IBM Security

Uniendo a las partes interesadas para modernizar CIAM en toda la organización

Introducción

Cuando crea una cuenta nueva, hace una compra o incluso se suscribe a un boletín de noticias, confía sus datos personales a una empresa. Tras el intercambio inicial, es posible que no desee que sus datos se usen para fines distintos de los acordados, aunque con su consentimiento quizá agradecería experiencias personalizadas y recomendaciones futuras. Lo importante es que dependa de usted y que pueda cambiar de idea en cualquier momento. Y si la experiencia no resulta ser muy fluida, o si empieza a perder la confianza en la empresa por cualquier motivo, probablemente la abandone y busque otra. La gestión de identidades y accesos del consumidor (CIAM en sus siglas en inglés) posibilita dichas experiencias de confianza bajo demanda y personalizadas entre una marca y sus consumidores. Y al actuar como consumidor usted mismo podrá empatizar con sus propios consumidores, lo que le permitrá realizar actualizaciones de la estrategia digital de su empresa para mantenerse competitivo.

CIAM, sin embargo, es mucho más que una actualización de sitios web o un proyecto de marketing; afecta a áreas funcionales de toda la organización, ya que evalúa y moderniza los puntos de contacto con los consumidores. Para asegurar que el eterno equilibrio entre comodidad y seguridad no se pierda, las organizaciones han de procurar que confluyan las partes interesadas del negocio y de la tecnología, y que reconozcan CIAM como una parte de la transformación digital centrada en resultados que puede compartir componentes tecnológicos con la IAM del personal. Si se implementa con una finalidad y siguiendo una estrategia, las organizaciones pueden maximizar su implicación con los consumidores al tiempo que minimizan los riesgos para la TI y el personal de seguridad.

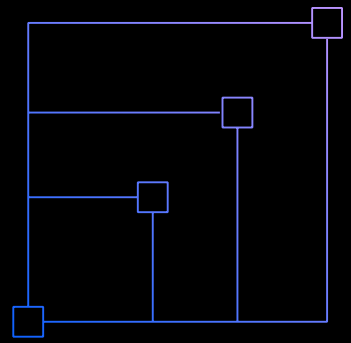
Sin una estrategia CIAM, las empresas se exponen a perder ingresos por abandono de los clientes: la fidelidad a la marca es frágil cuando las alternativas están a un clic de distancia. De manera similar, en el sector público, los organismos gubernamentales que aún se aferran a infraestructuras y procesos heredados pueden perder la confianza de los ciudadanos y no alcanzar los niveles idóneos de adopción de los servicios públicos. A pesar de tener misiones diferentes, tanto al sector privado como al público les une su necesidad de prestar un servicio a los consumidores a través de una experiencia digital fluida y a la vez segura para que sea posible compartir información respetando la privacidad. Y muchas organizaciones han tomado buena nota de ello, haciendo que CIAM se convierta en el mayor segmento del mercado total de IAM, con un pronóstico de crecimiento del 15,1 %[1] anual hasta 2025. Para quienes aún no han iniciado su modernización digital, uno de los primeros y más importantes pasos consiste en alinear los liderazgos de las diferentes áreas funcionales para que todos puedan beneficiarse del proyecto.

Directores de marketing (CMO)

Objetivo CIAM: Captar, promover y aumentar los usuarios mediante experiencias personalizadas que tengan presente la privacidad y que estén controladas por ellos.

En el sector privado, los profesionales del marketing compiten por conseguir la atención de los clientes potenciales y lo último que quieren es una experiencia de registro farragosa que ahuyente a los clientes en el último minuto. El abandono de los clientes puede tener una repercusión directa en los ingresos, por lo que los programas CIAM persiguen racionalizar y agilizar las experiencias de registro e incorporación para evitar este problema y convertir clientes potenciales desconocidos en oportunidades de negocio. Un formulario de incorporación ideal solicita la mínima información posible al cliente, disponiendo puntos de toque apropiados a fin de obtener progresivamente información adicional conforme crece la relación con el cliente.

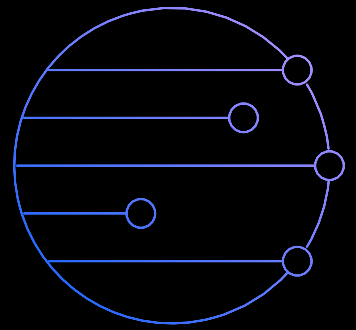
Las grandes organizaciones que posean varias submarcas habrán de diseñar sus almacenes de datos para mantener una única identidad por cada consumidor, integrando de paso la gestión de la relación con los clientes (CRM) y otras herramientas y sistemas de terceros. Con las identidades de los consumidores centralizadas, una implementación estratégica de las mejores prácticas de CIAM permitirá a los profesionales del marketing comprender mejor el comportamiento de sus consumidores y llevar a cabo campañas más orientadas y personalizadas. CIAM ocupa un lugar central en la experiencia digital tanto de clientes como de clientes potenciales, por tanto es de esperar que los responsables de marketing desempeñen un papel clave en el proceso de planificación de la modernización.



Directores de línea de negocio

Objetivo CIAM: Proporcionar una experiencia ágil y fluida con interfaces modernas y con el compromiso de contribuir a lograr los objetivos de la organización.

Los gerentes de negocio o responsables de organismos públicos comparten el objetivo de conseguir consumidores y posibilitar interacciones fluidas, aunque no necesariamente pensando en los ingresos. Por ejemplo, los organismos gubernamentales tienen que prestar servicios públicos a los ciudadanos y modernizar su implicación a través de un amplio abanico de preferencias de usuario y canales, por lo general sin contar con una función de marketing en la organización. Los responsables de los servicios públicos buscan transformaciones similares de la experiencia del usuario para simplificar el registro y reducir el abandono, y asegurar así la prestación de dichos servicios. Aunque no lleven a cabo campañas de marketing, estos gerentes de negocio buscan una única identidad para cada consumidor a fin de optimizar y agilizar las interacciones de los consumidores entre departamentos, eliminando así redundancias y comprendiendo mejor su comportamiento.

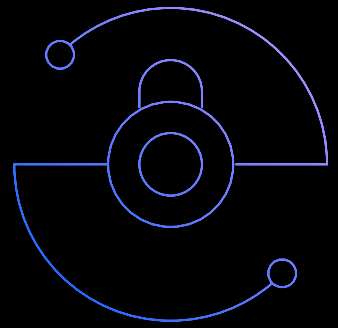


Responsables de seguridad y privacidad

Objetivo CIAM: Entregar interacciones de consumidor seguras que prevengan contra el fraude a los usuarios y contra el compromiso de las cuentas, y que ofrezcan una experiencia transparente controlada por el usuario a la vez que aseguran el cumplimiento normativo.

Como principio rector, los consumidores deberían saber quién está a cargo de sus datos y cómo se usan los mismos, y tener la opción de autogestionar sus propios datos y de modificar su consentimiento en cualquier instante. Esto ya es motivo suficiente para que las organizaciones prioricen la privacidad y la gestión de consentimientos en las experiencias digitales, por no hablar de la urgencia que añaden las regulaciones globales a esta cuestión. Las empresas han de atenerse a la normativa de cada región en la que operan si no quieren exponerse a sanciones y multas, y aunque la legislación sobre privacidad detalla minuciosamente lo que las organizaciones tienen que hacer, no suelen dar instrucciones concretas de cómo hacerlo. Una implementación CIAM adecuada actúa como única fuente de toda la información de identificación personal (PII). Los responsables de privacidad y los expertos de conformidad y cumplimiento pueden definir reglas y políticas con diversos propósitos de gestión de consentimiento para que el personal técnico las aplique en las aplicaciones que corresponda. Esto permite al personal de privacidad y cumplimiento ir más allá de las hojas de cálculo y cumplir con la realidad cambiante de la legislación de privacidad, haciéndolo más accesible.

Aunque un director de seguridad informática (CISO) tiene los mismos objetivos de privacidad y gestión de consentimientos que el responsable de cumplimiento, en ocasiones puede caer en la tentación de contemplar CIAM en su conjunto como una iniciativa de marketing y prestar más atención a otras prioridades. Tradicionalmente, la IAM de plantilla ha arrojado resultados bastante distintos de los que arroja la IAM de consumidores; sin embargo, ambas se benefician de soluciones comerciales que almacenan datos de forma segura y ayudan a mitigar el riesgo de vulneración de datos: merece la pena proteger las identidades tanto de empleados como de consumidores. Además, si las iniciativas CIAM no incluyen en su estrategia el estado actual de la infraestructura IAM, es probable que el CISO acabe implementando soluciones fragmentarias en el entorno de la organización, incrementándose el riesgo con puntos de acceso adicionales. Es del máximo interés para el CISO unificar los casos de uso IAM de plantilla y de consumidores bajo una única solución en la medida de lo posible, a fin de evitar silos de datos innecesarios.

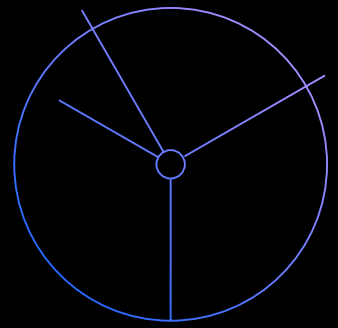


Directores de tecnologías de la información (CIO)

Objetivo CIAM: Reducir la complejidad de adoptar y mantener las soluciones IAM sin perder el ritmo de los estándares de identidad más recientes, a fin de mantener una postura de seguridad moderna.

Al margen de las ventajas que conlleva CIAM de cara al consumidor, el CIO tiene que evaluar el encaje de cada decisión tecnológica en el marco de la infraestructura global de la organización y del plan operativo. La simplicidad y la estandarización constituyen un ideal en sí mismas, de forma que la unificación de las funcionalidades IAM y CIAM en una única herramienta tiene sentido tanto desde el punto de vista del liderazgo de la TI como del de la seguridad. Con este enfoque, el entorno TI global ni crece en complejidad ni requiere que la plantilla adquiera nuevas destrezas. Probablemente, la reutilización de la misma solución para poblaciones externas conlleve una ventaja en términos de coste, con lo que los gastos operativos globales de la TI se mantendrán en mínimos.

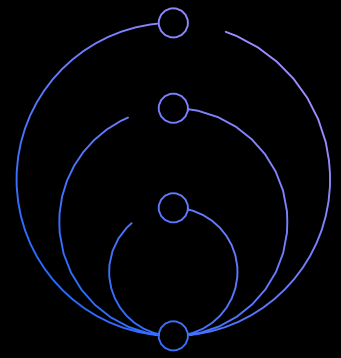
Una vez puesta en marcha la solución CIAM, cada minuto de interrupción puede suponer un perjuicio en términos de tiempo e ingresos para aquellas organizaciones cuyos clientes no puedan acceder a sus cuentas. Este hecho por sí solo explicaría por qué muchos responsables de TI prefieren soluciones basadas en la nube para los casos de uso CIAM desde el punto de vista del retorno de la inversión, ya que dichas soluciones tienden a ofrecer una disponibilidad y una escalabilidad mucho mayores que sus alternativas locales. Además, una IAM en la nube ofrece incentivos adicionales a las plantillas TI como, por ejemplo, un mantenimiento de infraestructura reducido, actualizaciones de software automáticas y una mayor celeridad en la obtención de valor.



Administradores y desarrolladores de IAM

Objetivo CIAM: Simplificar el trabajo de desarrollo y proteger y mantener las políticas de la aplicación mediante trabajos basado en flujos de configuración y mecanismos de desarrollo low-code

Mientras que las partes interesadas a nivel ejecutivo alinean sus objetivos de mayor nivel de negocio, costes operativos y mitigación de riesgos, los administradores y desarrolladores de IAM pueden influir en el desarrollo del programa CIAM evaluando las prestaciones técnicas de las soluciones en su conjunto. Pueden evaluar la logística de migrar o fusionar fuentes de datos y aplicaciones, además de aspectos clave como protocolos de autenticación , métodos MFA y canales de entrega. Para acelerar la obtención de valor, este equipo puede evaluar la documentación del API de las soluciones, recursos guiados y experiencias low-code, así como asegurarse de obtener un soporte adecuado durante la implementación y el mantenimiento de la solución. Prestaciones basadas en flujo de trabajo, como la gestión de consentimientos en la herramienta CIAM, pueden ahorrar más de un dolor de cabeza a los desarrolladores, por ejemplo, abstrayendo los detalles de la legislación de privacidad en sencillas llamadas de API que, de forma automática, se hagan cargo de los requisitos cambiantes. Antes de añadir otra herramienta más al mix, el personal técnico deberá llevar a cabo una asesoría global de la compatibilidad e integración con las soluciones IAM existentes, a fin de garantizar un encaje óptimo a largo plazo.



Enfoque CIAM integrado de IBM

Modernice sus experiencias digitales con el enfoque CIAM integrado de IBM

Con IBM Security, su organización puede captar clientes y conectar con ellos a través de interacciones multicanal a demanda personalizadas y seguras, combinando estrategia de identidad, experiencia en diseño digital y tecnología CIAM nativa en la nube. Combinando IBM Security Verify con IBM Security Services, podrá contribuir al alineamiento organizativo, hacer un seguimiento respetuoso y preciso de la información de los consumidores, y deleitar a sus consumidores con experiencias de marca sencillas y protegidas digitalmente.

Próximas etapas

Profundice con CIAM
Sepa más sobre las mejores prácticas CIAM, consideraciones de planificación y escollos a evitar

Descargue la guía →

Explore IBM Security Verify
Utilice IDaaS para modernizar las experiencias de usuario a través de inicios de sesión en redes sociales y de una autenticación adaptativa, a la vez que preserva la privacidad con gestión de consentimientos.

Infórmese sobre Verify →

IBM Security CIAM Services
Planifique, diseñe, despliegue y ejecute un programa CIAM conforme a objetivos de negocio usando un enfoque consultivo y colaborativo exclusivo

Obtenga ayuda con CIAM →

IBM España, S.A Tel.: +34-91-397-6611 Santa Hortensia, 26-28 28002 Madrid Spain

Producido en los Estados Unidos de América, febrero de 2021

[1] Markets and Markets, Consumer IAM Market Global Forecast to 2025