# Seguridad y privacidad de datos

PID_00246839

David Cabanillas Barbacil

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

# Índice

**Introducción** ..... 5

**Objetivos** ..... 7

**1. La seguridad del dato** ..... 9
1.1. El reto de la seguridad del dato ..... 9
1.2. ¿Qué es la seguridad del dato? ..... 12
1.3. Compitiendo con datos bajo la premisa de seguridad y privacidad ..... 14

**2. Privacidad y normativa de datos** ..... 16
2.1. Privacidad de datos ..... 16
2.2. Privacidad por diseño ..... 17
2.2.1. Principios de la privacidad por diseño ..... 17
2.2.2. Ventajas de la privacidad por diseño ..... 18
2.2.3. Barreras de la privacidad por diseño ..... 18
2.3. Normativas de datos ..... 19
2.3.1. Normativas ..... 19
2.3.2. Normativa europea ..... 21
2.3.3. Normativa española ..... 22
2.3.4. Más allá de las normativas de datos ..... 25

**3. Programa de seguridad de datos** ..... 27
3.1. Principios del programa de seguridad de datos ..... 28
3.2. Personas, procesos y tecnología ..... 29
3.3. Seguridad de datos en contexto de gobierno del dato ..... 31
3.4. Mejores prácticas ..... 32
3.5. Elementos clave de la seguridad y la privacidad ..... 34

**4. Técnicas y tecnología para la gestión de la seguridad y privacidad del dato** ..... 36
4.1. Técnicas ..... 36
4.2. Tecnologías ..... 36
4.3. Marco tecnológico ..... 38
4.3.1. Clasificación / sensibilidad de los datos ..... 39
4.3.2. Auditoría de los datos ..... 39
4.3.3. Anonimización de los datos ..... 39

4.3.4. Monitorización de los datos ..... 41

**Resumen** ..... 42

**Glosario** ..... 43

**Bibliografía** ..... 45

# Introducción

Como ya sabemos en la actualidad, el dato se ha convertido en uno de los activos más importantes. Vivimos una época en la cual la información fluye como nunca antes lo había hecho, y se multiplican las formas para capturar, procesar, almacenar, analizar y visualizar datos, así como sus casos de uso. Esto provoca la aparición de múltiples repositorios de datos como el *data warehouse* y *data lake*, y servicios fundamentados en datos, *big data* y *machine learning*. Este apalancamiento en tecnología y datos ha disparado también las brechas en seguridad en todos los sectores*. Por lo que toda organización tiene la imperiosa necesidad de proteger sus activos de datos, tal y como apunta Gartner.

**Lectura complementaria**

**Lowans, B.; MacDonald, N.; Meunier, M.; Reed, B.** (2016). *Predicts 2017: Application and Data Security*. Gartner

*** Más información en: https://goo.gl/fqlZq1**

Esta necesidad tiene dos vertientes:

- Como **organizaciones**, debemos invertir en capacidades de ciberdefensa para proteger nuestra marca, capital intelectual, información de clientes e infraestructura crítica; así como crear mecanismos para la detección de incidentes y la respuesta para proteger los intereses de la organización y sus elementos más importantes: personas, procesos, tecnología y datos.

- Como **usuario**, cuando tenemos una interacción con una organización (ya sea abriendo una cuenta bancaria, creando un usuario en una red social o reservando un vuelo en una aerolínea), se entrega información personal como nombre, dirección o número de tarjeta de crédito. Múltiples preguntas que nos suelen asaltar en todos estos casos son: ¿qué sucede con estos datos? ¿Podrían caer en manos equivocadas? ¿Qué derechos tengo con respecto a su información personal?

Estas dos vertientes confluyen. Por un lado, toda persona tiene derecho a la protección de sus datos personales. Por otro, según la legislación del país en el que opera la organización, los datos personales solo pueden recopilarse legalmente en condiciones estrictas, con un fin legítimo. Además, las personas u organizaciones que recogen y gestionan su información personal deben protegerla del uso indebido y respetar ciertos derechos de los propietarios de los datos. Por lo tanto, las organizaciones están obligadas por ley a ofrecer seguridad y privacidad en los datos que almacenan.

En este módulo, se describen la legislación, las políticas y las mejores prácticas que se deben incluir para que las organizaciones dispongan de datos seguros y privados, mediante el uso de procesos documentados, transparencia del uso, comunicación eficaz, revisión y aplicación de las prácticas de seguridad, capa-

citación suficiente del personal y un compromiso de proteger la integridad y el uso autorizado de los datos de los usuarios.

La seguridad del dato se enmarca también dentro del ámbito del gobierno del dato, de forma natural. La explotación eficiente del dato pasa por tener la capacidad de planificar, desarrollar y ejecutar políticas y procedimientos para asegurar la autentificación, autorización, acceso y auditoría de los activos de datos e información.

En este módulo, estudiaremos la necesidad e importancia de la seguridad y privacidad del dato, en qué consiste, qué aporta, cómo implementarla, qué debemos tener en cuenta como mejores prácticas y qué tecnologías soportan la seguridad y privacidad del dato.

# Objetivos

Este material didáctico está dirigido a:

**1)** Desarrolladores y consultores que quieren conocer qué significa la seguridad y privacidad dentro del *data governance*.

**2)** Desarrolladores y consultores que quieren ayudar al desarrollo de estrategias de seguridad y privacidad dentro del *data governance*.

**3)** Gestores y juristas que están interesados en la transformación digital de su organización y en la inclusión de gobierno del dato y su seguridad.

En los materiales didácticos de este módulo, encontraremos las herramientas indispensables para asimilar los siguientes objetivos:

1. Entender el concepto de privacidad y seguridad en el contexto del *data governance*.
2. Entender los problemas de seguridad y privacidad, así como las normativas.
3. Aplicar sistemas de seguridad en el *data governance*.

Si bien la obra es autocontenida en la medida de lo posible, los conocimientos previos necesarios son:

**1)** Conocimientos básicos sobre *business intelligence* y *big data*.

**2)** Conocimientos sobre estrategia y gestión de las tecnologías de la información (TI).

Se introducirán los conceptos necesarios para el seguimiento de este material.

# 1. La seguridad del dato

## 1.1. El reto de la seguridad del dato

En los últimos años, la seguridad del dato ha pasado de pertenecer fundamentalmente al ámbito técnico a convertirse en una prioridad de negocio. Este cambio de percepción se debe a la aparición de medidas legislativas, del uso de la tecnología, tanto en el ámbito profesional como personal, y a los crecientes problemas generados por una escasa atención a este punto.

Las organizaciones deben conocer qué riesgos existen y cómo mitigarlos. En esencia, la organización debe ser capaz de:

- Trabajar en un entorno de flexibilidad y movilidad organizativa, sin perder la confidencialidad, integridad o disponibilidad de los datos.
- Conocer y comprender el cumplimiento normativo para evitar sanciones y consecuencias penales.
- Conocer y aplicar las coberturas existentes ante el robo de información o ataque a los sistemas empresariales.
- Custodiar y mantener la confianza de los clientes y la reputación de la marca.

Sin embargo, el reto de la seguridad del dato es complejo, puesto que los riesgos podemos encontrarlos en personas, procesos y tecnología.

Estudios de Osterman Research como *SMB Rogue Access Study*, publicado en el 2014, ponen de manifiesto que los empleados son frecuentemente el origen de problemas de las brechas de seguridad, ya que el 68 % de los encuestados manifestaron que guardaron documentos corporativos en servicio de almacenamiento en la nube (como Dropbox o Google Drive). Estas brechas de seguridad de datos pueden ser por desconocimiento o a propósito, como en el caso de los documentos desclasificados por Snowden.

En junio del 2013, Snowden hizo públicos, a través de *The Guardian* y *The Washington Post*, documentos clasificados como alto secreto sobre varios programas de la National Security Agency (NSA), incluyendo los programas de vigilancia masiva PRISM y XKeyscore.*

***Más información en: https://goo.gl/5dBkRa**

Todo tipo de organizaciones están teniendo problemas relacionados con la seguridad de datos. Por ejemplo, el sistema de contraseñas de LinkedIn ha sido comprometido varias veces*. En el 2012, afectó a 6,5 millones de usuarios. En el 2014, a 117 millones. En el 2015, 37 millones de usuarios de Ashley Madison, servicio de citas en línea, fueron comprometidos**.

* Más información en: https://goo.gl/9p4cP8

** Más información en: https://goo.gl/le0Vj1

Como es posible imaginar, el tema de la seguridad y privacidad de datos no es nuevo. Ya en la década de los setenta, era una preocupación reconocida en ámbitos como registros médicos o información financiera. En esta década, se adoptaron las prácticas de información justas (FIP, acrónimo de *fair information practices*), que seguían estos puntos:

- **Franqueza**: no debe haber sistemas para recolectar datos personales sin el consentimiento/conocimiento de los individuos.
- **Revelación**: las organizaciones deben revelar a las personas de qué información disponen y cómo la utilizan.
- **Uso secundario**: la información recolectada para un propósito no debe ser usada para otro propósito sin el consentimiento del individuo.
- **Corrección**: las personas deben tener la capacidad de corregir o enmendar su propia información.
- **Seguridad**: toda organización que cree, mantenga, utilice o difunda datos personales identificables debe asegurar que los datos se están utilizando correctamente y tiene que tomar precauciones para evitar el uso indebido.

Hoy en día, los retos se han magnificado pero los cinco puntos descritos en las prácticas de información justas siguen siendo válidos. Se trata de un escenario más complejo, producto de un entorno cambiante y mucho más descentralizado, en el que el dato permite proporcionar servicios más personalizados a cambio de la privacidad, tal y como comenta Enrique Dans*.

* Más información en: https://goo.gl/x6Mrnp

> Aunque parece un futuro lejano, ya existen sistemas autónomos sin interacción humana y que se fundamentan en nuestras preferencias y comportamientos. Existen ya semáforos que se adaptan al flujo de tráfico, botones que nos permiten pedir de nuevo nuestra pizza favorita e incluso termostatos que gestionan la temperatura adecuada en nuestra casa.
>
> A medida que más elementos generan datos (como contadores inteligentes de agua, electricidad o gas, o dispositivos como Amazon Echo), es posible inferir comportamientos anómalos o descubrir aspectos personales y privados. Lo que puede llevar a plantearse preguntas como:
>
> - ¿Nos lleva el desarrollo de los *smart homes* a un desequilibrio entre conveniencia y privacidad?
> - ¿Debería Amazon alertar a la policía, por ejemplo, si su dispositivo captura determinadas grabaciones, bien efectuadas a propósito o bien accidentales, que permitan deducir que se está cometiendo un delito?
> - ¿Puede ser Amazon Echo presentado como prueba en un delito?

- ¿Si Amazon hubiera eliminado los datos, se podría considerar a la organización encubridora de un asesinato?

- ¿Qué sucede si se acepta como prueba la grabación del dispositivo y al final el culpable no lo era? ¿Qué sucede si datos de diferentes dispositivos no aclaran con exactitud el asesinato? Por ejemplo, que otra grabación de otro dispositivo se contradiga con la grabación del de Amazon Echo o demuestre que no podía estar en ese momento en la escena del crimen.

Estos escenarios ponen en evidencia que las organizaciones se enfrentarán a más y más desafíos de seguridad y privacidad, motivados por:

- ***Big data***: tal y como apunta *The Economist**, *big data* abre la puerta a lo siguiente:

*** Más información en el artículo del 2012: *The challenge of big data for data protection***

– La recolección de datos a gran escala permite el seguimiento y la creación de perfiles de usuarios.

– La seguridad de los datos distribuidos.

– Inexactitud y duplicidad a gran escala.

– Aumento de las posibilidades de vigilancia por parte del gobierno u organizaciones.

- ***Cloud computing***: el almacenamiento de datos en la nube genera dudas sobre la legislación que aplica en el centro de datos remoto y en la transmisión de datos.

- **Enriquecimiento de datos**: cuando se cruzan datos de múltiples fuentes, emergen patrones que pueden vulnerar la privacidad de los usuarios. Por ejemplo, si los bancos revisan todas nuestras compras, pueden conocer qué medicamentos estamos utilizando y, así, ofrecer diferentes precios en sus seguros o en la obtención de préstamos.

- **Fusiones y adquisiciones**: ¿qué sucede con el dato, como activo de valor, cuando dos organizaciones se fusionan o una compra a otra? Tal y como ilustra la figura 1, esta situación es más común: En el caso de la compra de

  WhatsApp por parte de Facebook, la Comisión Europea evaluó esta situación de consolidación para determinar si afectaba al mercado competitivo.

- **Transferencia automática de datos**: este proceso requiere ser validado para asegurar que los datos no sufren modificaciones durante la trasferencia. De hecho, aquí surgen iniciativas como *blockchain*. ¿Cómo se enfrentarán las organizaciones en un mundo interconectado de manera omnipresente, con datos distribuidos y con miles de intercambios de datos diarios?

Figura 1. Fusiones entre organizaciones que trabajan con datos


Fuente: David Cabanillas

## 1.2. ¿Qué es la seguridad del dato?

En la seguridad y privacidad de la información, el objetivo principal es la protección de los datos y tratar de evitar su acceso, pérdida y modificación no autorizada. La seguridad y privacidad deben garantizar, en primer, lugar la **confidencialidad**, **integridad** y **disponibilidad** de los datos. Estos puntos coinciden con el gobierno y la gestión del dato. Sin embargo, existen más requisitos como, por ejemplo, la **autenticidad** o la posibilidad por parte del usuario de poder **verificar/modificar/eliminar** los datos que contienen las organizaciones.

Tal y como articula la **Declaración Universal de los Derechos Humanos** (DUDH), la seguridad y la privacidad de las personas son un derecho, por lo que los diferentes estados han creado leyes. Estas medidas están dirigidas a regular los distintos aspectos de la actividad de negocio relacionados con las tecnologías de la información y la sociedad. El cumplimiento de las obligaciones legales proporciona unas garantías de protección de los derechos sobre los activos de información empresarial (carteras de clientes, contratos, patentes, etc.) que son trascendentales para el negocio, sin olvidar que así se respetan los derechos de clientes y usuarios.

**DUDH**

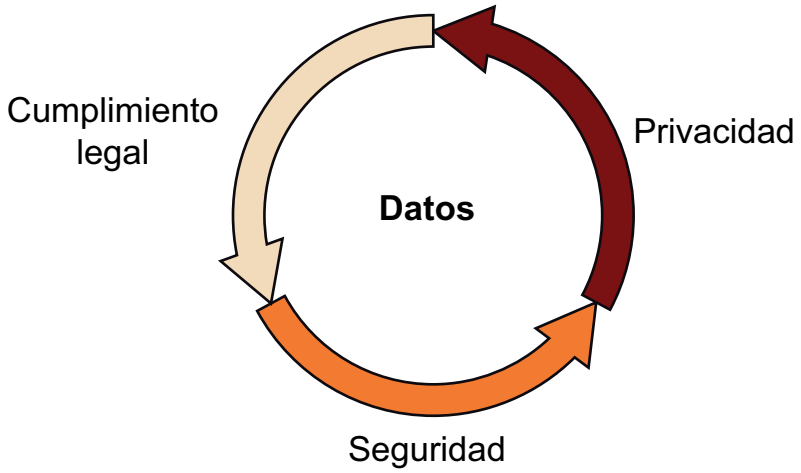
La Declaración Universal de los Derechos Humanos (DUDH) es un documento declarativo adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948, en París, y a través de 30 artículos enumera los derechos humanos considerados básicos.

El cumplimiento legal se refiere al conjunto de procesos, reglas, herramientas y sistemas utilizados por los departamentos jurídicos corporativos para adoptar, implementar y monitorizar un enfoque integrado de estas leyes dentro de las organizaciones.

El cumplimiento legal no es solo una obligación, sino que revierte también en el negocio y en la buena imagen de la organización.

La figura 2 muestra las relaciones entre estos tres elementos.

Figura 2. Elementos que engloban la seguridad y privacidad




Fuente: John Sotiropoulos

A lo largo de estos materiales, hablaremos de la seguridad y la privacidad del dato en su vinculación con el programa de gobierno del dato, si bien muchos de los aspectos que trataremos forman parte del ámbito de la seguridad de la información.

Se entiende por **seguridad de información** el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, y que buscan mantener la confidencialidad y la disponibilidad e integridad de datos y de la misma.

El respeto de la privacidad y seguridad de datos debe ser una consideración clave para cualquier organización, más allá del propio cumplimiento de las regulaciones existentes. Mientras que las regulaciones pueden ser la parte visible, las organizaciones deben, ante todo, considerar cómo sus acciones pueden afectar a sus relaciones con sus clientes. Esta es una cuestión de confianza y respeto, no simplemente de cumplimiento. Sin duda, hay mucho que podemos aprender aquí de lo que se ha implementado en el sector de la salud. En el entorno sanitario, más allá de obtener un diagnóstico preciso, las personas generalmente se sienten cómodas, ya que tienen confianza en sus médicos, porque entienden claramente que la información se mantendrá en confianza. De hecho, los médicos tienen un código de conducta muy conocido, el juramento hipocrático. Para las organizaciones, un acuerdo similar debe ser alcanzado con sus clientes. Tienen que ser francos y claros con respecto a

**Juramento hipocrático**

Uno de los párrafos del juramento dice: «Respetaré el secreto de quien haya confiado en mí».

qué información se está recopilando, cómo se utilizará y cómo beneficiará al cliente.

La información es uno de los activos más importantes de una organización. La defensa de este activo es una parte esencial para asegurar la continuidad y el desarrollo del negocio, por lo que las organizaciones deben adoptar una actitud proactiva, en la que se responsabilicen de lo siguiente.

**Proactiva**

Implica la toma de iniciativa en el desarrollo de acciones para generar mejoras.

- **Los datos de la organización deben de ser seguros y privados**: hoy día, los datos se consideran los activos más importantes de las organizaciones. Se debe asegurar su seguridad y privacidad.

- **Los datos personales de los clientes deben ser seguros y privados**: sin los datos, la organización no puede ponerse en contacto con el cliente, no puede referirse a transacciones anteriores, no puede entender su comportamiento. Por tanto, los datos son esenciales para ayudarnos a entender nuestro negocio pero, al mismo tiempo, se debe respetar, preservar y hacer cumplir la elección y el consentimiento del cliente a lo largo del ciclo de vida de la información, particularmente cuando se trata de decidir cómo se usa y distribuye la información personal dentro y fuera de la organización.

## 1.3. Compitiendo con datos bajo la premisa de seguridad y privacidad

Cuando una organización inicia su camino hacia convertirse en una organización orientada al dato, debe tomar decisiones importantes respecto al uso de los datos de clientes, la seguridad y la privacidad. Mientras que no hay duda de que se debe proteger el dato y se toman las medidas respectivas, la interpretación del uso a veces menoscaba la privacidad.

Vamos a considerar un par de casos. Por un lado, revisemos el enfoque de Google:

> El negocio de Google se fundamenta en los anuncios en su buscador. Una de las grandes preguntas es si estos anuncios en línea realmente empujan a la gente a comprar. Con el objetivo de responder a esta pregunta, Google ha empezado a usar todos los datos posibles a los que puede acceder como, por ejemplo, las transacciones de billones de tarjetas de crédito de sus clientes a través de sus sistemas de compra y pago, así como la información del resto de los servicios: Google, Gmail, Google+, Google Maps, Chrome, YouTube, etc.
>
> La combinación de todos estos conjuntos de datos permitirá determinar cuántas ventas han sido generadas con campañas digitales, lo que es el sueño hecho realidad para la industria*.

*** Más información en: https://goo.gl/xm7Xoa**

Como es posible imaginar, este comportamiento ha generado preguntas del uso de datos de cliente, respetando la privacidad, por parte de la compañía. Aunque estas dudas no son nuevas, puesto que Google usa los datos personales de sus usuarios para optimizar sus anuncios.

Un comportamiento similar es el de Facebook, que combina todos los datos posibles de cliente para optimizar sus anuncios.

Por otro lado, recordemos el enfoque de Apple:

> La gente ha confiado en nosotros con sus datos más personales. Nuestra obligación es la de conseguir las mejores medidas de seguridad que la tecnología nos ofrece. La historia nos ha enseñado que sacrificar nuestro derecho a la privacidad puede tener consecuencias.
>
> Tim Cook (CEO de Apple).

El enfoque de Apple está fundamentado en un estricto control sobre todo su ecosistema, que comprende hardware, software, aplicaciones y accesorios. Su explotación de los datos de cliente se fundamenta en la premisa de la privacidad, lo que supone, en la práctica, limitar la explotación de estos datos y usar técnicas de analítica que respetan la privacidad.

En industrias muy reguladas, como la financiera, las empresas deben seguir de forma estricta la regulación que protege los datos de cliente. Esto limita también su forma de explotación.

Por lo tanto, al abordar la privacidad y la seguridad de los datos, las organizaciones deben considerar los siguientes puntos:

- Adoptar un enfoque holístico de las necesidades de privacidad y seguridad de los datos, es decir, analizando la seguridad en su conjunto y no solo a través de las partes que los componen. Este enfoque de la planificación e implementación de la privacidad y seguridad reúne a los siguientes participantes:

  – Procesos empresariales propios que generan, recopilan y usan datos.

  – Tener roles específicos con respecto a datos confidenciales, tales como el director de privacidad y el departamento de TI.

- Aumentar los enfoques que se centran en el mero cumplimiento de la ley, haciendo respetar la privacidad de los datos y las medidas de seguridad basadas en principios generalmente aceptados. Las mejores prácticas del sector y las medidas de autorregulación que van más allá del simple cumplimiento de los reglamentos y normas.

- Aumentar los paradigmas prevalecientes de privacidad y seguridad de TI (que abordan las amenazas, al restringir el acceso a los datos y evitar que se escape de límites bien definidos mediante la evaluación de amenazas a datos en diferentes etapas del ciclo de vida de la información). Este enfoque ayuda a las organizaciones a identificar técnicas y no técnicas que pueden reducir los riesgos de seguridad y privacidad a niveles aceptables.

# 2. Privacidad y normativa de datos

## 2.1. Privacidad de datos

Como hemos comentado, las leyes de seguridad sobre los datos se perciben como un factor importante entre los usuarios y las organizaciones. Sin embargo, la privacidad se ha convertido en el más olvidado de todos los principios de seguridad de datos. Por ejemplo, una organización puede tener en forma segura los datos de sus clientes, pero a través del análisis y uso de esta información en su propio beneficio o el de terceros puede estar perjudicando a sus clientes, al vulnerar su privacidad (incluso por desconocimiento).

**Lectura complementaria**

**Bambaeur, D. E.** (2013). «Privacy Versus Security». *Journal of Criminal Law and Criminology* (núm. 3, vol. 10, págs. 667-684).

Aunque la seguridad es un elemento esencial de la privacidad, no es suficiente para asegurarla. La privacidad y la protección de datos abarcan un conjunto mucho más amplio de protecciones. Para poder entender la relación entre las dos, vamos a definir seguridad y privacidad. Ya sabemos que la seguridad consiste en habilitar y proteger las actividades y activos tanto de las personas como de las organizaciones, mientras que:

Se entiende por **privacidad** el respeto y protección de la información personal.

De este modo, la privacidad establece el marco normativo que permite decidir quién tiene la capacidad de acceder a información de forma legítima y alterarla. La seguridad implementa estas opciones a través de mecanismos tecnológicos.

Aunque la privacidad requiere que la información personal e identificable sobre las personas esté protegida contra el acceso no autorizado, es importante entender que la privacidad implica mucho más que garantizar el acceso seguro a los datos. En una palabra, la privacidad tiene que ver con el control de sus propios datos, y debe permitir a los individuos mantener el control personal sobre su información con respecto a su recolección, uso y divulgación. El significado de este concepto de privacidad quizá se expresa mejor como autodeterminación de la información.

**Autodeterminación de la información**

Es la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente, pero no exclusivamente, los almacenados en medios informáticos.

## 2.2. Privacidad por diseño

Si la privacidad es tan importante en el contexto de la seguridad, ¿qué pueden hacer las organizaciones para tenerla siempre presente? Pueden aplicar un marco de diseño de sistemas de información que la incluye por defecto.

Se entiende por **privacidad por diseño** el marco basado en la integración proactiva de la privacidad en el diseño y operación de sistemas de TI, infraestructura en red y prácticas empresariales.

En esencia, la privacidad por diseño está destinada a reflejar un enfoque holístico de la privacidad, en un ámbito organizativo, y es un proceso que involucra distintos componentes tecnológicos y organizativos, que implementan principios de privacidad y protección de datos. Estos principios y requisitos se derivan a menudo de la normativa en la que opera la organización. Como cualquier proceso, la privacidad por diseño debe tener objetivos bien definidos, metodologías y medios de evaluación.

**Lectura complementaria**

**Danezis, G.; Domingo-Ferrer, J.; Hansen, M.; Hoepman, J. H.; Le Métayer, D.; Tirtea, R.; Schiffner, S.** (2014). *Privacy and Data Protection by Design from policy to engineering*. Enisa.

Para poner en práctica este enfoque, es esencial la elaboración de un **análisis de impacto en la privacidad** (PIA, acrónimo de *privacy impact assessment*), que no es más que el ejercicio de análisis de riesgos con el que se intenta identificar todos los posibles riesgos para la privacidad que puede implicar un nuevo proceso, y a los que habrá que poner remedio. Como consecuencia, el diseño incorpora, desde su propia concepción, controles para mitigar las posibles vulnerabilidades de protección de datos y privacidad*.

*** Más información en: https://goo.gl/hhyL09**

Este enfoque debe ser tomado también en el momento de implementación de aplicaciones de inteligencia de negocio, analítica o *big data*.

### 2.2.1. Principios de la privacidad por diseño

Los seis principios fundamentales de privacidad por diseño son los siguientes:

**1) Proactivo y no reactivo**: anticipar, identificar y prevenir eventos invasivos antes de que sucedan. Esto significa tomar medidas antes de que se produzcan.

**2) Disponer de privacidad como ajuste predeterminado**: asegurarse de que los datos personales se protejan automáticamente en todos los sistemas de TI o prácticas empresariales, sin que se requiera ninguna acción adicional por parte de ningún individuo.

**3) Integrar la privacidad en el diseño**: las medidas de privacidad no deben ser complementos, sino componentes totalmente integrados del sistema.

**4) Mantener la funcionalidad completa**: la privacidad por diseño emplea un enfoque de ganar las dos partes o *win-win* a todos los objetivos legítimos del diseño del sistema; es decir, tanto la privacidad como la seguridad son importantes, y no es necesario hacer concesiones innecesarias para lograrlos.

**5) Asegurar la seguridad de punto a punto**: la seguridad del ciclo de vida de los datos significa que todos los datos deben ser usados y almacenados de forma segura cuando sea necesario, y destruidos cuando ya no se necesiten.

**6) Mantener la visibilidad y la transparencia abierta**: asegurar a las partes interesadas que las prácticas y tecnologías empresariales operan de acuerdo con los objetivos y están sujetas a verificaciones.

### 2.2.2. Ventajas de la privacidad por diseño

La certificación de privacidad por diseño ofrece a las organizaciones que la aplican la capacidad de:

- Asegurar el cumplimiento, al adelantarse a la legislación y minimizar el riesgo de incumplimiento de la misma.
- Reducir la probabilidad de multas y sanciones, incluidas las pérdidas financieras y/o la responsabilidad asociada con violaciones a la privacidad.
- Construir una marca con una mayor confianza de los consumidores, ganando así una ventaja competitiva sostenible.
- Gestionar mejor los incidentes posteriores a la infracción, para recuperar la confianza del consumidor.
- Mantener las mejores prácticas mediante la búsqueda de pruebas independientes de los controles de privacidad y seguridad, en lugar de más autoinformes o pruebas.

### 2.2.3. Barreras de la privacidad por diseño

Las organizaciones suelen justificar la no implantación de la privacidad por diseño, y argumentan alguna o varias de las siguientes justificaciones:

- Dificultades por parte de la dirección de las organizaciones para percibir los riesgos y los beneficios de la protección de datos. La inversión necesaria no se percibe como justificada.
- Por motivos similares, las empresas proveedoras de soluciones de software no encuentran en la inclusión de funcionalidad orientada a preservar la

privacidad una ventaja competitiva, por lo que el software comercializado adolece de este tipo de funcionalidad.

- La seguridad de la información (y aún más, la protección de datos) no está incluida todavía de manera generalizada como elemento integrante e importante en el ciclo de desarrollo de software usado por las organizaciones.

- Las organizaciones suelen tener dudas sobre cómo implementar soluciones tangibles para dar respuesta a los requisitos de control de la normativa de protección de datos. A esta situación contribuye la ausencia de estándares prácticos en un ámbito internacional, y que orienten a las organizaciones en la implementación efectiva de controles.

## 2.3. Normativas de datos

El conocimiento y la seguridad legal son necesarios para un uso responsable de los datos. El conocimiento de los usuarios sobre la normativa de protección de datos es cada vez mayor y, por este motivo, son cada vez más exigentes. Las exigencias de los derechos de los consumidores y la protección de datos personales son elementos clave. La tendencia en el número de leyes de privacidad de datos ha ido en aumento en los últimos años. De hecho, se ha pasado de 7 en los años setenta a 210 en el 2016, y esta tendencia va a seguir en los próximos años*.

**Normativa**

Una normativa es la agrupación de todas aquellas normas que son o pueden ser aplicables en una materia específica.

*** Más información en: https://goo.gl/qjfe5u**

El espíritu de toda norma debe ser un procesamiento justo, lícito y transparente. En el caso que nos ocupa, orientado al dato.

### 2.3.1. Normativas

Los diferentes estados y zonas a los que pertenecen suelen tener distintos enfoques en materia de protección de datos. En este material, vamos a centrarnos principalmente en comparar normativas que aplican a Estados Unidos, Europa y España, si bien es necesario comentar que sería necesario contextualizar los aspectos que se van a tratar, en función del país del lector. En Europa, la protección de datos es declarada como un derecho humano y regulada por la legislación de protección de datos. En cambio, en Estados Unidos, la actitud hacia la protección de datos se rige principalmente por las fuerzas del mercado.

Estas diferencias inciden profundamente en lo que se entiende por **privacidad** en cada país desde un punto vista normativo. Por poner algunos ejemplos:

- EE. UU. no dispone de ningún tipo de ley semejante a la LOPD (Ley orgánica de protección de datos) española, ni a la directiva europea que unifica normativas en los estados miembro.

- En EE. UU., las sanciones por las diferentes infracciones contra la protección de datos se deciden caso por caso. En Europa, sin embargo, ya están estipuladas de antemano y cuando se cometen, se aplica la multa pertinente, dependiendo del grado de la infracción.

- En EE. UU., las leyes de protección de datos protegen solo a los ciudadanos americanos. En cambio, en Europa se protege a todo aquel que esté dentro de la UE.

A estas diferencias, se suma el hecho de que el antiguo convenio de colaboración entre EE. UU. y Europa, llamado *safe harbor*, fue declarado inválido en octubre del 2015, a raíz de la denuncia de un ciudadano austriaco que pidió a las autoridades irlandesas que suspendieran la transferencia de sus datos personales a EE. UU. por parte de Facebook. Este acuerdo comprometía a las empresas y entidades de EE. UU. adheridas a respetar los principios de la protección de datos y adoptar las medidas de seguridad oportunas.

Aunque existan leyes para la protección de la privacidad, frecuentemente los gobiernos las modifican por situaciones de excepción. Por ejemplo, el STASI, el servicio oficial de seguridad del Estado de la República Democrática Alemana o RDA (informalmente conocida como Alemania Oriental), empleó a 500.000 informantes secretos. La tarea de 10.000 de estos informantes era escuchar y transcribir las llamadas telefónicas de los ciudadanos. Con la adopción de la Ley patriota de Estados Unidos, en respuesta a los sucesos ocurridos el 11 de septiembre del 2001, Estados Unidos redujo considerablemente las restricciones en la recopilación de datos personales por parte de los organismos encargados de hacer cumplir la ley.

En Estados Unidos, la legislación sobre privacidad ha adoptado un enfoque más sectorial. Diferentes leyes regulan cómo las organizaciones recogen, usan y protegen la confidencialidad de la información personal identificable (PII) en diferentes sectores. Algunos ejemplos incluyen la Ley de portabilidad y responsabilidad de seguros de salud (HIPAA), la Ley de transacción de crédito justa y precisa (FACTA) y la Ley de protección de la privacidad de niños en línea (COPPA). Las preocupaciones sobre las brechas de datos que podrían conducir a un aumento en el robo de identidad han llevado a la mayoría de los estados a promulgar leyes de notificación de violación de datos. La legislación federal sobre este asunto está siendo considerada en el Congreso de Estados Unidos. Impulsados por las mismas preocupaciones, estados como Massachusetts y Nevada también han promulgado leyes que requieren la adopción de tecnologías de cifrado para proteger la información personal sensible de los residentes del Estado, en diferentes escenarios.

Esta preocupación es universal. Muchas otras naciones también han promulgado una legislación integral sobre privacidad. Algunos ejemplos son la Ley de privacidad de Australia, la Ley de protección de datos personales de Argentina y la Ley de protección de datos personales (PIPEDA) de Canadá.

Teniendo en cuenta este panorama fragmentado por países y sectores, algunas instituciones han decidido crear recopilaciones de mejores prácticas para evitar riesgos. La Cloud Security Alliance (CSA) ha elaborado las 100 mejores prácticas para optimizar la seguridad y la privacidad dentro del *big data*.

**Lectura complementaria**

**VV. AA.** (2016). *Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy*. Cloud Security Alliance.

### 2.3.2. Normativa europea

El 25 de enero del 2012, la Comisión Europea (CE) anunció que trataría de unificar la ley de protección de datos en la Unión Europea a través de una propuesta de ley denominada Reglamento General de Protección de Datos (GDPR, acrónimo de *General Data Protection Regulation*). Estas nuevas normas de la UE sobre protección de datos refuerzan los derechos de las personas sobre sus datos personales e imponen multas para las organizaciones que no protegen sus datos. Los objetivos de la CE con esta nueva legislación incluyen:

**GDPR definición**

Por el reglamento (UE) 2016/679/CE *General Data Protection Regulation* (GDPR), el Parlamento Europeo, el Consejo Europeo y la Comisión Europea refuerzan y unifican la protección de datos para los individuos dentro de la Unión Europea (UE).

- La armonización de 27 reglamentos nacionales de protección de datos en una única reglamentación.
- La mejora de las normas de transferencia de datos empresariales fuera de la Unión Europea.
- La mejora del control del usuario sobre los datos de identificación personal.

El hecho de que se trate de un reglamento en lugar de una directiva significa que será directamente aplicable a todos los estados miembros de la UE, sin necesidad de legislación nacional de aplicación.

De manera previa a la GDPR, los países miembros de la Unión Europea están obligados a promulgar leyes que cumplan con la Directiva 95/46/CE, relativa a la protección de datos (DPD). Las directrices de la directiva se consideran una base para las leyes nacionales, y los órganos legislativos locales de los países miembros pueden incluir disposiciones que van más allá*.

*** Para saber más: https://goo.gl/h9HMpO**

En comparación con la Directiva 95/46/CE, el GDPR pretende ampliar el alcance de la legislación comunitaria en materia de protección de datos. Los principios de protección de datos son ampliamente similares a los principios establecidos en la Directiva 95/46/CE: equidad, legalidad, transparencia, limitación del propósito, minimización de datos, calidad de los datos, seguridad, integridad y confidencialidad*.

*** https://goo.gl/LhXeGS**

Con respecto al concepto de datos personales, en la Directiva se define como cualquier información relativa a una persona física identificada o identificable. En virtud del GDPR, una violación de datos personales es cualquier destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a los datos personales transmitidos, almacenados o procesados para otro uso. Esta amplia definición difiere de la mayoría de las leyes estatales de violación de datos estatales; por ejemplo, solo después de la exposición de información que puede conducir a fraude o robo de identidad, como la información financiera de la cuenta. Cuando los datos pierden su condición de personales y dejan de estar vinculados a un titular concreto, quedan fuera del ámbito de aplicación de la normativa de protección de datos.*

*** Más información en: https://goo.gl/8SBICW**

En definitiva, la GDPR busca proteger los datos personales y la forma en la que las organizaciones los procesan, almacenan y, finalmente, destruyen cuando esos datos ya no son requeridos. La ley provee control individual acerca de cómo las compañías pueden usar la información que está directa y personalmente relacionada con los individuos, y otorga ocho derechos específicos. Además, establece normas muy estrictas que rigen lo que sucede si se viola el acceso a datos personales, así como las consecuencias.

Esta ley tiene un impacto considerable en los sistemas de información y de análisis de las empresas. La existencia de un programa de gobierno del dato y la función vinculada a la seguridad del dato habrán ayudado a estar preparados de antemano.

### 2.3.3. Normativa española

En el Estado español, existen múltiples normas vinculadas a la seguridad del dato y la privacidad del dato que se publican en el *Boletín Oficial del Estado* (BOE). Esta lista tiene su equivalente en otros países, y va creciendo o recibiendo extensiones año tras año. Presentamos tan solo las normas generales, y sería necesario determinar las que aplican al propio sector.

Las podemos agrupar en diferentes ámbitos de aplicación:

- **Normativa relacionada con los servicios de la sociedad de la información**:

– Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI-CE) (BOE 166, de 12 de julio del 2002).

– Ley 56/2007, de 28 de diciembre, de medidas de impulso a la sociedad de la información (BOE 312, de 29 de diciembre del 2007).

– Real decreto 889/2009, de 22 de mayo, por el que se aprueba la Carta de derechos del usuario de los servicios de comunicaciones electrónicas (BOE 131, de 30 de mayo del 2009).

- **Normativa relacionada con el tratamiento de los datos de carácter personal**:

– Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) (BOE 298, de 14 de diciembre de 1999).

– Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE 17, de 19 de enero del 2008).

– Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE 251, de 19 de octubre del 2007).

- **Normativa relacionada con la propiedad intelectual**:

– Real decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de propiedad intelectual (LPI), y que regulariza, aclara y armoniza las disposiciones vigentes en la materia (BOE 97, de 22 de abril de 1996).

– RD 28/2003 de 7 de marzo, por el que se aprueba el Reglamento del registro central de la propiedad intelectual (BOE 75, de 28 de marzo del 2003).

– Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de propiedad intelectual, aprobado por el Real decreto legislativo 1/1996, de 12 de abril (LPI) (BOE 162, de 8 de julio del 2006).

- **Normativa relacionada con la Administración electrónica**:

– Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP) (BOE 150, de 23 de junio del 2007).

– Real decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica (ENS) (BOE 25, de 29 de enero del 2010).

– Real decreto 4/2010, de 8 de enero, por el que se regula el esquema nacional de interoperabilidad en el ámbito de la Administración electrónica (ENI) (BOE 25, de 29 de enero del 2010).

– Real decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE 278, de 18 de noviembre del 2009).

– Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común (BOE 285, de 27 de noviembre de 1992).

– Real decreto 209/2003, de 21 febrero, que regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos (BOE 51, de 28 de febrero del 2003).

– Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (BOE 276, de 17 de noviembre del 2007).

– Orden PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración general del Estado u organismos públicos vinculados o dependientes de aquella, y sobre la presentación ante la Administración general del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares (BOE 247, de 15 de octubre del 2007).

• **Normativa relacionada con la firma electrónica**:

– Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE 304, de 20 de diciembre del 2003).

– Orden de 21 de febrero del 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación de determinados productos de firma electrónica (BOE 45, de 22 de febrero del 2000).

– Real decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento que regula las obligaciones de facturación (BOE 286, de 29 de noviembre del 2003).

– Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el RD 1496/2003 (BOE de 14 de abril del 2007).

– Resolución de 24 de octubre del 2007, de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril (BOE 262, de 1 de noviembre del 2007).

– Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica (BOE 307, de 24 de diciembre del 2005).

– Real decreto 1586/2009, de 16 de octubre, por el que se modifica el Real decreto 1553/2005, de 23 de diciembre, que regula la expedición del Docu-

mento Nacional de Identidad y sus certificados de firma electrónica (BOE 265, de 3 de noviembre del 2009).

- **Otras normas de interés**

– Ley 2/2011, de 4 de marzo, de economía sostenible (BOE 55, de 5 de marzo del 2011) que modifica en parte la LAESCP, la LSSI-CE y la LPI.

– Ley 32/2003, de 3 de noviembre, general de telecomunicaciones (BOE 264, de 4 de noviembre del 2003).

– Orden ITC/1542/2005, de 19 de mayo, que aprueba el Plan nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («es») (BOE 129, de 31 de mayo del 2005).

– Real decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (BOE 102, de 29 de abril del 2005).

– Real decreto legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias (BOE 287, de 30 de noviembre del 2007).

– Real decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación (BOE 313, de 31 de diciembre de 1999).

– Real decreto 225/2006, de 24 de febrero, por el que se regulan determinados aspectos de las ventas a distancia y la inscripción en el registro de empresas de ventas a distancia (BOE 72, de 25 de marzo del 2006).

### 2.3.4. Más allá de las normativas de datos

En este apartado, nos hemos centrado en la seguridad y privacidad del dato. Sin embargo, el dato es solo uno de los componentes de la transformación en una organización orientada al dato. Debemos recordar que el otro elemento relevante es el algoritmo.

Estos se están usando el sector privado y público, y proporcionan mejoras desde la educación, el rendimiento empresarial o incluso combatir el crimen. Sin embargo, los propios algoritmos pueden llevar a escenarios en los que se deteriore u omita la privacidad. Estamos hablando de posibilidades de ampli-

ficar la discriminación estructural, producir errores para denegar servicios a individuos o incluso modificar el comportamiento de individuos.

Aunque no existen todavía normativas en este aspecto, entre la comunidad están empezando a aparecer las primeras voces para que, en la aplicación de estos algoritmos (como *machine learning*), se tengan en cuenta principios éticos o lo que podríamos llamar un *gobierno de algoritmos*:

- **Responsabilidad**: para cada sistema de algoritmos, debe existir una persona con la autoridad de gestionar con efectos adversos a la sociedad o a individuos particulares, de forma rápida y eficiente.

- **Explicación**: los efectos de un sistema de algoritmos deben poder ser explicados a las personas afectadas por dichas decisiones. Estas explicaciones deben ser accesibles y, sobre todo, comprensibles para todo tipo de público.

- **Exactitud**: los algoritmos pueden cometer errores, ya sea por la falta de calidad del dato o por el modelo elegido. Estas fuentes de errores deben ser identificadas, registradas y comparadas, lo que permitirá mitigar sus efectos.

- **Auditoría**: los sistemas de algoritmos deben ser diseñados de forma que puedan ser auditados por terceros para validar el comportamiento del algoritmo. En este sentido, estamos hablando de una auditoría privada, similar a las proporcionadas en las auditorías financieras.

- **Equidad**: los algoritmos son susceptibles de contener sesgos de sus programadores o incluso por el propio objetivo del mismo. Es necesario determinar si el algoritmo produce efectos discriminatorios.

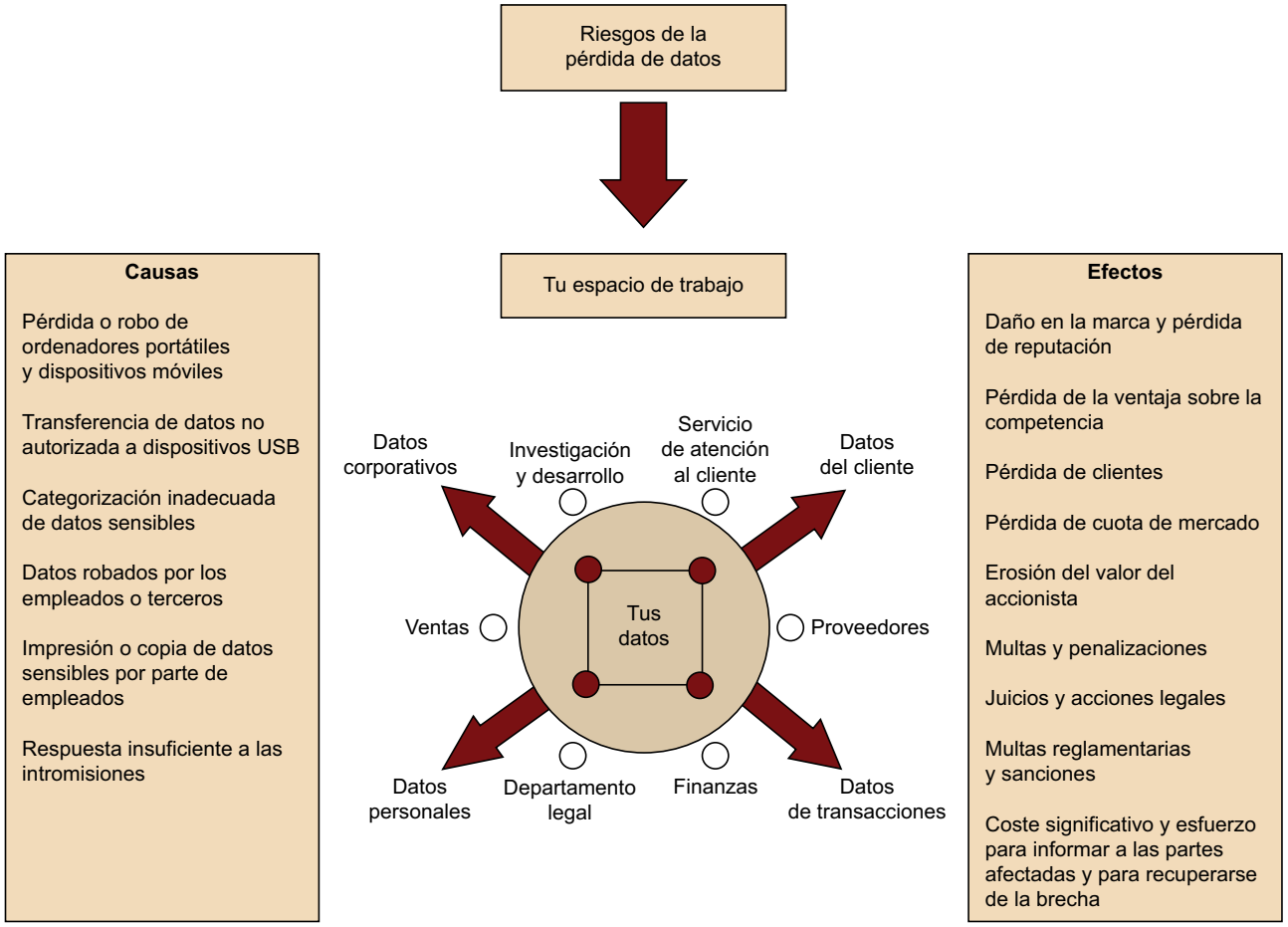
# 3. Programa de seguridad de datos

En un mundo hiperconectado, las organizaciones necesitan estar preparadas para las implicaciones que tienen sobre sus datos. McKinsey, en conjunto con el Foro Económico Mundial, estimó que los fallos de seguridad en las organizaciones podrían tener un impacto en la tecnología y la innovación empresarial de 3 billones de dólares en el 2020*.

*** Más información en: https://goo.gl/w5wUQB**

Existen múltiples riesgos de seguridad, tal y como ilustra la figura 3.

Figura 3. Riesgos de seguridad dentro de una organización




Fuente: Ernst and Young

Las organizaciones deben pensar que las brechas de seguridad afectan a todo tipo de datos, como los que se incluyen en la tabla 1.

Tabla 1. Tipologías de datos

| Corporativos | Transaccionales | Clientes | Personales |
|---|---|---|---|
| Precios/Costes | Pagos bancarios | Listado clientes | Nombre y apellidos |
| Clientes | Operaciones B2B | Hábitos de compras | Fecha de nacimiento |
| Nuevos diseños | Datos vendedores | Detalles de contacto | DNI, pasaporte |
| Patentes | Volúmenes de ventas | Preferencias | Datos genéticos |
| Análisis financieros | Ratios de descuentos | Perfil del cliente | Carné de conducir, matrícula coche |
| Documentos legales | Poder de compras | Histórico | Datos demográficos |
| Evaluaciones de empleados | Potencial de ingresos | Saldo de cuentas | Preferencias |

Es tan importante explotar los datos como asegurarlos. Según Scott Koegler, de Big Data Forum, obtener **datos protegidos pero procesables** es clave para desarrollar prácticas empresariales avanzadas mientras se protege la identidad del cliente. Esto nos lleva a considerar la implementación de un programa de seguridad de datos fundamentado en buenas praxis.

**Buenas praxis**

Por buenas o mejores prácticas se entiende un conjunto coherente de acciones que han rendido un buen o incluso excelente servicio en un determinado contexto, y que se espera que, en contextos similares, rindan similares resultados.

Se entiende por **programa de seguridad de datos** la metodología estratégica y sistemática para asegurar los datos dentro de una organización.

En definitiva, el programa persigue analizar y proporcionar una guía para mejorar la seguridad y privacidad de los datos. Instituir un programa de seguridad y privacidad de los datos dentro de una organización significa algo más que la adquisición de herramientas de seguridad y privacidad de los datos o la creación de unos roles o una colección de procesos relacionados con la seguridad y privacidad de los datos.

Es necesaria la elaboración de un programa donde se determine el modo de actuar, se definan objetivos y se designe a los responsables de cada iniciativa y acciones que hay que tomar. Y todo ello de una manera orquestada, en la que se conozca desde qué punto se parte en un ámbito de seguridad y privacidad, y hasta qué punto se desea llegar, así como los costes y los beneficios de esta transición.

### 3.1. Principios del programa de seguridad de datos

Los siguientes cuatro principios están diseñados para ayudar a las organizaciones a seleccionar las actividades que protegerán sus datos confidenciales.

- **Principio 1**: las políticas deben asegurar a lo largo de la vida de los datos su confidencialidad. Esto incluye el compromiso de procesar todos los datos de acuerdo con las leyes y regulaciones aplicables, preservar la privacidad, respetar la elección y el consentimiento del cliente y permitir a los individuos revisar y corregir su información, si es necesario.

- **Principio 2**: minimizar el riesgo de acceso no autorizado o uso indebido de datos confidenciales. El sistema de gestión de la información debe proporcionar acciones administrativas, técnicas y físicas razonables para garantizar la confidencialidad, integridad y disponibilidad de los datos.

- **Principio 3**: minimizar el impacto de la pérdida de datos confidenciales. Los sistemas de protección de la información deben proporcionar salvaguardas. Hay que establecer también planes adecuados de respuesta a la violación de datos, y todos los empleados que puedan estar involucrados en la respuesta a la brecha deben estar capacitados para aplicar las medidas oportunas.

- **Principio 4**: documentar los controles creados y demostrar su efectividad. Para que la organización ayude a garantizar los principios de privacidad y confidencialidad de datos, estos deben ser verificados a través de la monitorización, auditoría y uso de controles apropiados. Además, la organización ha de tener un proceso para reportar el incumplimiento y una hoja de ruta de las acciones claramente definida.

### 3.2. Personas, procesos y tecnología

Los tres elementos de cualquier programa de seguridad de datos son las personas, los procesos y la tecnología. Veámoslos:

- **Personas**: los procesos y las herramientas de gestión de datos son tan efectivos como las personas que los utilizan y los gestionan. Un primer paso importante es establecer un equipo de individuos de la organización, y dotarles de roles claramente definidos y responsabilidades, así como recursos adecuados para desempeñar sus funciones requeridas y orientación sobre los objetivos generales de la seguridad de los datos. Esencialmente, se trata de una organización cuyos miembros son colectivamente responsables de definir principios, políticas y procedimientos que rigen los aspectos clave de la clasificación, protección, uso y gestión de datos. Estos individuos desarrollan los perfiles de control de acceso de la organización, determinan qué constituye un uso de datos compatible con las políticas, notificación de infracciones de datos y rutas de escalamiento y supervisan otras áreas de gestión de datos relacionadas con la seguridad.

- **Procesos**: con las personas adecuadas involucradas, la organización puede centrarse en definir los procesos involucrados en la seguridad y privacidad de los datos. Esto comienza con el examen de varios documentos de autoridad (estatutos, reglamentos, normas en un ámbito de organización y estatales, políticas de la empresa y documentos estratégicos) que especifican los requisitos que se deben cumplir. Por último, la organización debe identificar amenazas contra la seguridad de los datos, la privacidad y el

cumplimiento en el contexto de flujos de datos específicos. Y determinar las acciones de control apropiadas.

- **Tecnología**: el siguiente paso es aplicar las herramientas para analizar los flujos de datos, e identificar los riesgos y aplicar las medidas necesarias de seguridad y privacidad.

Un programa consiste en un ciclo iterativo de evaluación, planificación, ejecución, gestión y revisión para la seguridad y privacidad de los datos. Esto requiere procesos repetibles que unan a las personas con una formación y que dispongan de las habilidades adecuadas con los instrumentos adecuados para pasar de la teoría a la práctica.

En el contexto de la seguridad, los usuarios son el eslabón «más débil» de la seguridad en una organización, ya que se trata de la primera línea de defensa ante los ataques a la seguridad cibernética. Javier Perea, director regional de Intel Security en España, comenta al respecto, en este informe:

**Lectura complementaria**

**Raj, R.; McFarland, C.** (2016). *Hacking the Human OS*. Intel Security

> Las últimas técnicas de ingeniería social puestas en marcha por los cibercriminales son cada vez más sofisticadas y difíciles de detectar y solucionar. Estas nuevas técnicas tienen en el punto de mira a los trabajadores de las organizaciones como objeto del ataque. Este informe destaca la importancia de concienciar y educar al usuario/trabajadores, para que asuman la seguridad de los datos como un hecho cultural. Por ejemplo, hoy día cualquier trabajador puede disponer de un *pendrive* de varios gigas en el que almacene información tanto de la organización como de sus clientes. Por mucha seguridad y privacidad que impulse la organización, si un trabajador utiliza la información de la organización fuera del entorno, seguro que provoca que toda esta seguridad sea en vano.

Casos como el ataque de ransomware fundamentado en WannaCry, en el 2017, ponen de manifiesto la necesidad de mejorar la educación y la formación en seguridad en las organizaciones, para reducir los casos fundamentados en la ingeniería social. Para ello, necesitamos roles liderando estas iniciativas.

Tradicionalmente, el C(I)SO, acrónimo de *chief (information) security office*, ha sido responsable de la seguridad en las organizaciones. A medida que van incrementándose las normativas vinculadas al dato, se han ampliado las competencias de este rol o ha emergido un nuevo rol denominado DPO, acrónimo de *data protection officer*. Las tareas principales del DPO son:

- Educar a la empresa y a sus empleados sobre los requisitos de cumplimiento importantes de seguridad de datos.
- Capacitación del personal involucrado en el procesamiento de datos.
- Llevar a cabo auditorías para asegurar el cumplimiento y abordar las posibles cuestiones de manera proactiva.
- Servir de punto de contacto entre la organización y las leyes e instituciones que regulan la seguridad.

- Supervisar el desempeño y asesoramiento sobre el impacto de los esfuerzos de la protección de datos.

- Mantener los registros de todas las actividades de procesamiento de datos efectuadas por la organización, incluyendo el propósito de todas las actividades de procesamiento.

- Interactuar con los clientes para informarles de cómo se están utilizando sus datos, sus derechos de borrar sus datos personales y las medidas que la organización ha puesto en marcha para proteger su información personal.

Evidentemente, aparte del DPO, el resto de los miembros de la organización también son responsables de la seguridad y privacidad de los datos.

### 3.3. Seguridad de datos en contexto de gobierno del dato

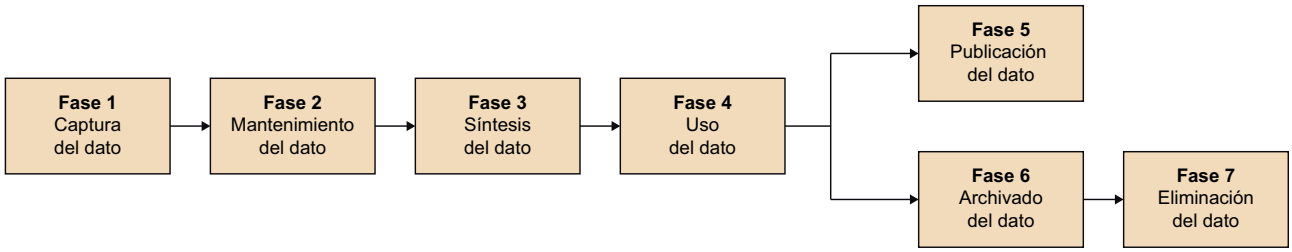
En el contexto de gobierno del dato, la seguridad y privacidad de datos es una función más que hay que hacer. Como ya sabemos, cada función tiene distintas actividades (planificación, control, de desarrollo y operativas), cada una de las mismas efectuada por el rol correspondiente.

Para la gestión de la seguridad de datos, estas actividades son:

- Comprensión de las necesidades de privacidad, confidencialidad y seguridad de datos (actividad de planificación).
- Definición de las políticas y estándares de privacidad y confidencialidad (actividad de planificación).
- Definición de los estándares y procedimientos de contraseñas (actividad de planificación).
- Diseño e implementación de los controles de seguridad de datos (actividad de desarrollo).
- Gestión de usuario, contraseñas y grupos de usuarios (actividad de control).
- Gestión de vistas de acceso de datos (actividad de control).
- Gestión de permisos de acceso de datos (actividad de control).
- Monitorización de la autentificación y del comportamiento de usuarios (actividad de control).
- Clasificación de la confidencialidad de la información (actividad de control).
- Auditoría de la seguridad de datos (actividad de control).

El programa de la seguridad de datos cubre estas funciones, que forman parte del marco más general a lo largo del ciclo de vida del dato que se ilustra en la figura 4.

Figura 4. Ciclo de vida del dato




Fuente: Marcos Pérez González

De forma que:

- En la **fase 1**, la organización debe asegurar que la captura del dato respeta la privacidad y la regulación propias del país donde opera la organización, y alineadas con las necesidades de la organización.

- En la **fase 2** y **3**, la organización se debe asegurar de que el mantenimiento y la síntesis del dato siguen las políticas y estándares de acceso, confidencialidad y privacidad. En este punto, es relevante tener en cuenta cómo el análisis del dato puede convertir datos anónimos en datos personalizados.

- En la **fase 4**, el uso del dato debe controlarse mediante las actividades de control del plan para asegurar que se trabaja en el contexto de vistas y permisos definido.

- En la **fase 5**, tenemos que asegurarnos de que el dato que se publica es correcto y, si son datos de clientes, asegurarnos de que sean anónimos.

- En la **fase 6**, se debe asegurar que los datos se encuentran seguros y que, en todo momento, sus metadatos (es decir, datos sobre los datos) muestran la relevancia de los mismos. Si algunos datos tienen caducidad, se deben archivar y, si los usuarios lo solicitan, se deben modificar.

- Finalmente, en la **fase 7**, debemos asegurarnos de que los datos son correctamente eliminados y, si en cualquier momento un usuario nos solicita la baja en nuestro sistema, de que realmente se lleva a cabo la eliminación de los datos.

### 3.4. Mejores prácticas

A continuación, listamos algunas de las mejores prácticas en el ámbito de la seguridad y privacidad del dato:

- **Priorizar los activos de información basados en los riesgos del negocio**: la mayoría de las instituciones no tienen suficiente información sobre la prioridad con la que necesitan proteger sus datos. En lugar de tratar de

asegurarlo todo, las organizaciones necesitan aplicar el enfoque 80-20 y centrarse en ese 20 por ciento de los datos que es más crítico. Una buena praxis consiste en crear una hoja de ruta de implementación sobre la seguridad que hay que aplicar a los datos, por dónde se debe comenzar, qué importancia tiene y, por tanto, qué esfuerzos debemos aplicar sobre los mismos, y construir una temporización sobre las acciones que se deben aplicar.

- **Proporcionar una protección diferenciada, basada en la importancia de los activos**: el uso de controles diferenciados (por ejemplo, cifrado, contraseñas más rigurosas, ...) permite a las instituciones concentrar tiempo y recursos en la protección de los activos de información que más importan.

- **Integrar la seguridad en el entorno tecnológico para impulsar su escalabilidad**: las herramientas de seguridad de datos necesitan ser automatizadas. Los actuales conjuntos de herramientas requieren una considerable inversión en la gestión cotidiana para llegar a ser eficaces. Las instituciones deben pasar de simplemente aplicar seguridad *ad hoc* a capacitar a todo su personal para incorporarlo desde el primer día en proyectos tecnológicos con datos seguros y privados.

- **Implementar defensas activas para descubrir ataques de forma proactiva**: hay una gran cantidad de información disponible sobre posibles ataques. Cada vez más, las empresas tendrán que desarrollar capacidades para agregar información relevante y analizar y ajustar sus sistemas de defensa en consecuencia (por ejemplo, *firewalls*).

- **Probar continuamente, con el objetivo de mejorar la respuesta a incidentes**: una respuesta inadecuada a una infracción (no solo por el equipo TI, sino también por el marketing, es decir, la parte de negocio, los asuntos públicos o las funciones de servicio al cliente) puede ser tan perjudicial como el incumplimiento propiamente dicho. Un programa no es un evento único, sino un proceso continuo que evolucionará con el tiempo. A menudo, es un cambio cultural en una organización y, por lo tanto, su implantación lleva tiempo. El programa debe ser revisado periódicamente y modificado cuando sea necesario.

- **Formar al personal de primera línea para ayudarle a entender el valor de los activos de información**: los usuarios suelen ser la mayor vulnerabilidad que tiene una institución; hacen clic en vínculos que no deberían hacer, seleccionan contraseñas inseguras y envían archivos confidenciales por correo electrónico a listas de distribución amplias. Las instituciones necesitan segmentar a los usuarios y ayudar a cada grupo a comprender los riesgos empresariales de los activos de información que tocan cada día.

- **Integrar la seguridad en los procesos de gestión de riesgos y gobernanza en toda la organización**: esto significa hablar de seguridad de TI en términos de negocio, frente a centrarse en los términos de TI que no pue-

den capturar el valor real de los datos que necesita asegurar. Además, las implicaciones de la seguridad deben integrarse en el amplio conjunto de funciones de gobierno corporativo, como la gestión de recursos humanos, la gestión de proveedores y el cumplimiento normativo.

- **Transparencia con los usuarios**: la información sobre las políticas de datos debe ser fácil de encontrar para el público (y no enterrada en el sitio web). El texto debe ser conciso y fácil de leer, sin jerga. Tiene que indicar cómo se recogen, comparten y usan los datos, quién tiene acceso a los mismos y qué salvaguardias protegen la privacidad de los estudiantes.

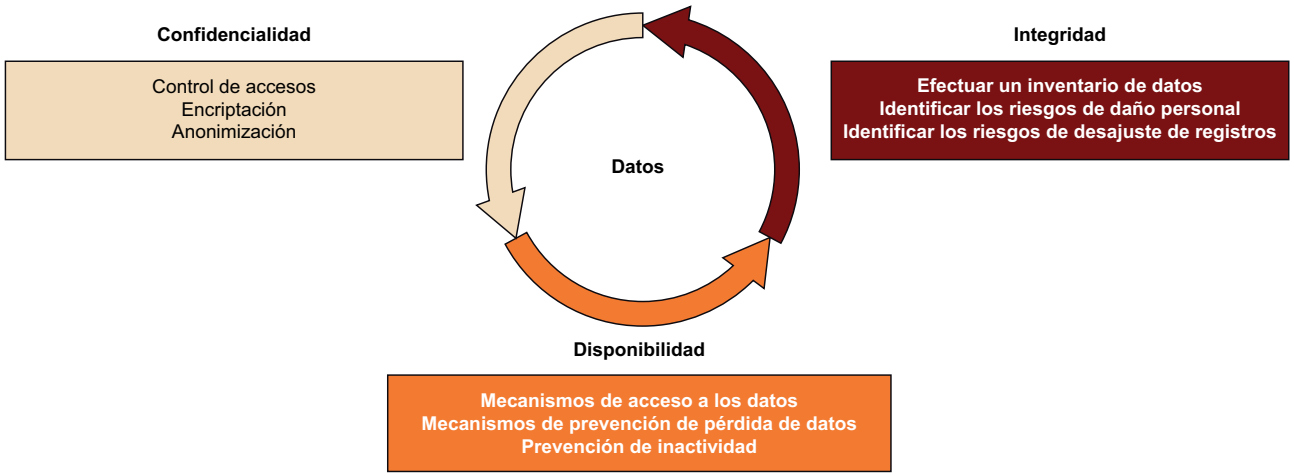
- **Transparencia con los usuarios en caso de brechas de seguridad**: la notificación oportuna de las infracciones de seguridad es importante para la confianza pública. Es improbable esperar que las brechas en los sistemas de datos terminen algún día, aunque esa es la meta. Sin embargo, los retrasos en la notificación de los usuarios sobre las infracciones los ponen en mayor riesgo, especialmente si los usuarios repiten las mismas contraseñas en varios sistemas. La notificación rápida permite a los usuarios cambiar de forma proactiva las contraseñas a través de varias aplicaciones. También les pide que consideren la monitorización de crédito o la protección contra robo de identidad si los números de seguridad social o la información tributaria están comprometidos*.

*** Más información en:** ***Privacy Rights Clearinghouse, 2016, June. Chronological Database of Data Security Breaches. Retrieved from Privacy Rights Clearinghouse website*** **https://goo.gl/28S4BA**

## 3.5. Elementos clave de la seguridad y la privacidad

La seguridad de datos digitales se basa en tres propiedades, a menudo identificadas con el acrónimo CIA *confidentiality*, *integrity*, *availability*. La figura 5 muestra estos tres elementos clave.

Figura 5. Elementos clave de la seguridad y la privacidad




Fuente: David Cabanillas

Solo puede satisfacerse si se respetan las propiedades antes mencionadas y se garantiza lo siguiente:

- **Confidencialidad**: se trata de una propiedad de la información que pretende garantizar el acceso solo a las personas autorizadas.

- **Integridad**: el término integridad de datos se refiere la corrección y completitud de la información de los datos. Por ejemplo, si una empresa tiene una dirección incorrecta para un cliente y envía facturas a esa dirección incorrecta, podrían retrasarse los pagos por parte del cliente, lo que podría conducir a deudas incobrables. La información personal será tan precisa, completa y actualizada como resulte necesario para los propósitos para los que se va a usar. La medida en que la información personal será exacta, completa y actualizada dependerá del uso de la información, teniendo en cuenta los intereses del individuo. Las organizaciones pueden seguir estas tres ideas:

– **Llevar a cabo un inventario de datos**: realmente, no hay manera de demostrar que la información personal que se ha recopilado es exacta y relevante para sus usos previstos, a menos que se sepa dónde está y qué proceso o quién la está utilizando.

– **Identificar los riesgos de daño personal**: ¿la organización tiene algún proceso de negocio que podría dañar a una persona si se utilizara información inexacta? Los ejemplos podrían incluir información de salud inexacta que resulte en diagnósticos erróneos o negaciones de cobertura de seguro; información de crédito imprecisa que da como resultado préstamos o trabajos negados; o información inexacta sobre el desempeño del trabajo, lo que resulta en oportunidades de empleo perdidas.

– **Identificar los riesgos de desajuste de registros**: ¿tiene la organización algún sistema en el que una persona pueda acceder a la información confidencial de otra persona a través de una autentificación o registro? Hay que concentrar la atención en los procesos de *customer relationship management* (CRM).

- **Disponibilidad**: los datos deben ser seguros y privados, pero también tienen que poder ser explotados por la organización. La disponibilidad del dato también se tiene que garantizar.

# 4. Técnicas y tecnología para la gestión de la seguridad y privacidad del dato

Hemos revisado hasta ahora los aspectos vinculados a los procesos, gobierno, políticas y estándares en el contexto de la gestión de datos maestros. En este apartado, vamos a centrarnos en las herramientas, técnicas y tecnologías que soportan la gestión de datos maestros.

## 4.1. Técnicas

Para poder respetar las preferencias de los clientes (respecto a cómo y cuándo su información personal puede ser recolectada, y potencialmente compartida con terceros) y las obligaciones de conformidad de seguridad y privacidad, estas tecnologías deben incluir las técnicas siguientes:

- **Clasificación**: capacidad de identificar dónde se encuentran los datos sensibles, tanto en los sistemas en el centro de datos de la organización como en la nube. Estamos hablando, por lo tanto, de técnicas de autodescubrimiento, catalogación y trazabilidad de datos.

- **Auditoría**: capacidad de entender a qué datos sensibles se accede y cómo se combinan, y quién está accediendo a los mismos. Por lo tanto, se usan capacidades de trazabilidad de datos.

- **Protección**: capacidad de proteger los datos sensibles en todos los ámbitos. Esta protección se lleva a cabo con técnicas de enmascaramiento (en inglés, *data masking*), anonimización y encriptación. Las técnicas de protección son uno de los puntos calientes de mercado, empujadas por las regulaciones; por ejemplo, en el área de lo que se conoce como *differencial privacy*.

- **Monitorización**: saber en tiempo real cuándo los usuarios, dispositivos o sistemas acceden a datos confidenciales.

**Enmascaramiento**

El enmascaramiento de datos garantiza el hecho de que la información original nunca estará disponible para el usuario final.

**Anonimización**

Con la palabra anonimización se reconoce el dato disociado, como aquel que no permite la identificación de un afectado o interesado.

**Encriptación**

La encriptación, o cifrado, hace que se dificulte el robo de información mientras es transmitida por algún medio, pero no impide el abuso de la misma o que sea susceptible de filtraciones, ni antes de que el cifrado se produzca ni una vez que la decodificación ha tenido lugar.

## 4.2. Tecnologías

Respecto a la seguridad TIC (acrónimo de tecnologías de la información y la comunicación), hay un amplio catalogo de servicios y herramientas que tienen diferentes ámbitos de aplicación. Estos ámbitos son la gestión de acceso

e identidad, seguridad en el puesto de trabajo, seguridad en aplicaciones y datos, seguridad en los sistemas y seguridad en red.

Aunque es cierto que todos ellos son relevantes para las organizaciones, vamos a centrarnos en aquellos que están vinculados a la seguridad y privacidad en aplicaciones y datos.

Las herramientas que cubren este ámbito son:

- **Antifraude**: herramientas de antiphishing, antispam, historial de navegación segura, etc.
- **Antimalware**: herramientas de antivirus, antispyware, etc.
- **Control de contenidos confidenciales**: son herramientas para la prevención de fuga de información (DLP, acrónimo de *data loss prevention*); gestión de ciclo de la información (ILM, acrónimo de *information lifetime management*); control de acceso de dispositivos extrapolables, etc.
- **Cumplimiento legal y normativo**: herramientas para el cumplimiento legal (por ejemplo, LOPD, LSSID, etc.) y para el cumplimiento normativo (por ejemplo, SGIS, gestión de riesgos, etc.).
- **Sistemas y herramientas criptográficas**: son herramientas para la encriptación de las comunicaciones, de los dispositivos móviles, de discos duros y soportes de almacenamiento.
- **Contingencia y continuidad**: herramientas de gestión de planes de contingencia y continuidad, de recuperación de sistemas, de copias de seguridad y de despliegue rápido de infraestructuras y virtualización.
- **Cortafuegos/VPN/IDS, IPS**: herramientas de cortafuegos en un ámbito de red, de aplicación, personales y corporativos, así como filtro de contenidos, VPN (acrónimo de *virtual private network*), IDS (acrónimo de *intrusion detection system*) e IDPS (acrónimo de *intrusion detection and prevention service*).
- **Auditoría técnica y forense**: son herramientas de auditoría de red y puertos, de sistemas y ficheros y de auditoría forense. Incluyen también tests de intrusión, borrado seguro, gestión de parches y vulnerabilidades.

Respecto a los servicios que pueden ser contratados, incluyen: cumplimiento con la legislación, gestión de incidentes (que consisten en prevención, detección y resolución), externalización de servicios de seguridad (lo que incluye seguridad gestionada, *outsourcing* y centros de respaldo), auditoría técnica (que incluye servicios de detención de intrusiones y auditoría forense, entre otros) e implementación y certificación de normativa (que incluye certificación y acreditación, planes y políticas de seguridad, análisis de riesgos).

De este modo, los enfoques tradicionales de seguridad de TI que se centran en la protección de la infraestructura mediante la protección de la red deben ser aumentados con medidas de protección, como las anteriores, que se centren de manera específica en la protección de los datos que se almacenan y se trasladan a través de esa infraestructura.

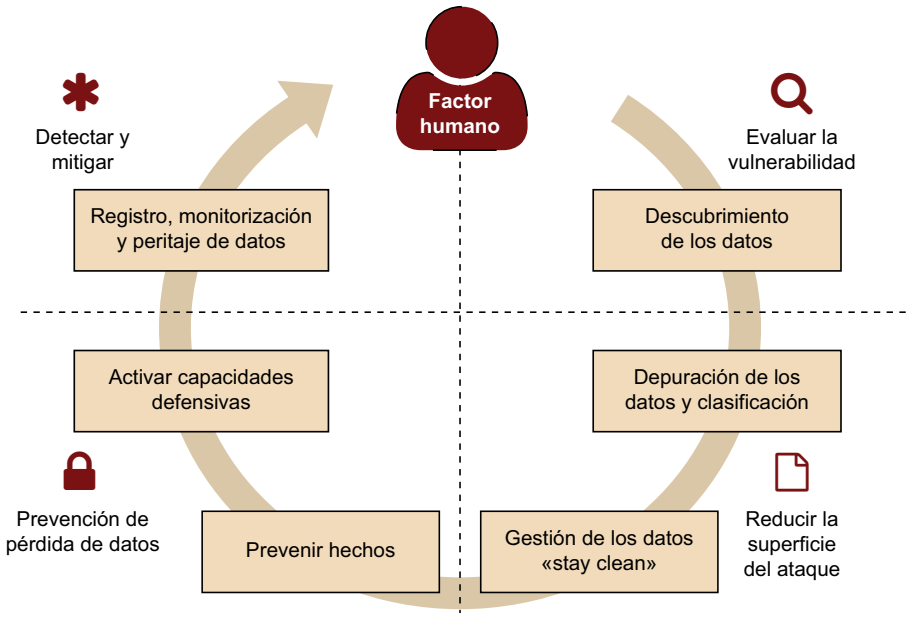
A esto también debemos añadir el hecho de que los propios sistemas de análisis (es decir, los sistemas que soportan el *data warehouse*, la inteligencia de negocio, *big data*, *business analytics*, etc.) deben incluir un componente de seguridad relacionado con las herramientas anteriores; de modo que, en lugar de definir una política para cada una de las herramientas, pueda ser posible establecer medidas en un ámbito de programa desde un componente central.

### 4.3. Marco tecnológico

Las herramientas anteriores deben trabajar de forma conjunta. La figura 6 muestra un marco o *framework* de seguridad. Este marco se compone de tres áreas:

**1)** Gestión proactiva y gobierno del dato (mitad derecha).
**2)** Prevención y monitorización activas (mitad izquierda).
**3)** Factor humano.

Figura 6. Marco que engloba la seguridad y privacidad dentro del *data governance*




Fuente: *Infinitive Insights*

En los siguientes puntos, se detallan las partes más relevantes dentro del marco que engloba la seguridad y privacidad en el *data governance*.

### 4.3.1. Clasificación / sensibilidad de los datos

Evaluar el nivel de sensibilidad de los datos de cada activo es algo que debe definirse en el contexto de las políticas gobernantes. Por ejemplo, en el ámbito del cuidado de la salud, las reglas de HIPAA determinan qué elementos de datos requieren protección, pero puede haber muchos contextos en los que se usen estos elementos de datos. Algunos requieren mayor protección que otros.

### 4.3.2. Auditoría de los datos

La auditoría y la presentación de informes son las claves para entender lo que sucede con los datos que no están bajo el control directo de la organización. Sin ellos, es difícil revertir transacciones no deseadas o fraudulentas. La auditoría también constituye la base de los regímenes de cumplimiento. Estas son las principales preocupaciones en esta área:

- **Alcance de la auditoría**: ¿qué es exactamente la auditoría en el servicio? ¿Cómo son de completas las auditorías y cuánto tiempo dura la información de auditoría? ¿Se persiste en la información del usuario para el análisis forense? ¿Se puede utilizar la información de auditoría para revertir las transacciones impropias? ¿Las auditorías se ajustan a las leyes, reglamentos, normas y prácticas de la industria?

- **Integridad de auditoría**: ¿cómo se protege la información de auditoría? ¿Quién tiene acceso administrativo a la misma? ¿Se almacena la información de auditoría de una manera segura y protegida?

- **Informes**: ¿la información de auditoría es fácilmente accesible? ¿Tiene suficiente margen para el cumplimiento y los controles de gobierno? ¿Es la información utilizable como un artefacto forense para fines legales?

### 4.3.3. Anonimización de los datos

Uno de los puntos más importantes para asegurar que los datos no puedan ser explotados por otras organizaciones es la anonimización de los datos. Si los datos personales son totalmente anónimos, ya no son datos personales. En este contexto, el anonimato significa que no es posible identificar a un individuo a partir de los propios datos o de esos datos en combinación con otros datos, teniendo en cuenta todos los medios razonablemente probables de ser utilizados para identificarlos. Sin embargo, esto no quiere decir que no sean útiles, simplemente que no se puede identificar al individuo. Un ejemplo sería que una empresa de marketing segmente a sus clientes por edades, no dispon-

ga de los identificadores de sus clientes pero sí sepa los porcentajes y tramos por edad. Esta información es útil para dirigir sus campañas de marketing.

Resulta muy ilustrativo, en este punto, el Informe 0283/2008 de la Agencia Española de Protección de Datos. En el mismo, estableció que bastará la mera posibilidad, incluso remota, de que mediante la utilización con carácter previo, coetáneo o posterior de cualquier medio (proceso informático, programa, herramienta del sistema, etc.) la información concerniente a los titulares de los datos pueda revelar la identidad de los mismos para que quede plenamente sometida a la Ley orgánica de protección de datos.

Los tres riesgos claves de la anonimización:

- **Singularización**: consiste en la posibilidad de extraer de un conjunto de datos algunos registros que identifican a una persona.

- **Vinculabilidad**: consiste en la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas.

- **Inferencia**: consiste en la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

En algunos casos, los datos utilizados para análisis de datos se anonimizan para los propósitos del análisis. Por ejemplo, la herramienta *smart steps* de Telefónica utiliza datos sobre la ubicación de teléfonos móviles en su red, con el fin de rastrear el movimiento de multitudes de personas. Esto puede ser utilizado por los minoristas para analizar cuántas personas pasan cerca de un lugar concreto. Los datos que identifican a los individuos son eliminados antes del análisis, y los datos anónimos se agregan para obtener información sobre la población en su conjunto y combinada con datos de investigación de mercado de otras fuentes*.

*** Más información en: https://luca-d3.com/**

**Más allá de la anonimización – políticas éticas**

Si bien la anonimización es un gran aliado para asegurar y otorgar privacidad a los datos, no es suficiente. El requisito de procesar datos personales de manera justa y legal tiene que ser un deber de las organizaciones que explotan los datos, lo que se considera **políticas éticas**. Se incluye dentro de estas políticas éticas, por ejemplo, la obligación de informar a las personas a qué se destinarán sus datos personales. Y se deberán cumplir, como concepto de políticas éticas.

- **Minimización de datos**: el principio de la minimización de los datos es esencialmente la idea de que, con pocas excepciones, una organización solo debe procesar los datos personales que realmente necesita procesar para lograr sus propósitos de procesamiento.

- **Exactitud**: encontramos riesgos evidentes para los datos si se procesan datos inexactos. Por lo tanto, los controladores son responsables de tomar todas las medidas razonables para garantizar que los datos personales sean exactos.

- **Periodos de retención de datos**: la idea de que los datos personales no deben conservarse durante más tiempo de lo necesario en relación con los fines para los que se recopilaron o para los que se procesan posteriormente es fundamental para garantizar un trato justo.

- **Seguridad de datos**: los controladores son responsables de asegurar que los datos personales se mantienen seguros, tanto contra amenazas externas (por ejemplo, *hackers* maliciosos) como contra amenazas internas (por ejemplo, empleados con malas intenciones).

- **Responsabilidad**: el principio de rendición de cuentas busca garantizar el cumplimiento de los principios de protección de datos.

Cualquier normativa debe ir orientada a la adquisición de las políticas éticas dentro de las organizaciones; se trata de algo parecido a un juramento hipocrático, pero dentro de las organizaciones y cómo estas usan los datos de sus clientes.

### 4.3.4. Monitorización de los datos

Monitorizar los datos se fundamenta en la definición de reglas (de manera similar a la calidad de datos) y en la revisión de patrones de comportamiento. La idea de fondo es que cada registro o grupo de registros en la tabla o tablas en cuestión se comprueban mediante una serie de pruebas, y se rastrea el número de infracciones de la regla. Esta monitorización viene acompañada de la generación de informes, así como de una revisión continua de las reglas para identificar nuevos casos más allá de los establecidos, a través de lo que se conoce como una auditoría forense.

## Resumen

En este módulo didáctico, hemos presentado el concepto de seguridad y privacidad del dato, que tiene el objetivo último de disponer de datos seguros y privados dentro de una organización.

En primer lugar, hemos mostrado los nuevos retos de seguridad a los que nos enfrentamos.

A continuación, hemos revisado en qué consiste un programa de seguridad y privacidad de datos y las mejores praxis, y lo hemos contextualizado dentro del gobierno del dato. Todo esto con foco en las personas, los procesos y los datos.

En el siguiente apartado hemos descrito el tema de la privacidad, y nos hemos centrado en la privacidad por diseño. Después, hemos descrito las diferentes leyes y normas con respecto a la seguridad y privacidad de los datos.

Por último, se han revisado las técnicas y la tecnología que forman parte de lo que se conoce actualmente como privacidad y seguridad de datos.

# Glosario

**afectado o interesado** *m* Persona física titular de los datos que sean objeto del tratamiento.

**amenaza** *f* Una amenaza informática es toda circunstancia, evento o persona con el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

**autenticación** *f* Procedimiento de comprobación de la identidad de un usuario.

***big data*** *m* Conjunto de estrategias, tecnologías y sistemas para el almacenamiento, procesamiento, análisis y visualización de conjuntos de datos complejos.

**cifrado** *m* Codificación de datos mediante distintas técnicas matemáticas que garantizan su confidencialidad en la transmisión.

**confianza** *f* Esperanza firme en que un sistema se comporte como corresponde.

**confidencialidad** *f* Requisito de seguridad que indica que el acceso a los recursos de sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.

**control de acceso** *m* Mecanismo que, en función de la identificación ya autenticada, permite acceder a datos o recursos.

**criptografía** *f* Disciplina que se ocupa de la seguridad de la transmisión y el almacenamiento de la información.

**dato de carácter personal** *m* Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión, concerniente a una persona física identificada o identificable.

**dato disociado** *m* Dato que no permite la identificación de un afectado o interesado.

**derechos de acceso** *m pl* Autorizaciones concedidas a un usuario para la utilización de los distintos recursos de un sistema, normalmente informático.

**disponibilidad** *f* Requisito de seguridad que implica que la información y los servicios del sistema continúen en funcionamiento y que los usuarios autorizados puedan acceder a los recursos cuando lo necesiten, donde lo necesiten y en la forma en que lo necesiten.

**encriptación** *f* Método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Solo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

**filtración de datos** *f* Una filtración de datos sucede cuando se compromete un sistema, y se expone la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, los cuales tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados.

**intrusión** *f* Intromisión informática en la que el atacante consigue obtener un control completo sobre la máquina. Durante una intrusión, el atacante puede obtener y alterar todos los datos de la máquina, modificar su funcionamiento e incluso atacar a nuevas máquinas.

**monitorización** *f* Despliegue de controles que aseguran que los datos siguen cumpliendo con las reglas de negocio que definen la calidad de los datos para la organización.

**persona identificable** *f* Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

**tratamiento de datos** *m* Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión; así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

**vulnerabilidad** *f* Estado viciado en un sistema informático (o conjunto de sistemas) que afecta a las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

Permitir que un atacante ejecute comandos como otro usuario. Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos. Permitir a un atacante hacerse pasar por otra entidad. Permitir a un atacante llevar a cabo una negación de servicio.

# Bibliografía

**Chio, C.; Freeman, D.** (2017). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. Londres: O'Reilly.

**Harari, Y. N.** (2017). *Homo Deus*. Londres: Harvill Secker.

**Hayden, L.** (2015). *People-Centric Security: Transforming Your Enterprise Security Culture*. Nueva York: McGraw Hill Professional.

**Jacobs, J.; Rudis, B.** (2014). *Data-Driven Security: Analysis, Visualization and Dashboards*. Nueva York: Wiley.

**O'Neil, C.** (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Londres: Penguin Books Limited.

**Payton, T.; Claypoole, T.; Schmidt, H. H. A.** (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Nueva York: Rowman & Littlefield Publishers.

**Schneier, B.** (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Nueva York: W. W. Norton & Company.