Consigue clientela respetando su privacidad

RESUMEN: Todas las empresas pueden hacer uso de la analítica Big Data para conocer a sus clientes, pero siempre respetando su privacidad y haciendo un buen uso de sus datos.

CATEGORÍAS: PROTECCIÓN DE DATOS

Nº HIPERVINCULOS: 1

La analítica de los Big Data descubre tendencias, muestra el comportamiento de los usuarios y permite realizar pronósticos. Los clientes desvelan, con sus datos de uso: cuáles son sus necesidades, cómo utilizan los productos y servicios, sus patrones de compra y anticipan los posibles cambios en la demanda.

Gracias a esta analítica, las empresas pueden optimizar la toma de decisiones, junto con sus estrategias de marketing, mejorando de esta forma su eficiencia interna. Y así, adaptando sus productos y servicios; a los gustos y necesidades de los consumidores.

No cabe duda de que cuanto mejor conozcamos a nuestros clientes y más nos adaptemos a ellos, nuestros productos y servicios serán mucho mejores.

Pero no todo vale, la retención masiva de datos (búsquedas, compras, comentarios…) con propósitos analíticos puede afectar a los derechos de los consumidores al suponer pérdidas en su privacidad y libertad individual.

Por ello, todas las empresas se enfrentan desde una perspectiva de seguridad y privacidad, a garantizar que los consumidores tengan el suficiente control sobre sus datos para prevenir el uso indiscriminado de estos.

Incibe señala una serie de retos de seguridad y privacidad a los que se enfrentan las empresas que usen Big Data:

- Falta de transparencia al solicitar el consentimiento.
- Pérdida de control del usuario sobre sus datos como en el caso de datos procedentes de sensores y cámaras, post en redes sociales o análisis de búsquedas en el web. Esto puede ser la causa de una pérdida de confianza.
- Reutilización de los datos más allá de su propósito original.
- Mala calidad de los datos o falta de integridad por proceder de fuentes no fiables.
- Inferencias no éticas y re-identificación al cruzar diferentes fuentes de datos que pueden causar violaciones de privacidad por desanonimización de los datos como muestran estos casos.
- Permanencia de datos personales durante largos periodos de tiempo, a la cual se opone el derecho al olvido.
- Pérdida o fuga de datos sensibles a gran escala con la consiguiente pérdida de imagen y daño a nuestros clientes.
- Discriminación en el caso de sistemas automáticos de toma de decisión por ejemplo si excluyen a usuarios por su supuesta capacidad de compra de la oferta de determinados productos y servicios.
- Dificultad para monitorizar y hacer cumplir los controles sobre la privacidad de los datos que hacen difícil por ejemplo la auditoría o la identificación de vulnerabilidades.