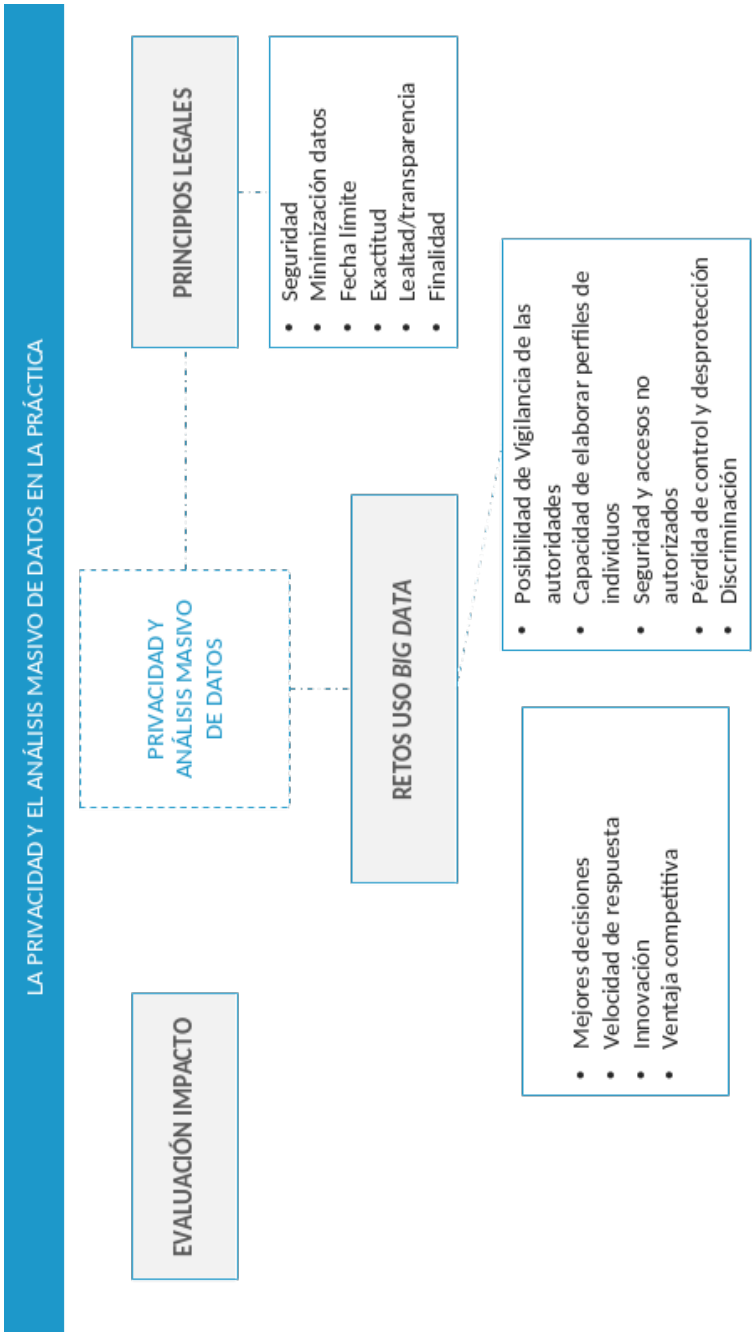
Estrategia y Gestión Empresarial Basada en Análisis de Datos

Tema 8. La privacidad y el análisis masivo de datos en la práctica

Índice

Esquema



8.1. Introducción y objetivos

Como ya hemos introducido en el tema anterior, la nueva cultura empresarial de gestión *data-driven* exige de un proceso de alfabetización digital y de la observancia de ciertos aspectos éticos y legales con los que han de operar las diferentes unidades de gestión y que, combinados con el análisis masivo de datos, genera una serie de restos específicos para la empresa que tratamos de abordar en este tema, centrado en la **interacción del *big data* y la protección de datos**.

Los **objetivos** y la relación de tópicos analizados en el tema son:

- Comprender los retos generales del uso del *big data* en el entorno de la empresa.
- Entender las implicaciones para la privacidad y los aspectos normativos que tener en cuenta en un proyecto que implique análisis masivo de datos.
- Realizar una breve introducción a las llamadas evaluaciones de riesgos en términos de privacidad.

8.2. El big data y sus retos

El **análisis masivo de datos**, popularmente conocido como *big data*, hace referencia a las nuevas posibilidades de uso automatizado de la información generada por la nueva capacidad tecnológica para recoger, almacenar, analizar y sacar todo el valor económico de los conjuntos de datos digitales generados en la nueva sociedad digital.

Estos datos, recopilados de diferentes formas y con diferentes fines por distintas instituciones, plataformas e incluso por los gobiernos, permiten a estos el análisis exhaustivo de los mismos a través de algoritmos más o menos complejos, que permiten mejorar la efectividad de sus acciones, pero también, en algunas situaciones, suponen un riesgo y amenaza sobre las libertades y los derechos de los ciudadanos.

Convendremos que el uso del análisis masivo de datos es un factor de competitividad que potencia la efectividad de las diferentes estrategias de la empresa en las diferentes unidades de la operativa de la empresa. Sus usos pueden ir desde el apoyo a la predicción de fallos o del mantenimiento de inventarios, al conocimiento de las preferencias o hábitos de compra, sin olvidarnos de los sistemas de recomendación o la segmentación de los grupos de consumidores y las previsiones de la demanda o de cualquier tipo de comportamiento por parte de los diferentes agentes con los que interacciona la empresa.

El reto principal es el **compatibilizar o conciliar** este uso optimizador y de aumento de la efectividad y competitividad con la no vulneración de derechos de los cesionarios de los datos, evitando que puedan ser usados para otros fines diferentes a aquellos por los que fueron cedidos o no poder ser usados en su contra. Sin embargo, habría que distinguir qué tipos de datos son los que presentan una mayor sensibilidad para los individuos y qué límites habría que imponer al uso de otros

datos derivados.

Los datos de los que dispone una empresa son sobre la base de voluntariedad consciente o no de su cesión:

- Datos **voluntarios**, es decir, aquellos en los que las personas participan de su creación y deciden compartirlos de forma consciente (por ejemplo, los datos que decidimos compartir en redes sociales públicas).
- Datos **observados**: los procedentes de los actos que realizamos, tales como las ubicaciones de nuestros dispositivos móviles o los datos sobre conexiones y usos de Internet, entre otros.
- Datos **inferidos**: los datos generados a partir del análisis de datos voluntarios u observados (por ejemplo, la solvencia o capacidad de endeudamiento que realizan las entidades financieras sobre la base de nuestro histórico bancario).

El uso de estos datos, por tanto conlleva unos potenciales beneficios para las empresas y un potencial riesgo o coste asociado de sobrepasar los límites legales al uso de la misma. El análisis coste-beneficio del *business compliance* ha de llevar a las empresas a elegir en el *trade-off* entre los límites al uso de los datos —riesgo moral, riesgo social o de reputación, riesgo penal y riesgo económico derivado del castigo por el incumplimiento de la norma— y los beneficios derivados de la monetización de sus potenciales usos.

En la mente de todos se encuentran numerosos ejemplos en los que diferentes plataformas y empresas de telecomunicaciones se enfrentan a multas multimillonarias por haber usado, rastreado y analizado, sin consentimiento, los datos facilitados sin consentimiento o con fines distintos a los expresados cuando se cedieron, es decir, con los llamados **términos del servicio**.

En general y a modo de resumen sistemático, la siguiente figura sintetiza los argumentos más comúnmente utilizados sobre potencialidades para las empresas y

amenazas para los usuarios del *big data*.

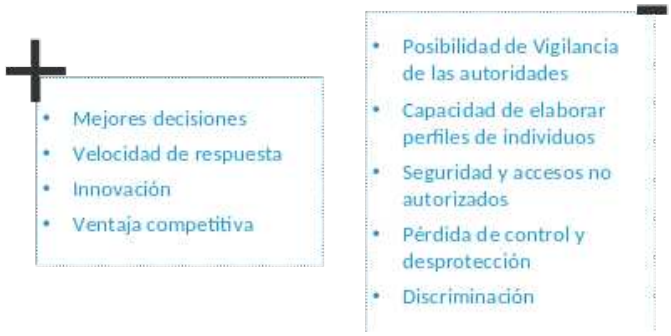
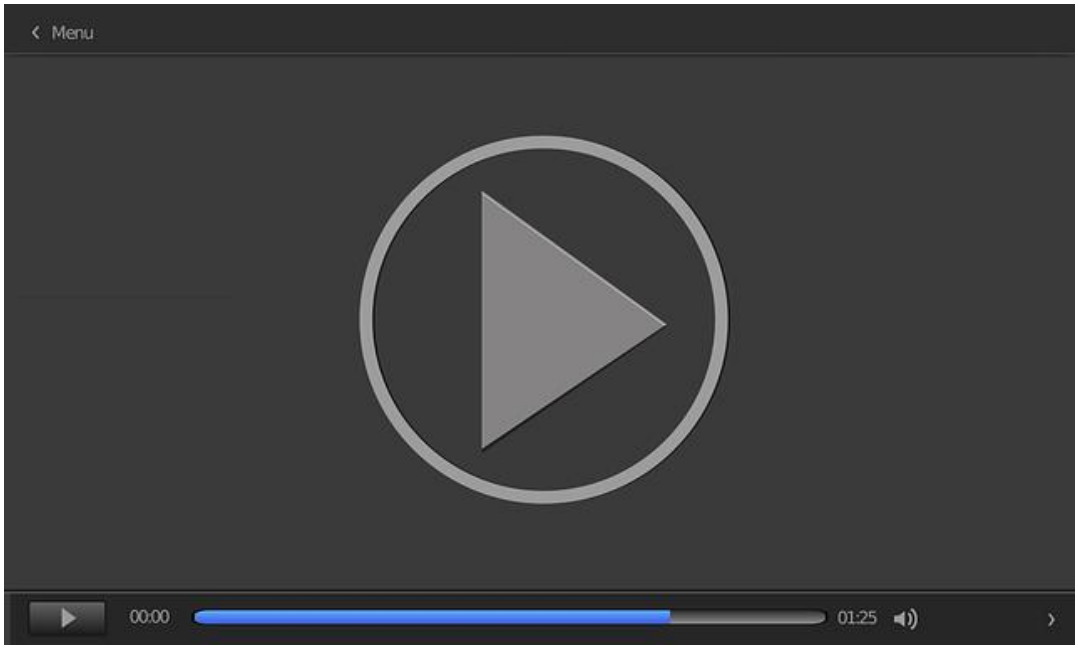


Figura 1. Ventajas e inconvenientes del *big data*.



Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=6d377954-577d-45d6-8b3b-b15d0080233b

8.3. Reglas y principios para un tratamiento de datos responsable

Recordemos en este apartado a modo de resumen cuáles deberían ser los **principios legales** que seguir en un tratamiento de datos. Como recordará el estudiante, el tratamiento de datos debe alinearse con los principios de la protección de datos personales, tal y como son entendidos en el RGPD (R (UE) nº2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016), principios relativos al tratamiento. Recordémoslos brevemente.

Figura 2. Principios legales en el tratamiento de los datos.

A todos estos principios deberíamos añadir el hecho de que es la empresa la que ha de garantizar estos principios y la licitud de los tratamientos, a través de su responsable o encargado de estos, con un consentimiento finalista, legítimo, explícito y demostrable, teniendo especial precaución con el hecho de que determinadas operaciones de análisis de datos o el enriquecimiento de los datos con otras fuentes externas no atenten contra la privacidad o posibiliten la identificación de personas físicas y jurídicas.

Igualmente se ha de garantizar el efectivo ejercicio de los derechos de acceso, rectificación, supresión y oposición. Caben ciertas excepciones normativas al tratamiento en fecha posterior en el caso de análisis de datos con fines históricos, científicos o relacionados con las operaciones de la estadística pública

Un aspecto de especial importancia en los entornos digitalizados y globales es que se han de poner en marcha métodos efectivos que impidan que terceros puedan utilizar la información para identificar a los sujetos de la misma o sus ubicaciones, cuestión especialmente delicada cuando nos movemos en marcos internacionales en los que las normativas aplicables en materia de protección no son coincidentes.

En definitiva, una **delimitación precisa de la finalidad** con la que se recogen los datos, que sea **legítima**, acompañado del **principio de minimización** (sin solicitar información que no sea estrictamente necesaria para los objetivos), deberían ser los principios orientadores de la privacidad en relación con el análisis masivo de datos.

Teniendo siempre presente el haber obtenido un consentimiento válido y haber sido especialmente transparentes con el cesionario de los datos en lo referente a qué información se recopila, con qué fin y si hay o no transmisión a terceros.

Se incluye, cuando sea preciso, información sobre los algoritmos utilizados para la creación de perfiles, haciendo uso de la anonimización (cuando sea posible) como forma de garantizar la privacidad, cumpliendo la normativa e intentando que las clasificaciones generadas de la analítica sean justas en el sentido de minimizar la generación de clasificaciones incorrectas (falsos positivos o negativos).

8.4. Evaluaciones de impacto

Como cualquier otra evaluación de tratamientos o de posibles efectos, una evaluación de impacto en materia de protección de datos no es más que un análisis prospectivo de los potenciales riesgos que los protocolos y prácticas de tratamiento de datos de una empresa pueden plantear en términos de protección de datos personales.

En nuestro ámbito y como aproximación inicial al análisis de una metodología de **evaluación de protección de datos (PIA, *privacy impact assesment*)**, repasamos en este apartado los principios orientadores que nos ofrece la Agencia Española de Protección de Datos, en su guía acerca de cómo diseñar e implementar una evaluación de impacto en materia de protección de datos, práctica en general no obligatoria desde el punto de vista legal.

Algunas excepciones que plantea el Reglamento General de Protección de datos hacen referencia a situaciones en las que el tratamiento de la información pueda poner en peligro la tutela efectiva de derechos y libertades de los interesados, a causa de la finalidad, por la naturaleza de los datos, por el tipo de tecnología que se usa.

Por ejemplo, sería obligatorio en casos en los que se proceda a la elaboración de perfiles de los que se deriven consecuencias jurídicas o videovigilancia de zonas públicas, entre otras.

No obstante, la **evaluación de impacto** sí es muy recomendable en el ámbito de las empresas *data-driven* y especialmente importante en aquellas empresas que hayan incorporado el análisis masivo de datos a su operativa.

En general, y sin ánimo de exhaustividad, se recomienda que esta evaluación esté presente, al menos, cuando:

Ideas clave

- Los datos vayan a ser usados para perfilados (ya pueden ser estos relativos a grupos de clientes o a perfilados de desempleados para el posible diseño de tratamientos formativos que aumenten su empleabilidad).
- Los datos existentes para los que se pidió consentimiento vayan a ser enriquecidos con nuevas fuentes de datos.
- Se contengan datos personales de colectivos vulnerables —por ejemplo, menores— o si se pretende predecir o evaluar comportamientos de los incluidos en el fichero de datos.
- El análisis de datos pueda generar consecuencias.
- Se usen tecnologías intrusivas (visualización).
- Se manejen grandes volúmenes de datos con técnicas de *big data*, procedentes del IoT *(Internet of things)* o de los dispositivos y sensores de *smart cities*.
- Existan cesiones de datos.
- Existan transferencias internacionales de datos.

Llegados a este punto, delimitemos el contenido y alcance de una evaluación de impacto en materia de protección de datos. Aunque la finalidad última de la evaluación es establecer una estrategia previa que nos garantice, *a priori* y al menos, el cumplimiento de la normativa en protección de datos personales, esta evaluación debería realizarse durante el proceso de creación de la empresa y, en cualquier caso, cada vez que se lance un nuevo bien o servicio o se ponga en marcha un nuevo sistema de información o se produzcan cambios sustanciales en los existentes.

Con carácter general, las fases de elaboración de una evaluación de impactos en materia de protección de datos se resumen en la siguiente figura.

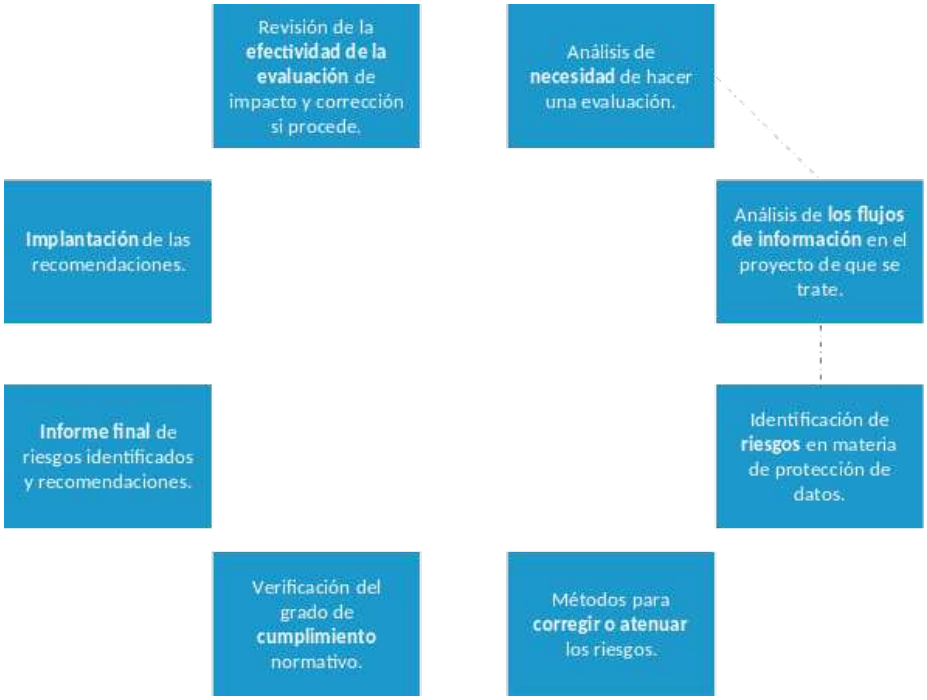


Figura 3. Proceso de evaluación de impactos.

En definitiva, el objetivo de la evaluación de impacto en materia de protección de datos es el de realizar una evaluación *ex-ante* de los riesgos potenciales existentes, comenzando por la propia necesidad o no de realizar esta evaluación de impacto para, en su caso, proponer medidas que mitiguen o eliminen estos riesgos.

Todo el proceso ha de tener un carácter dinámico, en tanto en cuanto el informe inicial, caso de ser asumido por la dirección, ha de ser implementado y corregido en su caso gracias a la retroalimentación y continua evaluación de sus resultados.

8.5. Referencias bibliográficas

Unión Europea. Reglamento (UE) nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, *L119/1*, 4 de mayo de 2016.

Data Protection Impact Assesment (DPIA)

EDPB. (S. f.). *Data Protection Impact Assessment (DPIA)* [En línea]. Recuperado de https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en

Documentos del Comité Europeo de Protección de Datos sobre evaluación de impacto y principios orientadores.

Privacidad: principios y directrices

Agencia Española de Protección de Datos. *Privacidad: principios y directrices* [En línea]. Recuperado de https://www.aepd.es/reglamento/cumplimiento/index.html

Sección de la web de la Agencia Española de la Protección de Datos en la que puedes profundizar en los principios de la privacidad.

1. Entre los principios de la privacidad se enmarca el establecimiento de una fecha límite para la conservación de los ficheros, excepto:

A. Para algunas empresas.

B. Si se dispone de autorización.

C. Para algunos fines de investigación y estadísticos.

D. Todas son correctas.

2. Sobre la base del principio de minimización de datos, el enriquecimiento de datos con otras fuentes:

A. Debe ser una conducta prohibida.

B. Supone una violación del principio, aunque es legal.

C. Es uno de los casos en los que la AEPD recomienda una evaluación de impacto.

D. Ninguna de las anteriores es correcta.

3. En un informe de evaluación de impacto en materia de protección de datos qué fase o fases precederían a la de elaboración del informe:

A. Diseño de métodos de mitigación atenuación.

B. Identificación de riesgos.

C. Análisis de la necesidad de la evaluación.

D. Todas las anteriores son correctas.

4. ¿En qué casos de los siguientes no se recomienda la realización de una evaluación de impacto?

A. Cuando el tratamiento afecta a un número elevado de personas.

B. Cuando se traten con técnicas de big data o de videovigilancia.

C. Cuando existan cesiones de datos.

D. Cuando el tratamiento es esporádico y limitado.

5. ¿Qué afirmación de las siguientes es falsa dentro de las evaluaciones de impacto?

A. La normativa europea obliga a la realización de evaluaciones de impacto anuales a las nuevas empresas.

B. La evaluación de impacto es un proceso sistemático y revisable.

C. El resultado de la evaluación se debe plasmar en un informe.

D. La evaluación de impacto debe ser un proceso periódico.

6. Señala cuál de los siguientes argumentos referidos al big data supone una desventaja para el usuario:

A. Pérdida de privacidad.

B. Pérdida de control en sus decisiones de compra.

C. Las dos anteriores son correctas.

D. Ninguna es correcta.

7. Desde el punto de vista de las empresas, señala cuál de las siguientes afirmaciones es una ventaja derivada del uso del big data:

A. Puede obtener una mayor rentabilidad, ya que ofrece soluciones mejor adaptadas a las necesidades de los consumidores.

B. Incrementa la velocidad de respuesta a los mercados.

C. Las dos anteriores son correctas.

D. Ninguna es correcta.

8. Con respecto al proceso de evaluación de impactos, podemos afirmar que:

A. El informe final de riesgos supone el punto final del proceso.

B. El proceso es estático y solo se pone en marcha cuando se detecta algún problema.

C. Es independiente de la dirección.

D. Ninguna es correcta.

9. La evaluación de impacto está recomendada cuando:

A. Los datos vayan a ser usados para establecer perfiles.

B. Cuando los datos requeridos vayan a ser completados.

C. Cuando los datos pertenezcan a colectivos vulnerables.

D. Todas son correctas.

10. ¿Cuál de estas opciones no está entre los principios orientadores de la privacidad?

A. No solicitar información por encima de la estrictamente necesaria.

B. Solicitar todo tipo de información para no volver a molestar al usuario.

C. Informar de la finalidad y del uso de la información.

D. No transmitir a terceros la información obtenida.