

2. APLICACIONES DEL BIG DATA EN EL MUNDO REAL

FUENTE: [migueltecnologia](#)

A continuación se muestran algunos **ejemplos de usos actuales de Big Data**:

- ◆ La empresa IBM tomó toda la información de los crímenes en Chicago y la procesó para hacer **análisis predictivos**. Con ello se consiguió detectar dónde era probable que ocurrieran los crímenes antes de que sucedieran. Esto lleva a la posibilidad de disminuir la criminalidad de una ciudad gracias al uso de Big Data. En el vídeo siguiente se muestra una dramatización que presentó IBM:



Police Use Analytics to Reduce Crime (IBM Commercial)



CityCop
273 suscriptores

Suscribirse

👍 164



➦ Compartir

➦ Guardar



<https://youtu.be/5n2UjBO22EI?feature=shared>

- ◆ En el campo de la salud hay múltiples usos. Por ejemplo, es posible **codificar el material genético** para conocer los alimentos más adecuados para un individuo y prevenir enfermedades crónicas. Se puede monitorear a bebés prematuros para **predecir sus enfermedades** antes de que aparezcan los primeros síntomas. Incluso se puede hacer un modelo informático para controlar la evolución de las epidemias.
- ◆ El Big Data está muy presente en el desarrollo científico, por ejemplo, en el **Colisionador de Hadrones (LHC) del CERN** se pueden llegar a producir 600 millones de colisiones por segundo. El control de este proceso exige analizar 30 Petabytes de datos en tiempo real, lo que exige una potencia de análisis de datos enorme (un Petabyte PB equivale a 10^{15} Bytes).
- ◆ Varias empresas de **logística** han empezado a usar Big Data para **optimizar sus rutas de entrega**, de tal modo que los tiempos de entrega son muchos menores, al igual que el combustible necesario.

3. LOS RIESGOS DEL BIG DATA

Cada vez generamos más datos. En el 2013 los usuarios de Internet habían generado cuatro zetabytes de información, lo que equivale a cuatro mil millones de terabytes. Y el crecimiento de datos es exponencial, ya que cada vez hay más personas generando datos con mayor frecuencia. (1 terabyte **TB** equivale a 1.024 gigabytes **GB**)

Así, los datos se han convertido en «el nuevo petróleo», el combustible que las empresas utilizan para generar negocio. Estas almacenan e interpretan los datos disponibles en la red para llegar a más usuarios y ofrecerle productos y servicios más personalizados, abrir nuevos mercados, hacer test de productos..., sin olvidar el potencial de persuasión de las redes sociales.

Pero el usuario empieza a ser consciente del valor de sus datos, a la vez que crece su preocupación por la seguridad de los mismos.

En este sentido, cuando pensamos en seguridad de los datos en internet, pensamos en ciberataques y en brechas de seguridad. Pero no es lo único que preocupa respecto al almacenamiento masivo de datos. ¿A qué riesgos nos expone el Big Data?:

1. La discriminación predictiva

El análisis predictivo puede ser utilizado para tomar decisiones sobre la adecuación de un usuario para, por ejemplo, acceder a un determinado trabajo, a un préstamo en un banco, conceder una tarjeta de crédito o un seguro de vida. Es decir, para tomar decisiones que afecten negativamente a las personas.

El riesgo no está en los datos en si, sino en la interpretación y/o asociación que pueden llegar a hacer las empresas, y en la toma de decisiones automática o basada en criterios poco lícitos. ¿Pueden llegar a discriminarse usuarios por una predicción hecha por un algoritmo? En este sentido, las empresas tendrán que llevar a cabo un esfuerzo para equilibrar el análisis predictivo con la atención personalizada, evitando las decisiones tomadas exclusivamente por un ordenador.

2. La pérdida de anonimato

Cada vez es más difícil, para el usuario común, llevar a cabo una acción online sin asociarla a su identidad. Necesitamos identificarnos para prácticamente cualquier cosa. De hecho, cada vez es más difícil para las empresas desvincular los datos para que no se pueda identificar a las personas, ya que generamos una ingente cantidad de información que se puede cruzar y conectar.

La clave para las empresas será la implementación de sistemas de seguridad que garanticen la privacidad y seguridad de los datos, y la capacidad para generar confianza en los usuarios. Por parte de los usuarios, cada vez se educa más en limitar la cantidad de información personal que se vuelca en la red.

3. El uso gubernamental de la información y el control social

Los gobiernos almacenan cada vez más datos personales de los ciudadanos: nombre, raza, sexo, lugar y fecha de nacimiento, números de Seguridad Social, de carnets de conducir, de teléfono, fotografías, huellas dactilares, información financiera... e incluso tendencias sexuales o afinidades políticas.

El uso inapropiado de esta información es un peligro muy real. Los casos recientes de los gobiernos de [Rusia](#), [China](#) o [Australia](#) (por el uso o [recopilación de datos](#)) son solo la punta del iceberg.

Para evitar los problemas anteriores, cada vez más los gobiernos intentan limitar el acceso a los datos por parte de empresas. Sin embargo, a su vez, también se establecen leyes para controlar la información que circula por internet. Ésto puede llevar a limitar o directamente prohibir aquélla que los gobiernos estimen poco adecuada o perjudicial según su criterio, imponiendo a las empresas que manejan datos un control sobre las plataformas y usuarios que generan y difunden contenidos. Esto es un arma de doble filo pues aunque siempre se argumentará que se trata de proteger a la población de información “sensible”, “perjudicial para la salud” o “contraria a los valores comunitarios”, se convierte en un mecanismo de control para evitar que se genere, difunda o acceda a contenidos contrarios a la narrativa oficial, imponiendo una censura y vulnerando el principio de la libertad de opinión y expresión.



Estimado anunciante:

En febrero del 2024, Google actualizará la [política Contenido inapropiado](#) para aclarar la definición del término "Acontecimiento Sensible".

Un "Acontecimiento Sensible" es un evento o suceso imprevisto que pone en un riesgo considerable las capacidades de Google de ofrecer datos validados, relevantes y de alta calidad, así como de reducir la monetización o la aparición en posiciones prominentes de contenido que muestre una falta de sensibilidad o saque provecho de tales eventos. Durante un Acontecimiento Sensible, Google puede llevar a cabo distintas acciones para hacer frente a esos riesgos.

Algunos ejemplos de Acontecimientos Sensibles son aquellos con un impacto social, cultural o político significativo, como emergencias civiles o sanitarias públicas, desastres naturales, actos terroristas y actividades relacionadas con el terrorismo, conflictos o actos de violencia masiva.

Ejemplos de lo que no está permitido (lista no exhaustiva):

- Productos o servicios que sacan provecho, niegan o justifican un Acontecimiento Sensible, lo que incluye una subida abusiva o inflación artificial de precios que impida o restrinja el acceso a suministros básicos; y la venta de productos o servicios que puedan escasear ante la demanda durante un Acontecimiento Sensible
- Uso de palabras clave relacionadas con un Acontecimiento Sensible para tratar de conseguir más tráfico
- Contenido que afirme que las víctimas de un Acontecimiento Sensible son responsables de su propia tragedia o en el que se las culpe de una manera similar; contenido que afirme que las víctimas de un Acontecimiento Sensible no merecen soluciones ni apoyo; y contenido que afirme que las víctimas de determinados países son responsables de una crisis sanitaria mundial o se la merecen

4. El negocio de los datos

El Big Data ha generado nuevos modelos de negocio, algunos de ética discutible, como el negocio de la compraventa de datos. Cada vez más empresas venden datos enlazados al perfil del usuario, con lo que la empresa compradora puede ofrecer productos altamente personalizados. Así, los datos de un embarazo, las tendencias sexuales de la persona o una enfermedad pueden quedar revelados por la atención que preste a la publicidad a la que someten a la persona, aunque esta no lo desee y dejándole poco margen para la privacidad.

5. Los ciberataques

La cada vez mayor interconectividad y tráfico de datos hace que incremente también el riesgo de robo, pérdida, suplantación de identidad... Cada vez los ataques de ciberseguridad son más graves y de peores consecuencias.

FUENTE: elaboración desde [Mitek Systems](#) y [Pedro Baños](#)

CUESTIONES II:

1.- Nombra 3 ejemplos de usos del Big data en la vida real

-
-
-

2.- Nombra al menos 3 riesgos del BIG DATA

-
-
-

3.- ¿Qué problemas puede causar la “discriminación predictiva”?

4.- ¿Qué peligro encuentras en que alguien disponga de información sobre tus gustos, opiniones, habilidades, medios...?

5.- ¿De qué maneras el Big Data puede vulnerar la intimidad?

6.- ¿Qué tiene que ver la información con el control social?