de las normativas sobre privacidad».*
>
> *– DJ Landreneau*
> *Director of Data Privacy Strategy en Tealium*
> *(página 36, La organización del futuro)*

El primer paso para crear una dinámica de confianza con sus clientes es recopilar únicamente los datos necesarios y de un modo que respete la privacidad del cliente. Para lograr este objetivo fundamental, deberá hacer lo siguiente:

Crear un buen programa de gobernanza de los datos

Redefina qué significa la privacidad para su organización.
Las empresas deben adaptar su mentalidad interna a la privacidad de los datos e incorporar en el núcleo de su marca el respeto por el cumplimiento de las normativas sobre privacidad de los datos de clientes. Casi todos los empleados de una organización interactuarán con los datos de clientes en alguna de sus funciones, por lo que es fundamental que comprendan qué es la privacidad en términos claros y explícitos que se transmitan de forma periódica y visible. También debe definir qué personas se ocupan de la privacidad de los datos y establecerlas como expertos internos en la materia (SME) para quienes tengan dudas. Asegúrese de que se sepa que la privacidad de los datos es importante.

Elabore el borrador de un manifiesto sobre la privacidad y hágalo de dominio público.
Las políticas de privacidad de los datos de clientes de la organización no solo deben comentarse, sino que hay que dejar constancia de ellas por el bien de sus empleados y de sus clientes. La mayoría de los clientes consideran que las notificaciones de las marcas sobre la seguridad de los datos son extremadamente complejas. **En Estados Unidos, solo el 3 % de los ciudadanos afirman que comprenden cómo funcionan realmente las leyes actuales sobre la privacidad online. A esto se une el hecho de que el 79 % de los estadounidenses que no forman parte de empresas fuertes admiten hacer un mal uso de los datos**, y la brecha de confianza se puede ver tan claro como el agua. Las políticas de privacidad deben definirse con claridad y se debe poder acceder a ellas adecuadamente en su sitio web y en la documentación interna para que todo el mundo tenga acceso a ellas.

El **3 %**
de los estadounidenses afirma que comprenden cómo funcionan realmente las leyes actuales sobre la privacidad online.

El **79 %**
de los estadounidenses que no forma parte de empresas fuertes admite hacer un uso indebido de los datos.

Dé prioridad al cumplimiento de las normativas sobre privacidad de los datos, tanto para ahora como para el futuro.

Dada la dimensión global de las normativas sobre privacidad y los negocios internacionales, si en su empresa no han empezado aún a abordar políticas como el RGPD y la CCPA, por nombrar solo algunas, deben hacerlo ya. No se trata solo de que su empresa esté obligada a comunicarse con sus clientes europeos y a gestionar los datos de esos clientes conforme al RGPD, sino que las medidas que tome ahora para cumplir este reglamento la preparará para cumplir también otras normativas sobre privacidad futuras.

Revise detenidamente todas las directrices sobre privacidad de los datos aplicables a su organización y diseñe un plan de acción para cumplirlas ahora y en el futuro. Tendrá que incorporar flexibilidad y escalabilidad, además de planificar la revisión periódica de las leyes que regulan el cumplimiento de su empresa en todo el mundo y actualizarlas cuando sea necesario.

Utilice el sentido común a la hora de preparar a su empresa para la evolución constante de las normativas sobre privacidad de los datos.

Cuando prepare a su empresa para próximas normativas relacionadas con los datos, piense en qué tipo de protección desearía para sus propios datos.

Los siguientes son algunos pasos clave:

- Elabore un mapa de datos que refleje con claridad los datos que su empresa tiene, qué se hace con ellos y a dónde van.
- Defina con claridad su posición actual en torno a las ventas basadas en datos y planes futuros para usar datos de terceros.
- Inserte mecanismos para abordar el acceso, la modificación y la eliminación de los datos en función de derechos individuales.

Recuerde que la confianza es un trabajo de toda la empresa.

Como hemos comentado, su empresa debe incluir su postura respecto a la privacidad de los datos en la declaración de su misión y en los valores fundamentales de la empresa. Todos los empleados de la organización que toquen datos de clientes deben comprender y preocuparse por la privacidad de los datos. Se unirán en esta importante labor de dar prioridad al respeto por los datos de clientes. Un hecho que ayudará a su propio equipo a convertirse en el principal defensor de su marca es establecer una base interna de confianza y convicción, que se reflejará después hacia afuera para facilitar la generación de la confianza de los clientes.

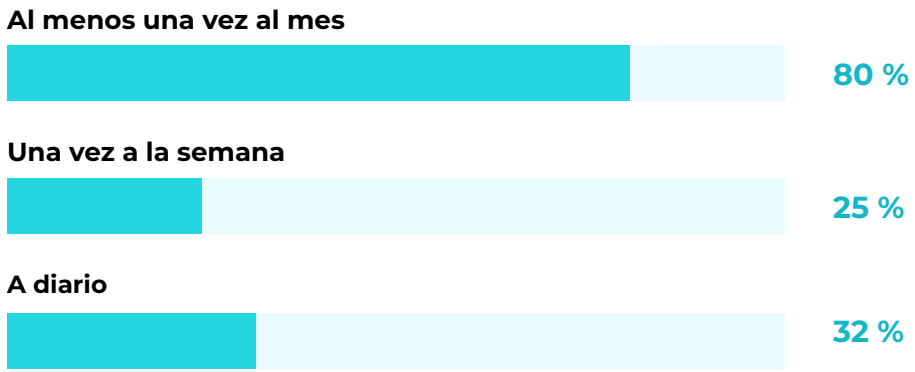
2.ª recomendación: Dar a los clientes un motivo para que den su consentimiento

Los clientes están hartos de que se les pida permiso y el cansancio por pedirles constantemente que indiquen sus preferencias de privacidad cuando visitan sitios web es real. Según Pew Research, **el 80 % de los estadounidenses adultos afirma que se le pide aceptar una política de privacidad al menos una vez al mes**. Otro **25 % dice que esto le ocurre casi a diario**. De los estadounidenses a los que se presenta un acuerdo de privacidad, **el 32 % afirma ver uno aproximadamente una vez a la semana**.

Con todas estas solicitudes de consentimiento que reciben sus clientes desde todos los rincones de Internet, debe ser realmente estratégico sobre cómo va a pedir el consentimiento. El consentimiento debe enfocarse como una relación continua con sus clientes que incluye una solicitud para que lo concedan y una estrategia de intercambio de valor que motive al cliente a volver a por más en lugar de tomar sus datos y salir corriendo. Este es el motivo por el que los profesionales del marketing no deben limitarse a dejar esta labor a los departamentos de privacidad, datos e informática.

La forma en la que se recopilan los datos de los clientes es tan importante como los datos que se les piden.

Frecuencia de la solicitud de consentimiento en relación con la privacidad en Estados Unidos



Diseñe una estrategia de recopilación de datos continua

Sea transparente.
Su política de privacidad no se aplica únicamente a los clientes más informados y expertos en tecnología. Los clientes están deseosos de que las empresas expliquen sus prácticas de forma clara y concisa. Hacer esto reforzará la reputación de su organización como empresa digna de confianza. Cuanto más claras sean sus políticas, menos parecerá que esté ocultando algo. No disimule la realidad del uso que van a dar a los datos ni intente engañar a los clientes para que proporcionen información. La terminología complicada no sólo desanima, sino que da ganas de marcharse. Explíquese de forma sencilla, clara y honesta.

Diseñe un intercambio de valor en el lugar y el momento que sea importante.

> *«Para pensar en cómo vamos a segmentar a nuestros clientes, debemos obtener datos sobre ellos y la clave para eso es generar confianza, tener un intercambio de valor sólido y comprender que el consumidor habitual actual sabe que nada es gratis. Si rellenas un formulario, estás proporcionando algunos datos y esperas algo a cambio. Por tanto, nos corresponde a nosotros asegurarnos de que el intercambio de valor sea claro y que cumplamos lo que decimos que vamos a hacer».*
>
> ***– Jetta Hansen***
> *Senior Data Analyst en Nav Inc.*

En lugar de mantener la recopilación de datos en segundo plano, conviértalo en un apretón de manos con sus clientes. Cuando la gente llega a su propiedad digital, es importante tratarla como el primer paso de una relación mutuamente beneficiosa. Un aviso sobre la privacidad con una estética atractiva y un lenguaje claro será la primera impresión de su marca y debería transmitir la importancia que su empresa da a la vigencia de los datos.
Y no debe quedarse ahí. El intercambio de valor debe continuar más allá de los datos de primera parte y de la información de identificación personal (IIP). El intercambio de datos de parte cero, donde su marca pide a un cliente su opinión y otra información por medio de encuestas y comentarios, debe tener lugar en el momento en que tenga sentido en el recorrido del cliente. Esto lleva el intercambio de valor a un saludo continuo entre el cliente y su empresa, donde la relación puede hacerse más profunda y ampliarse con el tiempo.

Convierta la solicitud de datos en una experiencia del cliente por sí sola.
Es un ejercicio de honestidad que refuerza la confianza del cliente en su marca y ayuda a explicar por qué necesitan sus datos. Las organizaciones más expertas convierten la experiencia de recopilación de datos en un punto crítico del intercambio de valor. Diga a sus clientes de forma explícita cómo van a usar en su empresa los datos que les piden para mejorar constantemente las experiencias individualizadas, con ejemplos concretos basados en sus propias ofertas. ¿Su empresa vende ropa? Dígales que van a usar sus datos para ofrecerles descuentos en sus vaqueros favoritos. Convierta el intercambio de datos en una experiencia emocionante.

Explique con total claridad el acceso a los datos.
Permitir que sus clientes tengan el control sobre los datos que su empresa recopila fomentará una relación de confianza. Esto incluye dejar que los clientes accedan a sus datos personales, que se corrijan sus datos, que se eliminen esos datos si lo piden o que se los puedan llevar a otro proveedor. Esto no solo debería ser posible, sino también fácil de hacer. La ventaja añadida aquí es que, si sus clientes se ocupan de mantener sus propios datos, mejorará la calidad de esos datos, lo que a su vez hará que el trabajo de personalización sea más satisfactorio. Para empoderar a sus clientes de forma que puedan administrar sus propios datos, debe disponer de la tecnología adecuada en su stack para hacerlo a gran escala, en todos los canales de forma cohesiva y en tiempo real.

Incluya flexibilidad para el futuro.
El tipo de datos que las empresas pueden recopilar cambia constantemente y es imposible adivinar qué deberán incluir en la política de su empresa dentro de cinco años. Deje espacio para hacer cambios que reflejen la política, la demanda de los clientes y las nuevas tecnologías. Utilice también un enfoque universal para la forma en la que gestionan todo el conjunto de datos de su empresa. Aunque una ventana emergente es una opción en la actualidad, podría estar prohibido dentro de unos años, o todos sus formularios podrían requerir en algún momento una doble confirmación del consentimiento. Considere todas las posibilidades cuando cree sistemas e invierta en tecnologías que le ayuden a recopilar y administrar los datos de clientes.

El uso de un lenguaje estricto y claro en los requisitos de consentimiento, los derechos de acceso y las protecciones de seguridad contribuirá en gran medida a evitar confusiones, tanto internamente como con sus clientes.

Consejo

Debe ser coherente

3.ª recomendación: Diseñar un Customer Journey que genere confianza

Los clientes ahora demandan una experiencia relevante, que depende de que los datos del cliente estén unificados. Cuando tiene datos de cliente unificados, puede presentar su organización de un modo cohesivo y significativo a sus clientes. Si los datos no están unificados, resulta terriblemente obvio. Tanto si publica anuncios digitales para promocionar productos que un cliente ya ha comprado como si envía correos electrónicos a un cliente que haya cancelado su suscripción o se haya negado a dar su consentimiento, los clientes se dan cuenta cuando los equipos de su empresa no trabajan de forma coordinada, porque el resultado es una mala experiencia del cliente. Pero, en lugar de ver esto como una dificultad tremenda que su empresa debe superar, véalo como lo que realmente es: una oportunidad para crear experiencias de confianza increíbles.

Con el stack tecnológico de marketing adecuado (que maximiza los datos de los clientes de un modo flexible y respetuoso con la privacidad), puede crear magníficas experiencias del cliente y generar fidelidad de marca.

Ha determinado los datos que definitivamente necesita recopilar para optimizar las operaciones de su empresa. Ha creado una buena estrategia para recopilar los datos, comunicar cómo se van a usar y cómo se puede acceder a ellos. Ahora debe segmentar y activar los datos.

El 62 % de los clientes espera que las marcas personalicen cada interacción. Al planificar el recorrido único y personalizado de cada cliente, puede lograr un mejor conocimiento de sus clientes y ofrecerles comunicaciones de marketing individualizadas que también se pueden escalar.

Privacidad en Internet y datos online de acuerdos de privacidad en Estados Unidos

Esperan que las marcas personalicen cada interacción

62 %

Abandonan la experiencia cuando la oferta es irrelevante

74 %

Elabore y ofrezca un Customer Journey personalizado

Defina las audiencias y los segmentos de clientes respetando sus preferencias de consentimiento.

La personalización se puede hacer a gran escala con la ayuda de una solución como un CDP. Podrá definir audiencias muy específicas como punto de partida para la elaboración de recorridos del usuario extraordinarios. Integre estas audiencias clave en su CDP y asigne los clientes a esas audiencias, al tiempo que respeta sus preferencias de consentimiento.

Planifique puntos de contacto significativos e integre la automatización del marketing.

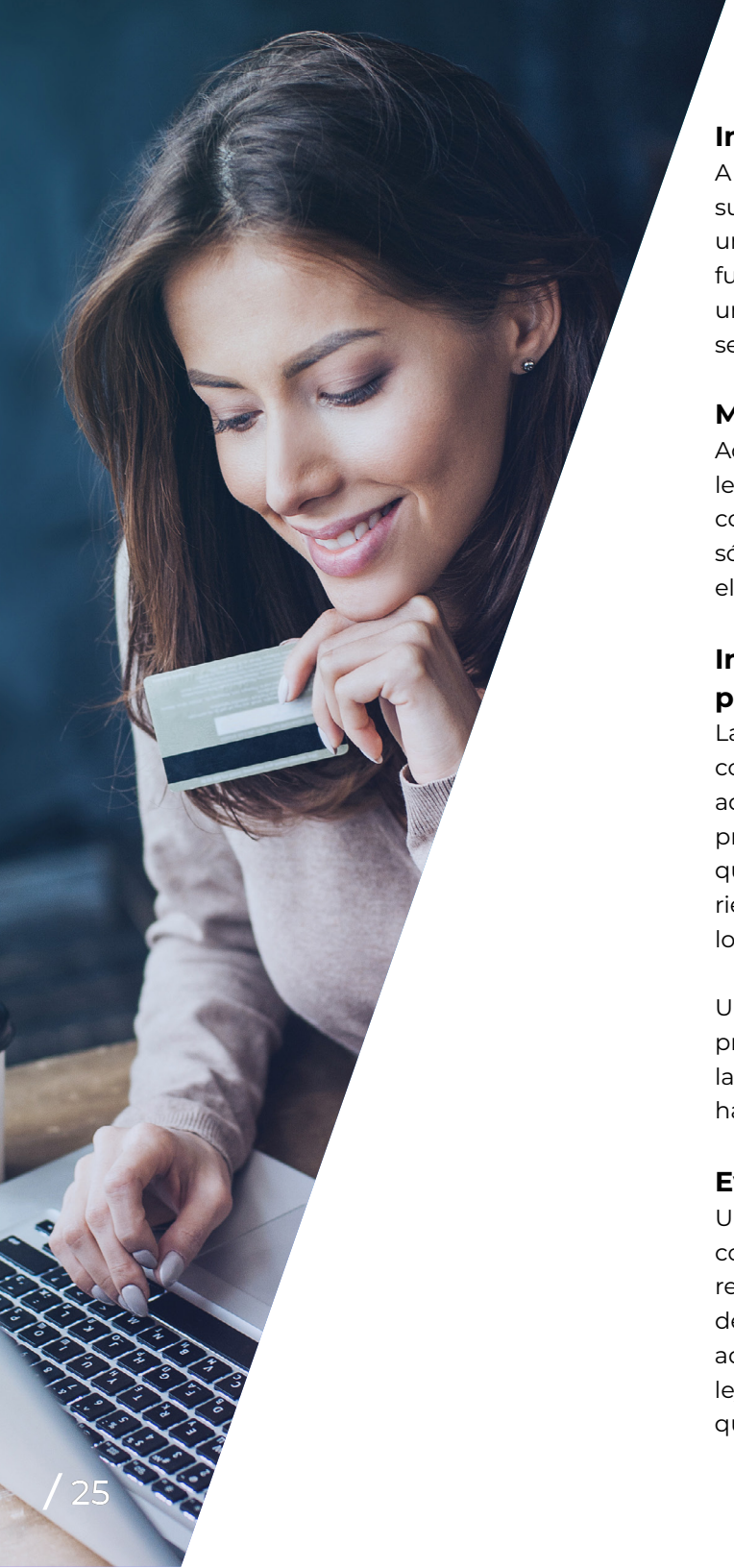
Una vez que tenga el punto de partida (cuando el cliente entre en una audiencia), defina a dónde desea llevarlo y qué contenido, mensajes, ofertas especiales y valor proporcionará a lo largo del camino para dirigirlo al último destino en función de su consentimiento.

Sea transparente en cuanto al modo en el que usarán sus datos personales durante su experiencia.

Igual que hará saber a un cliente cómo usará sus datos cuando los recopile, querrá mantener esta transparencia a lo largo del recorrido del usuario. Puede parecer obvio una vez que haya obtenido permiso para usar sus datos personales, pero los clientes necesitan que se les recuerde constantemente que su empresa trabaja para beneficiarlos a ellos.

Asegúrese de proporcionar vías de salida para los clientes a lo largo de su recorrido.

Es posible poner a un cliente en un recorrido y que el cliente pronto descubra que no es adecuado para él. Puede que haya cambiado algo en su entorno (quizá se haya mudado y ya no tenga las mismas necesidades cotidianas) o que algo que al principio le parecía interesante ya no lo vea tan genial. No se lo ponga difícil a estas personas si desean abandonar el recorrido. Y definitivamente no deje cómo única opción «cancelar la suscripción». Cuando el cliente cambie de opinión, convierta la experiencia en un aprendizaje para ambas partes.



Incluya el acceso del cliente al control de los datos en todos los canales.
A este respecto, facilite e incluso empodere al cliente para determinar sus intereses y actualizar sus propios datos. Ofrezca este acceso en cada punto de contacto, siempre que sea posible, y use un stack tecnológico de marketing que sea lo suficientemente flexible como para gestionar esta funcionalidad. Sus clientes valorarán la simplicidad y el empoderamiento. Convierta la experiencia en una forma de generar confianza y aumentar la fidelidad de los clientes en lugar de hacer que se alejen.

Mantenga siempre la coherencia en los mensajes y el lenguaje.
Además de proporcionar acceso al control de los datos en todos los canales, asegúrese de utilizar un lenguaje y mensajes coherentes en torno a sus políticas de privacidad, de modo que se reconozcan y comprendan con facilidad. La coherencia es un componente principal en una experiencia del cliente sólida y la coherencia en los mensajes sobre privacidad irá cobrando importancia a medida que pase el tiempo.

Incluya suficiente flexibilidad como para abordar el panorama cambiante de la privacidad.
Las normativas sobre privacidad evolucionan constantemente, con el objeto de proteger a los consumidores y empoderarlos para controlar sus propios datos. Dicho esto, las empresas tienen que adaptarse rápidamente a medida que estas normativas cambian y, para ello, deben implementar los procesos y la infraestructura que les permitan estar preparadas ahora y en el futuro. Las empresas que no estén preparadas se verán obligadas a rehacer toda su infraestructura y sus estrategias, con el riesgo de quedarse atrás. Por tanto, es importante interactuar con los profesionales de privacidad de los datos a la hora de planificar los recorridos del usuario y centrarse en la optimización continua.

Un ejemplo excelente de preparación para el futuro es la inversión en un enfoque de datos de primera parte. Todos sabemos que la desaparición de las cookies de terceros se avecina. Por eso, las empresas innovadoras están adoptando estrategias de datos de primera parte de confianza habilitadas por un CDP.

Evite recorridos de usuario que compitan entre sí.
Un componente fundamental a la hora de respetar la privacidad de sus clientes es no abrumarlos con un engagement innecesario. Evite poner a los clientes en demasiados recorridos o en recorridos que compitan entre sí. Deberá priorizar los recorridos del usuario y recurrir a soluciones de inteligencia artificial y Machine Learning, como Tealium Predict ML, para entregar el mensaje adecuado en el momento oportuno. Se ha demostrado que las técnicas de ML no solo cumplen las leyes en materia de privacidad, sino que también proporcionan una nueva fuente de ingresos de la que se benefician tanto los clientes como las empresas.

Por qué empresas de todo el mundo confían en Tealium

«La gestión del consentimiento es esencial para la organización del futuro. Con Tealium, Kmart ha consolidado los flujos del consentimiento en toda la empresa para ofrecer experiencias del cliente que dan prioridad a la privacidad en todos los puntos de contacto. Creemos que este enfoque ha preparado a nuestra empresa de cara al futuro para mantener la conformidad en un panorama normativo en constante cambio».

– Photi Orfanidis,
Architect, Marketing & Loyalty Technologies en Kmart Group Australia

«Con Tealium podemos sacar el máximo partido a los datos que los clientes comparten con nosotros. El uso de datos de primera parte con el consentimiento de nuestros clientes para crear una visión completa nos permite mejorar el engagement, ya que ofrecemos un contenido más útil y personalizado, al tiempo que damos prioridad a la privacidad de los datos. Esto nos permite estar ahí para ellos en los momentos más importantes, ya sea cuando notifiquen que han perdido una tarjeta o cuando decidan comprar una casa».

– Bobby van Groningen,
IT Engineering Lead en ABN AMRO

Tealium fundó el espacio de las Plataformas de Datos de Cliente. Nuestro recorrido comenzó cuando nuestros fundadores, Mike Anderson y Ali Benham, crearon el píxel de rastreo en WebSideStory (ahora Adobe Systems) e inventaron el rastreo del comportamiento de los clientes online. Tealium creó el primer CDP en 2013 y ha trabajado con más de 1000 empresas y sectores altamente regulados.

Tealium ofrece un conjunto completo de servicios para la gestión de los datos de los clientes en tiempo real, en todos los canales y dispositivos, con más de 1300 integraciones, centros de datos en todo el mundo y el cumplimiento de las normativas sobre privacidad integrado en nuestro ADN. Ofrecemos un CDP que da prioridad a los datos. La privacidad y el consentimiento no fueron una ocurrencia de última hora, sino impulsores para utilizar los datos de clientes con el fin de crear la mejor experiencia del cliente con confianza. El panorama de la privacidad y el consentimiento cambia de forma rápida y constante. Las organizaciones tienen la tarea de adaptarse con la flexibilidad suficiente como para proporcionar una experiencia del cliente efectiva, al tiempo que siguen cumpliendo las nuevas normativas y adoptan los cambios tecnológicos. Para lograr este complejo objetivo, las empresas necesitan una solución que unifique los datos y que esté integrada en todo el stack tecnológico, de modo que la aplicación automatizada de las políticas de privacidad se realice en consonancia con la experiencia.

Para abordar los requisitos cambiantes de privacidad y consentimiento en el panorama actual, que es tan competitivo, debemos basarnos en que la gobernanza automatizada de los datos se implemente al mismo tiempo que se orquesta la experiencia del cliente. Esto significa que esta solución central debe servir como repositorio de confianza de los datos de clientes para que la empresa cumpla la promesa de respetar íntegramente las normativas sobre privacidad.

Algunas características que la tecnología de la solución central debe incluir:

- Gestión de etiquetas para optimizar la recopilación de datos en los sitios web.
- Integración con las plataformas CMP que gestionan el inventario de privacidad y las solicitudes de acceso de los interesados.
- Funcionalidad central y automatizada de Data Management.
- Paneles para visualizar la cadena de suministro de datos a lo largo de todos los recorridos.
- Certificaciones de InfoSec para validar su compromiso y adherencia a las normativas sobre privacidad.
- Resolución de la identidad en tiempo real para garantizar que se apliquen las preferencias de forma precisa antes de activar los datos.
- Amplia integración con todas las demás tecnologías orientadas a los clientes que incorporen los mismos principios de privacidad y entreguen los datos en tiempo real.

La mejor forma de conseguir esto es con una Plataforma de Datos de Cliente unificada, en tiempo real, ampliable con CMP y que se integre perfectamente con soluciones analíticas y canales tecnológicos orientados a los clientes. **Ahí es donde entra Tealium.**

Rol de Tealium en una iniciativa de privacidad y consentimiento

El primer rol de Tealium en una iniciativa de privacidad y consentimiento es **actuar como plataforma de gobernanza con la tarea de recopilar datos de los clientes.** Está configurado para funcionar de manera automatizada.

Cuando se trata de gestionar la privacidad de los datos de los clientes, la Plataforma de Datos de Cliente de Tealium desempeña un rol central en toda la cadena de suministro de datos. En primer lugar, las tecnologías de recopilación de datos de Tealium recopilan conjuntos de datos de clientes junto con sus preferencias de privacidad, en tiempo real y en cualquier tipo de dispositivo.

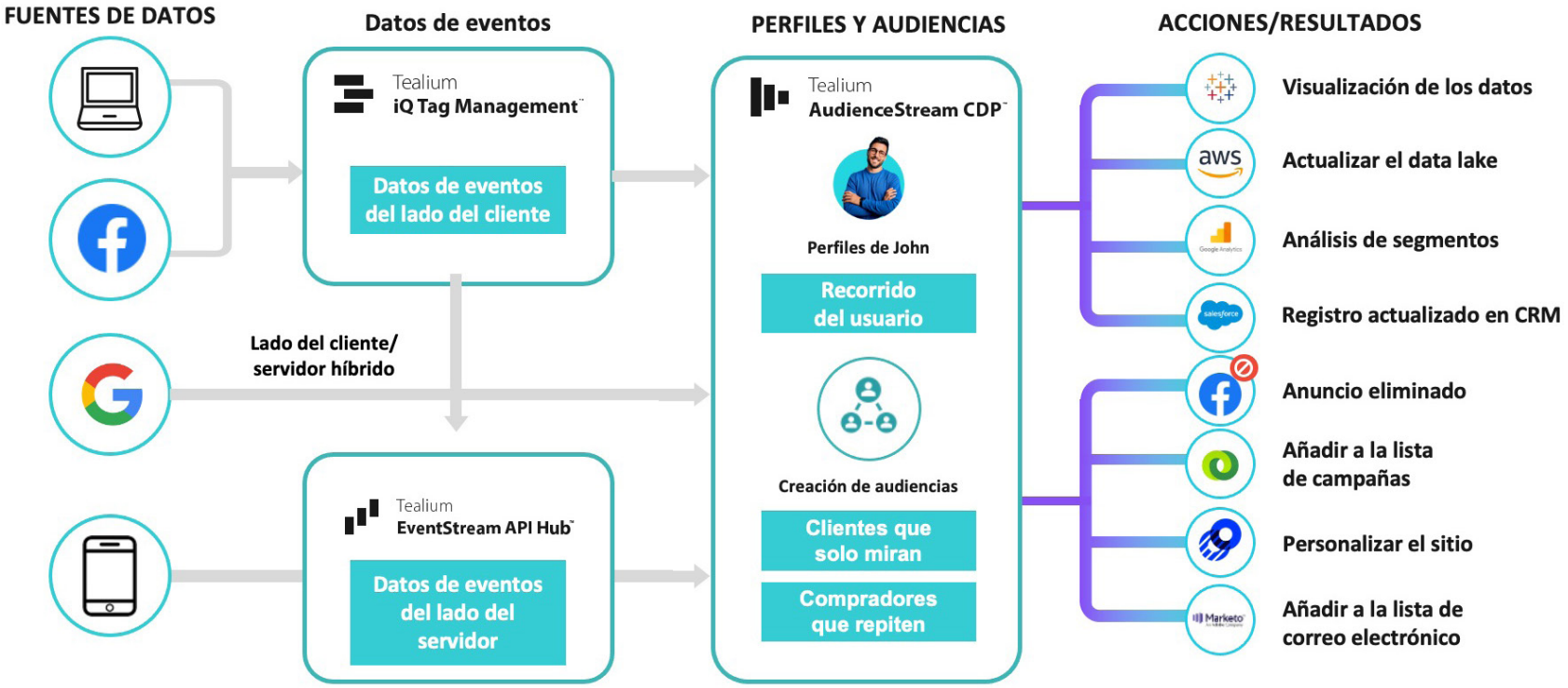
Las preferencias de privacidad se pueden recopilar de varias formas:

- Con el aviso integrado de Tealium Consent Manager (la empresa debe determinar el factor de forma y la normativa sobre privacidad específica).
- Con otra tecnología externa que la empresa elija.
- En algunos casos, las empresas no pueden ofrecer un aviso emergente, por lo que configuran una página web denominada «Política de privacidad» para mostrar estas preferencias.

En cualquiera de estos escenarios, Tealium detecta las preferencias del cliente y las aplica, al tiempo que recopila otros datos pertinentes sobre el cliente, como datos demográficos, de navegación y de transacciones. Finalmente, en función de las preferencias del visitante, Tealium organiza todos los datos y los envía a la tecnología de destino adecuada.

Tealium respalda sus opciones de seguridad y privacidad con certificaciones de terceros, como HIPAA, ISO 27001 y 27018, Escudo de la privacidad (Privacy Shield) y SSAE18 SOC 2, tipos I y II. Podemos ayudar a su empresa a cumplir cualquier normativa sobre privacidad que su política o sector requieran.

Obtención del consentimiento



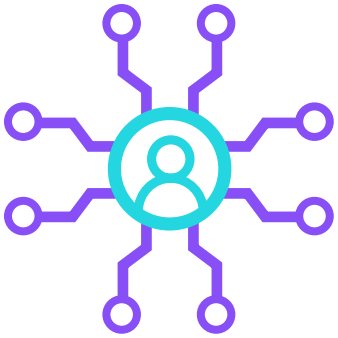
Tealium iQ (TiQ) Tag Management

El sistema Tealium iQ (TiQ) Tag Management para sitios web tiene la capacidad de detectar, recopilar y transmitir datos de clientes a medida que van surgiendo en tiempo real, incluidas las preferencias categóricas de marketing y la decisión de dar o denegar el consentimiento.

Tealium EventStream API Hub

Tealium EventStream recopila datos en sitios web, aplicaciones móviles y dispositivos de IoT y OTT que se pueden enviar al Customer Data Hub y al CDP para una mayor conciliación con un perfil unificado. Además, Tealium proporciona interfaces basadas en archivos y mediante programación para los mismos fines.

Gestión y orquestación del consentimiento



Después de obtener el consentimiento, el segundo rol de Tealium es **orquestar el enriquecimiento y la activación de esos datos en todo el ecosistema tecnológico.**

Una vez que el cliente haya dado su consentimiento, la empresa puede establecer un perfil de cliente que refleje la experiencia que haya elegido y las necesidades de engagement. Esto pone de relieve muchos más requisitos para mantener la integridad y la portabilidad de los datos del cliente.

El conjunto de soluciones de Tealium se amplía con la gestión del ciclo de vida del consentimiento en el CDP AudienceStream para este fin.

CDP Tealium AudienceStream

La recopilación de datos no es una tarea que se realice solo una vez. Las preferencias de los clientes varían continuamente, produciendo cambios en el perfil del cliente. El CDP Tealium AudienceStream se integra directamente con EventStream y TiQ para conciliar los cambios en los datos y la identidad asociada a medida que se capturan sesiones del usuario en sitios web y otros dispositivos. Este tipo de automatización aborda directamente el coste, el tiempo y el riesgo que conllevaría la gestión manual o por silos de la privacidad de los datos. AudienceStream controla los cambios exactos que tienen lugar en los datos de clientes y automatiza la evolución del conjunto de datos a lo largo del tiempo. Esta evolución produce nueva información sobre el comportamiento de los clientes y se añade de inmediato al conjunto de datos.

El CDP de Tealium controla las tecnologías que reciben los conjuntos de datos de clientes y, lo que es aún más importante, cuáles pueden orquestar con precisión la cantidad de datos necesaria. Esto garantiza que los datos de clientes se usen en la medida en la que se necesiten. Además, el CDP de Tealium tiene características de seguridad integradas que permiten designar los datos como información de identificación personal (IIP) según requiera cada normativa sobre privacidad. También se puede configurar para tratar esos datos de forma segura y conforme con la ley. Esto incluye técnicas de cifrado, hashing y desidentificación, así como la capacidad de almacenamiento restringido.

Integración con soluciones de partners de Tealium

La orquestación del perfil de cliente implica una orquestación determinada y conforme de los datos del cliente con todo el stack tecnológico de la empresa. Tealium se integra con más de 1300 tecnologías por medio de una interfaz intuitiva para añadir valor a este trabajo. De esta manera, no solo se orquestan con eficacia los destinos de los datos del cliente, sino que las fuentes que exponen los datos también se incluyen en la automatización. Otros puntos de contacto del cliente online y offline producen datos del cliente relevantes y la plataforma de Tealium está configurada para conectarse a cada uno de ellos cuando sea necesario, lo que mitiga el riesgo que supondría una ingeniería personalizada para una estrategia empresarial que evoluciona rápidamente.

Diseñada para ofrecer escalabilidad y fiabilidad

Los datos de clientes son uno de los activos más valiosos de cualquier empresa. Incluso la interrupción más leve del tiempo de actividad puede causar problemas de cumplimiento normativo y personalización si esos datos se demoran o se pierden. Asegúrese de que el proveedor de su CDP pueda satisfacer las necesidades de su centro de datos a nivel regional e internacional y de que tenga una probada trayectoria de fiabilidad y disponibilidad.

Aunque el tiempo de inactividad es un importante motivo de preocupación, un aspecto del que no se habla lo suficiente en el contexto de las tecnologías base, como un CDP, es el perjuicio y los costes que supone tener que reemplazarla. Elegir un CDP que dé prioridad a los datos y que se escale a medida que su negocio crezca con la flexibilidad que aporta la neutralidad respecto al proveedor garantiza que no será necesario reemplazar su inversión en los datos de clientes a medida que se expanda a nuevas áreas geográficas o aumenten los datos que procesa.

Desarrollada para empresas, creada para todos

Tealium goza de la confianza de los clientes empresariales más exigentes, casi 1000 empresas globales de diferentes sectores, incluidos los de retail, asistencia sanitaria, farmacéutico, deportes y entretenimiento, turismo, juegos, seguros, Administración pública, educación, automoción, etc. Estas empresas confían en Tealium no solo por nuestros permisos y seguridad de nivel empresarial, sino también por la velocidad y la fiabilidad de nuestra plataforma.

Colaboradores

Julian Llorente Perdigones
DJ Landreneau
Ted Sfikas
Matthew Parisi
Phil Hollrah
Karen Naves
Heidi Bullock
Hilary Noonan

Este informe ha sido publicado por

TEALIUM®

Tealium conecta los datos de los clientes, abarcando la red, los dispositivos móviles, el mundo offline y la Internet de las Cosas, para que las marcas se puedan conectar con sus clientes. El ecosistema de integración llave en mano de Tealium apoya a 1300 proveedores y tecnologías del lado del cliente y del servidor, haciendo posible que las marcas creen una infraestructura de datos de clientes unificada y de tiempo real. Las soluciones de Tealium incluyen una plataforma de datos de clientes con machine learning, gestión de etiquetas, un hub de API y soluciones de gestión de datos que hacen que los datos de clientes sean más valiosos, aprovechables y seguros. Más de 850 empresas líderes de todo el mundo confían en Tealium para fortalecer sus estrategias en materia de datos de clientes.

Para más información, visite

tealium.com/es