Cumplimiento y prioridades de GDPR en España

Realizado por Delfos Research con el patrocinio de Commvault

Diciembre 2017

Autores: Alberto Bellé y Fernando Maldonado.

Resumen ejecutivo

El Reglamento General de Protección de Datos (que en adelante abreviaremos como GDPR de acuerdo con sus siglas en inglés) no es simplemente una regulación sobre datos personales; se trata de un nuevo marco que fija los cimientos para el desarrollo de una verdadera economía del dato. Aunque en el corto plazo las empresas se centran en su cumplimiento, está emergiendo un cambio de mentalidad. El objetivo último ya no es el mero cumplimiento, sino dar más poder a los clientes y alcanzar una mayor trasparencia. Si bien los avances hoy se pueden producir por miedo al regulador, mañana sencillamente serán la única forma posible de permanecer en el mercado.

GDPR abre un nuevo espacio de relación con el cliente, en el que la transparencia y la agilidad de respuesta adquieren gran importancia. La percepción de marca y la experiencia de usuario se van a ver afectadas en gran medida por cómo la empresa gestione la información y materialice los derechos de sus clientes en la práctica. Se establecen además unas reglas de competencia en el mundo digital, dado que el dato tiene que ser localizable y portable (es decir, poderse transferir de forma estandarizada). Un cliente puede pedir que se le entreguen sus datos de uso y facturación de un servicio a un competidor, y la empresa no puede negarse.

Por ello, el dato personal deja de ser una materia prima y se convierte en un activo crítico para el negocio. En consecuencia, no puede haber datos personales sobre los que la empresa no tenga control. Esto apunta directamente a la existencia de repositorios de datos corporativos, bien dentro del data center o en los dispositivos de usuario, sobre los que no haya visibilidad. En particular, son los datos no estructurados los que presentan un grado de control menor por parte de las organizaciones. La nueva regulación eleva el requerimiento de visibilidad y control sobre estos datos al mismo nivel que la empresa debe tener con cualquier otro activo crítico, incluyendo su monitorización, así como la creación de informes y auditorías sobre los mismos.

Para que los derechos del ciudadano recogidos en GDPR se hagan realidad (tales como la privacidad y control, la gestión de accesos, el borrado o la ya mencionada portabilidad), es necesario que se vinculen con la gestión de los datos corporativos. La capacidad de respuesta en los términos que establece la regulación requiere tener en marcha los mecanismos para buscar, encontrar, eliminar, retener o tratar aquellos datos en los que GDPR sea aplicable.

Finalmente, se debe recalcar que el proceso de cumplimiento de GDPR es un continuo, nunca puede darse por terminado. No existe un certificado de cumplimiento de GDPR, ni unas condiciones fijas. El reglamento deja en manos de cada empresa las decisiones que consideren más adecuadas. Por ello, en este contexto de transformación digital, las organizaciones van a necesitar capacidades de gestión de los datos que les permitan maniobrar en esta dinámica de cambio acelerado, y responder tanto al cliente como al regulador.

Índice

1. GDPR, los cimientos de una nueva economía del dato

La nueva regulación europea sobre la protección de datos personales llega en un contexto de transformación digital, en el que el dato se está convirtiendo en el principal activo para los negocios. El regulador ha tenido que encontrar un equilibrio entre dos fuerzas. Por un lado, la necesidad por parte de las empresas y organismos públicos de explotar datos personales para ofrecer nuevos servicios o simplemente mantenerse competitivas; por otro, el derecho a la privacidad de las personas. Además, lo ha tenido que hacer en un contexto de cambio tecnológico profundo.

Esta regulación, que entra en vigor en mayo de 2018, establece un nuevo marco de responsabilidad para las empresas que tienen o utilizan datos personales. La propiedad de los mismos queda en la práctica en manos de las personas, mientras que las empresas tienen el rol de usuario bajo permiso. Es más, estas estarán obligadas a un ejercicio de trasparencia tanto hacia el cliente como hacia el regulador; deberán detallar cuál es la situación de los datos y para qué los están utilizando.

Por tanto, el principal mensaje que nos llega de esta regulación es que los datos personales ya no se pueden gestionar sin una estrategia definida sobre su uso y protección. Todas las empresas tienen que tener y hacer explícita la suya.

Esto exige un cambio de mentalidad. Por ejemplo, la regulación es deliberadamente imprecisa en torno a las medidas de seguridad necesarias para garantizar la protección y privacidad de los datos personales: no provee de un listado de requisitos a cumplir. El regulador se rinde a la evidencia de que el cambio tecnológico se produce tan rápido que deja en manos de las empresas cómo se debe concretar esa protección.

La GDPR no es solo una nueva regulación de protección de datos adaptada a la era digital, es la norma que define las reglas del juego de un nuevo entorno competitivo: la economía del dato.

La gran cantidad de aspectos que cubre este reglamento puede abrumar a las organizaciones. Entre las empresas consultadas para este estudio existe cierta unanimidad en que “esta regulación era necesaria, pero al mismo tiempo es muy exigente en sus plazos”.

Este informe se centra en conocer las prioridades de las empresas más avanzadas en la aplicación de GDPR. Es decir, aquellas que ya tienen en marcha un proceso de cumplimiento normativo, y de hecho ya cumplen o han progresado en gran medida en una amplia proporción de los aspectos del reglamento. Se apoya en un conjunto de entrevistas a 40 responsables del cumplimiento en empresas de tamaño mediano y grande de todos los sectores. El objetivo es identificar qué aspectos están priorizando y así servir como referente para el grueso del mercado que se encuentra todavía perfilando su estrategia.

2. Responsabilidad en su cumplimiento, un esfuerzo trasversal

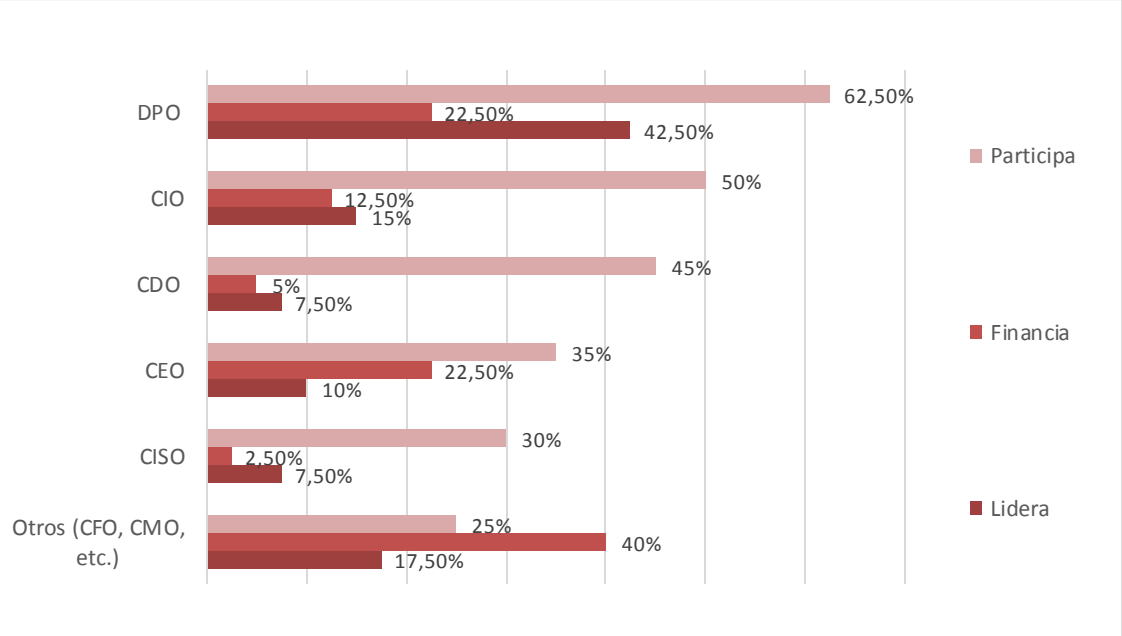
La responsabilidad sobre el cumplimiento de GDPR se eleva hacia la alta dirección en función de cómo son de críticos los datos personales para el negocio. Por ejemplo, en aquellas que realizan una explotación intensiva de datos personales se hace necesaria no solo la involucración del CEO sino incluso su liderazgo. Por otro lado, en aquellas donde los datos personales de clientes se capturan y procesan de forma marginal, el CEO delega en terceros el liderazgo de las distintas iniciativas. Cada empresa debe encontrar su propio enfoque.

En este punto conviene recordar que los datos personales también abarcan a los propios empleados. Esto explica por qué entre grandes empresas el departamento de recursos humanos tiene un papel activo en la definición de las prioridades de cumplimiento.

La GDPR también reconoce que no todas las empresas son iguales en la captura y tratamiento de datos personales. De hecho, distingue entre dos roles: controlador y procesador. El primero es la entidad que determina los propósitos y medios para procesar los datos; el segundo, es aquella que procesa los datos en nombre del primero. Estos roles no son excluyentes y en algunas empresas se dan de forma simultánea. Asimismo, la regulación exige que se nombre un cargo específico como responsable del cumplimiento (el Data Protection Officer o DPO), en un número de casos.

Por tanto, el primer aspecto a contemplar en la definición de la estrategia es si la empresa es controladora, procesadora o ambas. Y a partir de aquí establecer quién lidera, quién financia y qué departamentos estarán involucrados, y si es necesaria la creación del DPO.

Gráfico 1. Liderazgo, participación y financiación de las iniciativas GDPR.



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

Entre las empresas más avanzadas en el cumplimiento de GDPR en España se observa lo siguiente:

1. Los departamentos técnicos, que tendrán que implementar muchas de las iniciativas, cuentan con un alto grado de participación, pero la proporción de empresas en la que lideran es mucho menor.
2. La creación del DPO es una realidad en estas empresas y aunque frecuentemente tiene un papel de liderazgo, no es siempre es así. En algunos casos lo lidera directamente el CEO y en otros se crea un comité.
3. El departamento financiero es quien generalmente financia las distintas iniciativas con un marcado carácter trasversal y sin que exista un presupuesto definido de antemano.

No obstante, es importante tener en cuenta que GDPR no es un proyecto que termina el 25 de mayo de 2018. Más bien al revés, es en esa fecha cuando comienza una nueva etapa en la que se va a operar con los datos bajo un nuevo marco. Por ello, es necesario adquirir una perspectiva de un cumplimiento continuado. Las organizaciones que han pensado en GDPR como una iniciativa, tendrán que asegurar que sigue existiendo un liderazgo para el futuro.

3. Gestionar el dato con una perspectiva de ciclo de vida

Una vez definido quién lidera, financia y participa, el siguiente paso es evaluar qué iniciativas se van a llevar a cabo y con qué prioridad. En este informe se toma la perspectiva del ciclo de vida del dato para revisar las distintas acciones posibles.

La premisa es que el dato hay que entenderlo desde la perspectiva completa del ciclo de vida. Esto significa que se hace necesario un adecuado control del mismo desde su captura hasta su eliminación. Todas las etapas están conectadas, no puede gestionarse el dato si falta una etapa del ciclo.

En concreto este informe se organiza como sigue:

- *Captura del dato: la necesidad de diseñar una estrategia.*

  Las empresas tienen que diseñar una estrategia de captación de sus datos; tienen que hacerlo no solo porque la regulación los obligue, sino porque en adelante formará parte de un nuevo modelo de relación entre empresas y clientes basado en el permiso y la transparencia. Si la captura no se aborda de forma adecuada se menoscaba el resto de iniciativas.

- *Almacenamiento: un criterio adicional de decisión.*

  Las decisiones sobre qué tecnologías se utilizan para cubrir las necesidades de almacenamiento han venido determinadas por las necesidades del negocio en términos de rendimiento, latencia y coste. Sin embargo, ahora surgen nuevos agentes externos a la organización, clientes y regulador, con necesidades de acceso a la información que no se pueden planificar o anticipar, a las que hay que dar servicio de forma ágil. Esto tiene que encontrar su reflejo en las decisiones de almacenamiento.

- *Datos no estructurados: gestión más allá del data center.*

  Las empresas no estaban preparadas para el crecimiento exponencial de sus datos no estructurados, y menos aún para convertir su explotación en una variable competitiva. La consecuencia más directa ha sido la proliferación de datos sobre los que la empresa no tiene visibilidad ni control, que han adquirido la denominación de datos oscuros. Estos tienen el agravante de contener datos de carácter personal. En muchos casos, existen copias en múltiples ubicaciones posibles más allá del data center; por ejemplo, *PCs* y *smartphones*. Los datos personales oscuros o fuera del control de la organización ya no tienen cabida en la nueva regulación.

- *Uso y privacidad: escrutinio en el acceso.*

  El foco ya no está tanto en el dato en sí como en el uso que se hace del mismo, en quién, cómo y para qué accede a información de carácter privado. Aunque aquí algunas empresas se sienten preparadas, lo cierto es que todas esas capacidades de escrutar quién está accediendo a qué información y bajo qué permisos deben combinarse con formación y herramientas de soporte al empleado. Pero, todos esos mecanismos internos ya

implantados en las empresas no están ni orientados ni concebidos para que sea el cliente quien lance las preguntas sobre el uso y reciba la respuesta.

- *Fin del ciclo de vida: borrar un dato es posible.*

Existen distintos desencadenantes para que se produzca el borrado de los datos: que el cliente lo pida, que su valor dentro de la empresa esté amortizado o que el regulador lo estime oportuno. En cualquier caso, las empresas se han acostumbrado a que una vez que el dato entra en la organización, se queda en esta, en sus sistemas de almacenamiento. El problema que se plantea si un cliente exige el borrado es tanto tecnológico (dónde está ese dato o si estará duplicado), como operativo (quién lo borra o quién garantiza que se ha borrado).

3.1. Captura del dato: la necesidad de diseñar una estrategia

Para algunas empresas, explotar la información personal de sus clientes se ha convertido en una oportunidad para ofrecer nuevos servicios en la economía digital. Para otras, es ya una cuestión de supervivencia en el mercado. Los clientes están dispuestos a ceder parte de su privacidad si a cambio reciben valor, bien a través de una mejor experiencia, un trato personalizado o un ahorro de tiempo y dinero.

Sin embargo, las empresas no siempre son trasparentes sobre el uso que van a dar a los datos. En particular, si una vez que pasan por el tamiz de los algoritmos se revela nueva información. Por tanto, el problema desde la perspectiva del cliente no está en el dato en sí, sino en el uso que se haga de este. El regulador lo tiene claro y exige a las empresas que notifiquen qué uso van a hacer de los datos y, si se producen cambios o nuevos usos, que estos sean comunicados al cliente para que los acepte.

Como consecuencia, la captura del dato determina su ciclo de vida en la organización. El dato solamente puede utilizarse para el objetivo para el que ha sido recogido. Además, el proceso mismo de su captura tiene que introducir un consentimiento explícito. Ya no es suficiente con el consentimiento tácito.

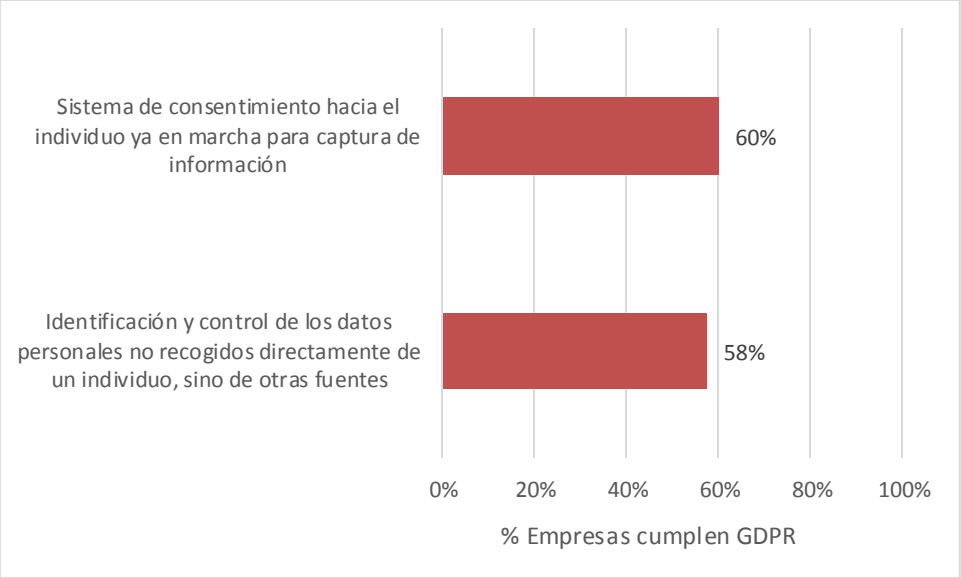
Para cerrar el círculo, las restricciones para el uso de los datos aplican también a aquellos recogidos antes de la entrada en vigor de GDPR. En este caso, las empresas tienen que asegurarse de que los usos del dato están claros y aprobados por el individuo.

Aquí es necesario que se produzca un cambio de mentalidad en la organización. El dato personal hay que tratarlo como un activo que pertenece al individuo. La empresa tiene un permiso de uso, pero tiene que responder ante el individuo si este así lo requiere.

El riesgo es que pueden aflorar usos del dato de los que el individuo no era del todo consciente antes del contexto de GDPR, más restrictivo. El reglamento también aplica para datos personales adquiridos de fuentes externas, dado que hay que notificarlo al individuo.

Las empresas que ya han cambiado de mentalidad saben que esto debe entenderse como el germen de un nuevo marco de relación, que se basa en una mayor trasparencia y un mayor empoderamiento del cliente. Esto hace necesario encontrar mecanismos que permitan una comunicación fluida y eficiente, lo que irremediablemente pasa por utilizar medios digitales e interactivos.

Gráfico 2. Mecanismos para la captura de datos



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

Como indica el gráfico, la captura de datos, bien sea de forma directa o a través de terceros, está ya integrada en el cumplimiento de GDPR en aproximadamente el 60% de las empresas.

En opinión de Delfos, la mejor manera de abordar el consentimiento es con un enfoque de transacción. Es decir, proporcionando al cliente un valor a partir de su consentimiento, devolviéndole a cambio información de utilidad, o una experiencia individualizada.

Si se diseña bien el mecanismo de consentimiento, puede mejorar la relación en todo el ciclo. En primer lugar, permite educar e informar al cliente de acuerdo con su perfil específico (nutrir el lead). En el caso del marketing, esto representa la formalización del marketing bajo permiso. Además, hace posible personalizar el propio producto de acuerdo con las necesidades individuales. Finalmente, permite mejorar y hacer más proactiva la prestación del servicio post-venta. No obstante, para que el consentimiento sea fluido y no sobrecargue al cliente, la comunicación debe de estar coordinada en todos los departamentos.

Este sistema de permisos tiene que ir conectado con las decisiones posteriores, de forma que se controle el alineamiento del uso con el consentimiento. Este control debe aplicarse a todos los participantes en la cadena de valor, lo que adquiere particular relevancia cuando la actividad de marketing o servicio al cliente están externalizadas. En consecuencia, es necesario prepararse para escenarios complejos permitiendo una gestión granular, dinámica y escalable :

- Granular: Distintos individuos pueden otorgar distintos consentimientos sobre cómo utilizar sus datos.
- Dinámica: Nuevos usos requerirán consentimientos adicionales.
- Escalable: Las exigencias del cliente pueden producirse de forma masiva y repentina.

3.2. Almacenamiento: un criterio adicional de decisión

Los criterios para las decisiones de almacenamiento de datos se han tomado siempre bajo una perspectiva de negocio. En el mejor de los casos, en función del rendimiento necesario en su uso, así como las latencias. La decisión sobre cuál es la tecnología más adecuada es dinámica.

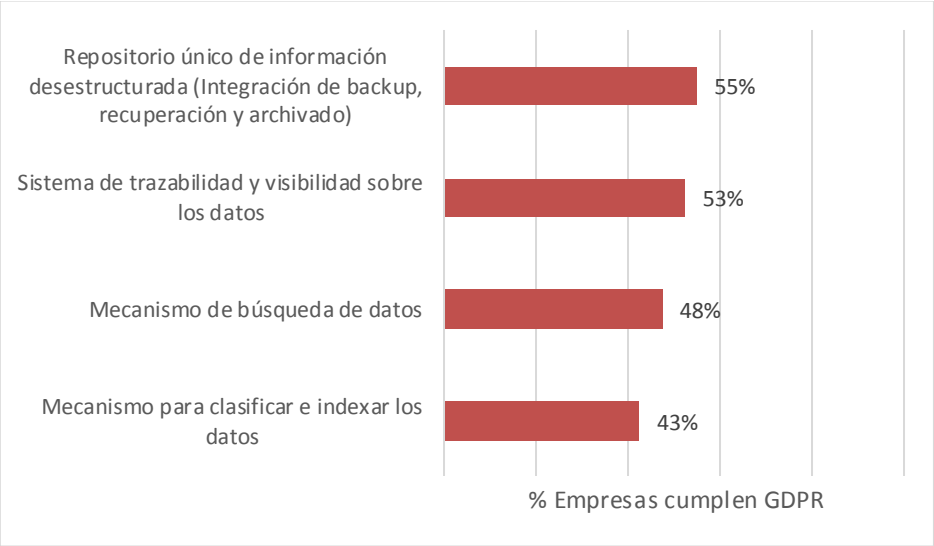
GDPR añade un criterio adicional: la necesidad de proporcionar los derechos al individuo sobre sus datos personales, y de hacerlo de forma ágil. Los derechos que añade GDPR son los de transparencia sobre su ubicación, limitación de uso, borrado (olvido) y portabilidad (que puedan transferirse a otra organización en un formato estandarizado).

Esto implica que el componente de relación con el cliente establecido en la etapa de consentimiento se amplía a la hora de cumplir sus derechos. Es decir, la calidad del servicio al cliente no solamente va a estar determinada por el producto o servicio, sino también por la eficiencia y celeridad con la que se resuelven los requisitos sobre su información.

Las implicaciones para el almacenamiento se hacen claras sin pensamos en peticiones no a nivel individual, sino en masa. Podemos considerar un escenario en el que millones de usuarios de un servicio reclamen información sobre la situación de su información personal, o su uso, por ejemplo en el caso de un rumor de vulnerabilidad, o incluso la notificación de una brecha.

El responsable de almacenamiento ya no puede pensar solo en términos de tecnología. Tiene que conocer la naturaleza del dato que almacena, y coordinarse con los usuarios del mismo. Estos abarcan desde las áreas de negocio hasta los desarrolladores, si utilizan datos personales para las aplicaciones. Además, pueden extenderse más allá de la organización, si forman parte de la cadena de valor, o si están integrados en una plataforma de servicios. En definitiva, su rol está evolucionando de administradores del almacenamiento a custodios del dato.

Gráfico 3. Sistema de almacenamiento



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

Tal y como puede verse en el gráfico, en las decisiones de almacenamiento han primado los criterios de infraestructura. En primer lugar, crear un repositorio de datos, donde no lo había, o donde la información estaba fragmentada. A partir de un almacenamiento integrado, se busca abordar la trazabilidad y visibilidad del dato, de forma que se evite el dato oscuro.

Esta forma de acción obedece a un pensamiento secuencial, en la que primero se resuelve la fragmentación del almacenamiento y la necesidad de visibilidad sobre los datos.

Una vez resuelto esto, la organización está preparada para poder atender los derechos del cliente o individuo. En este segundo nivel de acción, las empresas que han implementado un mecanismo de búsqueda son menos del 50% del total. En función del negocio, va a ser necesario crear capacidades para búsquedas complejas. Por ejemplo, si un usuario quiere eliminar sus datos, estos pueden estar ubicados en diferentes sistemas, como aplicaciones de *front-end*, el CRM o analíticas. También pueden estar en forma de datos no estructurados en servidores de ficheros, o dispositivos de usuario. Esto adquiere un nivel adicional de complejidad si se considera el *back-up*.

Finalmente, el mecanismo para clasificar e indexar los datos es el que se implementa en menor proporción. Este es el primer paso para poder segmentar los datos, discriminar los personales y sensibles de los que no lo son, y crear políticas que puedan cambiarse dinámicamente. Todavía no existe suficiente concienciación de la necesidad de clasificar los datos. Sin embargo, es un elemento esencial para una estrategia avanzada de almacenamiento. Parte del reto es que hay un histórico inmenso de datos no clasificados.

El almacenamiento ya no es una un problema a resolver o una necesidad que administrar. Las empresas más avanzadas gestionan el almacenamiento de forma proactiva, de forma que se pueda gestionar el dato de forma dinámica, con políticas automatizadas y cambiables.

Las organizaciones tienen que prepararse para un escenario en el que el envío de datos, incluso el intercambio de datos con clientes va a formar parte de su modelo de relación. El cliente va a querer ese nivel de interacción con la misma inmediatez que la de los productos o servicios.

3.3. Datos no estructurados: su gestión más allá del *data center*

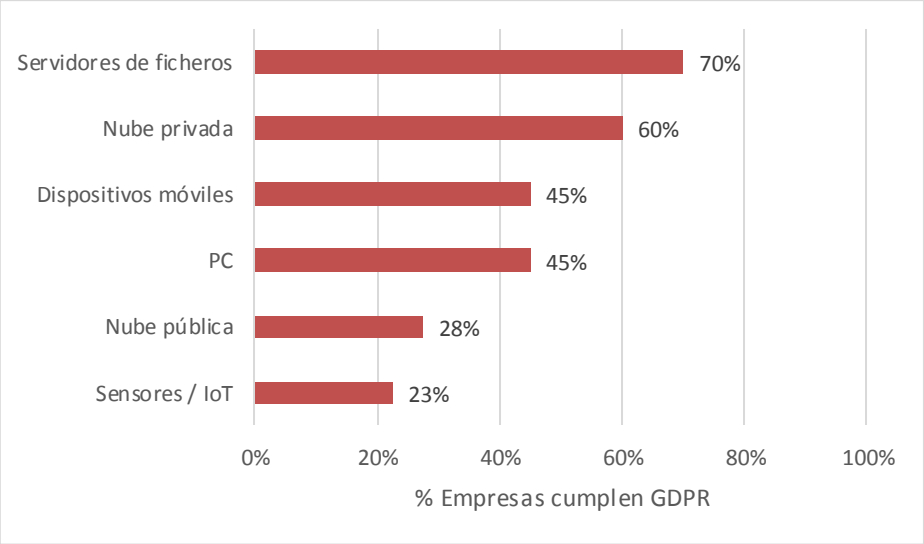
Solo hay un problema mayor que el de un crecimiento exponencial de datos no estructurados, y es no estar experimentándolo. Esto significaría que la empresa no compite en experiencia de cliente, en ofrecer un servicio personalizado, o que no ha transformado su modelo de negocio hacia un entorno digital.

Actualmente, la principal fuente de generación de datos es el propio cliente. Hablamos de datos de geolocalización, correos electrónicos o llamadas al *call center*. Para las empresas, el control de esta tipología de datos es algo sin resolver. La consecuencia más directa es que la mayor parte de este tipo de datos en las organizaciones son "datos oscuros", es decir, datos sobre los que la empresa no tiene visibilidad, ni control, pero que están ahí.

El reto está cuando dentro del dato oscuro encontramos datos personales, como C.V., documentos escaneados como DNI o pasaporte, correos electrónicos, grabaciones de llamadas, o incluso las direcciones IP. GDPR separa explícitamente los datos personales sensibles, que incluyen aspectos como la información sobre religión, afiliación política entre otros. Sobre estos últimos, los requerimientos de protección son mucho más estrictos.

La flexibilización del puesto que hace que el usuario pueda realizar copias de los datos en diferentes dispositivos, como tabletas o *smartphones*, en algunos casos desde el hogar, que pueden estar fuera del control de la organización. Las iniciativas de trabajo flexible tienen que ser compatibles con la necesidad de vigilar y proteger los datos. Las empresas necesitan tener visibilidad sobre dónde se encuentran los datos personales en todo momento. En este contexto, ya no tiene cabida la existencia de "datos personales oscuros", que estén fuera del radar de la empresa y no estén protegidos. Todos los datos tienen poder ser identificados o descubiertos, sea cual sea su ubicación, en la empresa o en la nube.

Gráfico 4. Control de datos no estructurados



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

En España, el nivel de control sobre los datos no estructurados es proporcional a su cercanía al *data center*. Aparecen tres niveles de control:

- Dentro del *data center*: Servidores de ficheros y nube privada. Hay una mayoría de organizaciones que tienen control sobre el acceso a los datos dentro de la organización, una proporción que supera el 60%.
- Dispositivos del empleado: Las empresas que tienen control sobre estos datos están ligeramente por debajo del 50%. Esto representa un riesgo para la organización, dado que la pérdida de estos dispositivos puede causar brechas de seguridad. De hecho, estos dispositivos están ganando interés por parte de los hackers. Además del riesgo, también afecta a la capacidad de reacción. La solución pasa por varias acciones: en primer lugar, controlar el dato, de forma que puedan ejercerse políticas independientemente del dispositivo, y se respete la privacidad del empleado; en segundo lugar, indexar y clasificar el dato para saber si una brecha afecta a datos personales; en tercer lugar, formar al empleado, para asegurar que sus hábitos de uso son compatibles con las políticas de seguridad.
- Datos fuera de la organización: Cloud pública e IoT. El porcentaje de empresas que controlan estos datos no estructurados es inferior al 20%. La razón, en el caso de cloud pública, es que la organización confía en el control de privacidad que realice el proveedor. En el caso de IoT, se trata de una tecnología todavía no utilizada por muchos negocios. En este caso, el control sobre los datos es todavía más crítico, ya que estos salen de la propia organización.

El criterio para controlar los datos no estructurados no debe de ser su ubicación, aunque este sea el más intuitivo, sino la naturaleza del dato y su propia sensibilidad. Por esa razón, GDPR incide en el análisis del impacto en el cliente como paso previo a las medidas de seguridad. Por ejemplo, un dispositivo *wearable* de salud, o de IoT en un vehículo pueden contener información más sensible y de mayor impacto que muchos de los datos que se encuentren en el *data center*.

3.4. Uso y privacidad: escrutinio en el acceso

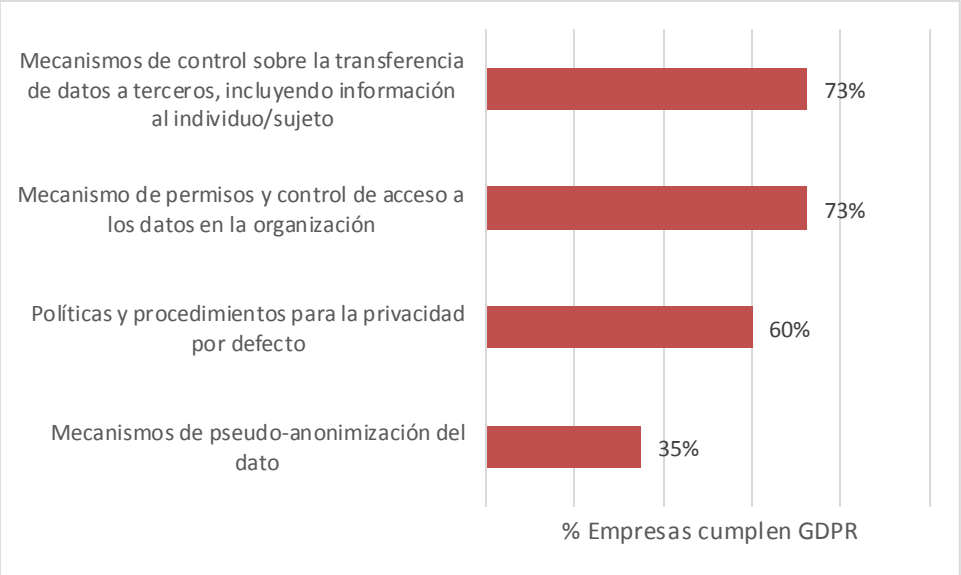
La GDPR deja claro que el foco ya no está tanto en el dato en sí como en el uso que se hace del mismo: en quién, cómo y para qué accede a información de carácter privado. El uso de los datos tiene que ser consistente con el consentimiento otorgado por el individuo, por tanto, tiene que existir una conexión entre la captura y el uso del dato.

Dado que en este punto el usuario puede ser el eslabón débil de la cadena de cumplimiento, es necesario dotarle de los recursos adecuados. El primer paso es una formación y sensibilización sobre la regulación, cómo usar adecuadamente el dato, y las implicaciones de usos inadecuados. Además, es necesario alinear esta formación con el gobierno del dato: una política de protección de datos que permita a todos conocer cuáles son sus responsabilidades. Esta política tiene que tener dos partes:

- Roles de uso de datos en la organización, y cuál es la interacción y responsabilidad sobre el dato de cada uno de ellos.
- Soporte al usuario con una herramienta de gobierno que le permita conocer cómo tiene que utilizar la información en su contexto diario.

Además, hay que tener en cuenta que la utilización del dato no tiene lugar únicamente dentro de la organización, sino también fuera de ella, a través, por ejemplo, de modelos de *outsourcing*. Aquí procede de nuevo la distinción entre el rol de controlador y el de procesador de datos. El marco de protección tiene que funcionar de igual manera si el uso de la información se produce dentro o fuera. Ello implica revisar los contratos y acuerdos entre la empresa y colaboradores externos, y asegurar que cumplen las condiciones de GDPR.

Gráfico 5. Privacidad y control



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

Las empresas españolas son conscientes de los riesgos cuando el dato sale de la organización, y entran otros actores de la cadena de valor. Por ello, más del 70% tiene un mecanismo de control de la transferencia de datos a terceros, por ejemplo empresas que analizan o gestionan sus datos o simplemente realizan la logística.

Los mecanismos de permisos y controles de acceso tienen un porcentaje similar de cumplimiento. La revisión de privilegios de forma granular se ha convertido en esencial.

Un dato sorprendente es que las empresas consideran que el nivel de implantación de políticas y procedimientos de privacidad por defecto es alto. Este es un aspecto que tiene una dimensión tecnológica, pero quizá la más importante es cultural. Esta tiene que ver con la minimización del dato externo: recoger la mínima información necesaria, guardarla por el mínimo tiempo posible y procesarla para lo mínimamente exigido. En definitiva, considerar que más dato del necesario representa un riesgo para el individuo y para la organización.

Un aspecto donde impacta este criterio es la actual cultura de copia, en la que un conjunto de datos se copia tantas veces como tareas se realizan (desarrollo, analítica, backup, entre otras). Las organizaciones deben de realizar las tareas, si es posible, con una copia única. Esto también afecta a los hábitos del empleado. De nada sirve limitar el acceso de un usuario dentro del *data center*, si este tiene copias fuera del control de la empresa. Este aspecto desplaza la prioridad desde las políticas y tecnologías al propio dato y al usuario del mismo. En opinión de Delfos, es necesario combinar el control de uso con el control de datos no estructurados en los dispositivos de empleado.

La *pseudo-anonimización* del dato es el aspecto menos conocido, lo que se refleja en su bajo nivel de cumplimiento. Afecta principalmente a las analíticas, en las que va a ser requerido anonimizar el dato, para extraer conclusiones que no estén vinculadas a individuos. La combinación de diferentes fuentes y datos sobre un mismo individuo puede dar una gran profundidad de información, revelando datos de los que el propio individuo puede no ser consciente. De ahí que GDPR sea tan estricto con la transparencia sobre el uso.

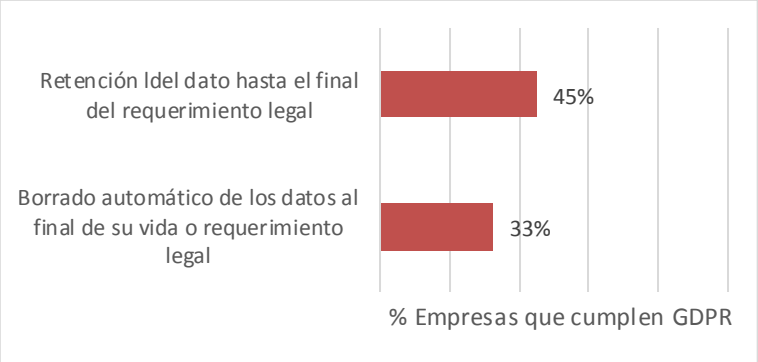
3.5. Fin del ciclo de vida: borrar un dato es posible

Es necesario que haya un final de ciclo de vida contemplado en la empresa para los datos personales. De no ser así, se genera una fuente de sobrecostes, así como de riesgos. En muchas industrias existe regulación sobre el período de retención de los datos. En la práctica, la retención es problemática cuando se trata de datos no estructurados o datos oscuros.

En definitiva, la organización tiene que establecer desde el principio el período de retención, y aplicar las políticas adecuadas. Hay que considerar también cuándo el borrado del dato se realiza a petición del cliente. No obstante, en este punto es relevante distinguir el ciclo de vida desde la perspectiva de su explotación por parte de la empresa y desde la perspectiva legal. Existirán ocasiones en que por razones regulatorias la empresa debe guardar el dato incluso cuando el cliente le pida expresamente que lo borre.

De todo ello se deduce que es necesario un sistema de gestión del ciclo de vida de los datos, que incluya un conjunto de políticas, y en el que se toman las decisiones en función del negocio, GDPR, y aspectos de tecnología. Es decir, un marco de gestión integrada del dato.

Gráfico 6. Fin del ciclo de vida



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

En España hay una cultura de almacenar y no borrar el dato. Este hábito está relacionado con la falta de visibilidad sobre el mismo, que hace imposible aplicar políticas para su destrucción.

Esto es una fuente de riesgos: si tiene lugar una brecha de seguridad que afecta a unos datos que deberían estar destruidos, y estos en consecuencia afloran, pueden causar un grave impacto en el usuario y el negocio. A esto habría que añadir el régimen sancionador, dado que confluiría la brecha de seguridad con el incumplimiento en el borrado de datos.

Finalmente, hay que tener en cuenta que puede existir un requerimiento legal para retener el dato, aunque el usuario solicite su borrado. En este caso, habría que combinar su archivado con una restricción en su acceso.

3.6. Necesidad de abordar el ciclo del dato de forma integrada

En este punto hay que destacar que el ciclo del dato tiene que abordarse de forma integrada. Todas las etapas están interrelacionadas, y si solo se pone el foco de cumplimiento en alguna de ellas, las carencias se pondrán al descubierto. Esto se puede ver con claridad con el ejemplo a continuación. Una persona puede realizar una queja de que ha sido contactada sin su consentimiento (por ejemplo, una llamada telefónica). La empresa tiene que verificar en primer lugar la etapa de captura del dato, para saber si consta en sus registros el consentimiento, y para qué acciones. Asimismo, tiene que contrastarlo con el uso (en este caso la llamada) que ha originado la queja de cliente, y dar al cliente una respuesta ágil.

Pero la incidencia puede no terminar ahí. El cliente puede decidir que se cambien sus permisos de uso. La empresa tiene que ser capaz de actualizar sus sistemas, de forma que no se le contacte en el futuro para ese tipo de campañas. Finalmente, si ha habido un error en el sistema (por ejemplo, datos de consentimiento tácito anteriores a GDPR no revisados), tiene que ser capaz de actualizar los permisos, para evitar que repita el error en un elevado volumen de individuos.

El proceso puede terminar con una solicitud de borrado de datos. Ello requiere identificar los datos de cliente, estructurados o no (desde contactos en el servidor de correo hasta registros de conversaciones), así como ubicar dónde se encuentran los datos, dentro o fuera del *data center*. A continuación, hay que chequear si existe un requerimiento legal de retención del dato, y proceder a su borrado o restricción del uso.

Este tipo de peticiones pueden además producirse a escala, como resultado de una incidencia en masa, o una brecha. En definitiva, el ejemplo ilustra el efecto dominó que puede desencadenar una petición o queja, aparentemente inocua, que revelaría todas las carencias en el ciclo del dato. Todo este conjunto de acciones por debajo de una solicitud de cliente es imposible de acometer de forma ágil si no hay una conexión entre las diferentes etapas del ciclo, y si no existe un grado de automatización.

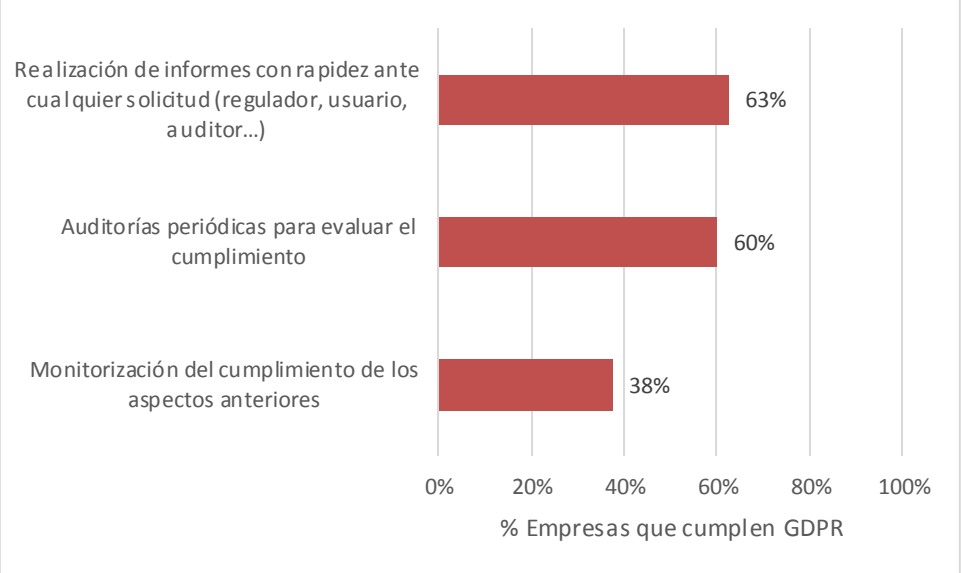
4. Monitorización, auditoría e informes

Todos los elementos descritos anteriormente en el ciclo de vida del dato, necesitan ser monitorizados y registrados. Es decir, la empresa tiene que ser capaz de demostrar que tiene una estrategia y unas políticas claramente definidas, y tiene que verificar que además se cumplen.

En este sentido, es importante destacar que las políticas deben de realizarse con perspectiva de ciclo. Si la captura del dato no se realiza de forma adecuada este será un problema que lastrará el resto de fases. Todas las etapas de la vida del dato están interconectadas. Por eso la aproximación debe ser holística.

Dado que el regulador puede pedir sin previo aviso un informe que refleje estos puntos, para que se entregue de forma prácticamente inmediata, un mecanismo para obtener esta información de forma manual no es viable. Es decir, es necesario introducir la automatización en la monitorización y generación de informes de uso, tratamiento y seguridad de los datos.

Gráfico 7. Monitorización, auditoria e informes



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

Aunque hay una mayoría de empresas que han implantado mecanismos internos de control del dato, el reto con el que se encuentran es que estos no están ni orientados ni concebidos para que sea el cliente quien lance las preguntas y reciba la respuesta. Por ello, más del 60% de las organizaciones han hecho un esfuerzo para conseguir realizar informes con rapidez ante cualquier solicitud, así como auditorías periódicas.

Cuando se trata de realizar una monitorización continua, la proporción baja, lo que indica una brecha entre el enfoque externo de cumplimiento y el interno. La monitorización del uso de datos puede detectar patrones de uso inadecuados, evitando que deriven en situaciones de

incumplimiento. Esta medida no debe limitarse a la organización, sino extenderse a toda la cadena de valor, o ecosistema de plataforma en el que participe la empresa. En definitiva, la realización de los informes debería de ser una consecuencia natural de la monitorización.

No obstante, cuando se aborda la monitorización, no solo hay que considerar los derechos hacia el cliente, sino también hacia el empleado, dado que este último como individuo también está protegido por la regulación. Es decir, hay que encontrar un equilibrio de forma que se pueda monitorizar el uso, sin fiscalizar los hábitos del empleado.

5. Seguridad

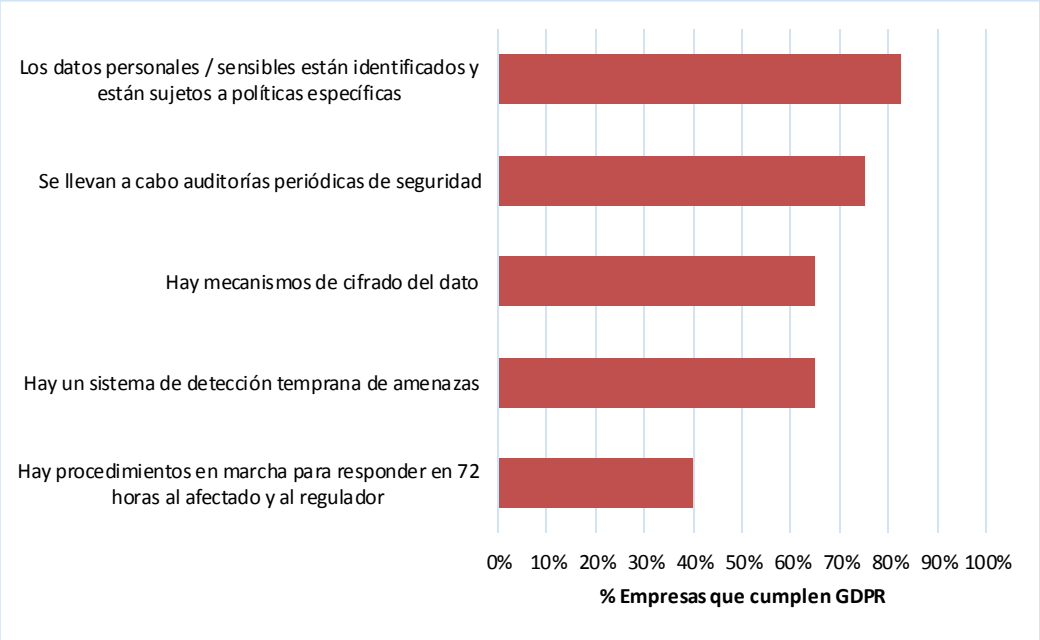
La principal diferencia entre GDPR y las regulaciones anteriores, es que la seguridad ya no se trata como un requisito, o como una lista de condiciones. Se deja a la discreción de cada organización el tomar los mecanismos de protección del dato más adecuados.

El regulador se rinde a la evidencia de que el ritmo de cambio tecnológico es tan rápido que ninguna lista de verificación de medidas de seguridad es efectiva. Por tanto, deja en manos de la propia empresa una estrategia de seguridad centrada en la gestión de riesgos. En primer lugar, es necesario realizar un análisis de impacto para las personas, en el caso de que se produzca una brecha de sus datos personales.

Además de incidir en la prevención, GDPR incide en la resiliencia, es decir, en la capacidad de respuesta en caso de que se produzca una brecha o ataque. Es obligatorio notificar una brecha en 72 horas desde que se produzca, tanto al regulador como a los individuos afectados.

Se trata en definitiva de un reconocimiento de que no es posible una seguridad infinita, sino que toda empresa es susceptible de problemas de seguridad que deriven en fugas de información. En este escenario el regulador se plantea qué deben hacer las empresas cuando esto suceda y la respuesta es, en primer lugar comunicarlo al regulador y a los clientes afectados para minimizar el impacto.

Gráfico 8. Seguridad



Fuente: Delfos Research, 2017

N = 40

Situación de las empresas avanzadas en el cumplimiento de GDPR

En España la detección de datos personales y sensibles, así como las políticas especiales de seguridad, están ya implementadas en una amplia mayoría de empresas. Asimismo, tienen lugar auditorías periódicas de seguridad.

Estos aspectos han sido de gran relevancia antes de la entrada en vigor de GDPR, ya que entran de lleno en las políticas de seguridad. En el caso del cifrado del dato, o la detección temprana de amenazas, la proporción de cumplimiento baja. Esto contrasta con la importancia que da GDPR al cifrado del dato (se nombra en cuatro ocasiones en el reglamento). Estese valora como un avance importante que permite suavizar otros criterios de cumplimiento, ya que el impacto de una brecha sobre un dato cifrado es menor que si no lo está.

Finalmente, la respuesta ágil en 72 horas, es el aspecto donde la proporción de cumplimiento es menor. Ello se debe a que requiere por un lado una detección temprana, ya no de amenazas, sino de ataques, combinado con una agilidad en las respuestas, que va más allá de las propias políticas de seguridad, y entra en la propia capacidad de reacción y resiliencia de la organización. Este aspecto está conectado con el control sobre el dato descrito en la sección de almacenamiento. Para comunicar una brecha en menos de 72 horas, es necesario contar con mecanismos para saber si ha afectado a datos personales, y saber con certeza si procede o no una notificación a los afectados y al regulador. Es aquí donde entran los mecanismos de identificación, clasificación e indexación del dato.

Hay que nombrar en este punto el requerimiento de seguridad por diseño. Esta no se puede medir de forma directa, ya que tiene que ver tanto con la arquitectura de almacenamiento como con los procedimientos a lo largo del ciclo de vida del dato.

6. Recomendaciones

En la regulación GDPR confluyen varios aspectos: el conjunto de elementos que cubre es amplio, es más restrictiva que la mayor parte de las leyes nacionales, entre ellas la LOPD, pero al mismo tiempo no contiene un listado de acciones específicas a cumplir.

Por ello, ante el imperativo de cumplir en todas las áreas, una organización puede verse desbordada. Si bien recomendamos apostar por GDPR de forma exhaustiva, creemos que el cumplimiento debe abordarse de forma escalonada, de acuerdo con un marco de prioridades.

En primer lugar, recomendamos un análisis de deficiencias (*Gap Analysis*) que permita identificar las principales carencias o lagunas en relación con la normativa, así como las acciones necesarias. Estas se pueden ordenar de forma que se resuelvan en primer lugar los aspectos más prioritarios. Recomendamos utilizar dos criterios para organizarlas: criticidad y urgencia.

En base a los resultados del estudio, presentamos una matriz de acciones como referencia. No obstante, a nivel individual, cada empresa tiene que encontrar su propio camino en función de su situación. Es decir, cada empresa tiene que crear su propia matriz.

Esta matriz divide las acciones en cuatro cuadrantes en función de la prioridad: En rojo, las acciones más prioritarias, dado que confluyen alta urgencia y alta criticidad. A continuación, en anaranjado, las áreas en las que destaca solo uno de los dos criterios. Finalmente, en gris, se representan la las acciones con criticidad y urgencia moderadas, que pueden abordarse en un plazo más dilatado.

Figura 1. Matriz de cumplimiento

Fuente: Delfos Research, 2017

A continuación, se detallan las principales acciones para cada uno de los cuadrantes del gráfico:

Urgencia y prioridad elevadas (color rojo): Acciones inmediatas

- **Identificar datos críticos:** Esta acción se basa en el hecho de que no se pueden controlar ni proteger los datos que no se ven. Esto afecta principalmente a los repositorios no estructurados de datos, actualmente en ubicaciones con poca visibilidad. Por tanto, en primer lugar, la empresa tiene que conocer dónde se encuentra la información en cada momento. Este es el punto de partida para las acciones posteriores, como buscar, encontrar, eliminar o portar datos, así como monitorizar el uso que se hace de la misma. Es aquí donde se pone en valor el indexado de los datos no estructurados.
- **Seguridad:** Revisar la seguridad desde la perspectiva de GDPR, en el que además de un enfoque proactivo orientado a gestión de riesgos y evaluación de impactos, es necesario notificar una brecha en menos de 72 horas. Todo esto lleva a hacer foco no solo en las herramientas de prevención de amenazas, sino también en la detección temprana de las mismas.
- **Asignar DPO (Data Protection Officer):** La empresa tiene que determinar si tiene la obligatoriedad de crear el puesto específico de DPO. En cualquier caso, debe decidir cómo coordina el proceso de cumplimiento normativo no solo hasta la fecha de entrada en vigor del reglamento, sino también a partir de la misma.

Urgencia más elevada que la criticidad (color anaranjado): Resiliencia para resolver lo urgente cuando se presente

- **Gestión de crisis:** Asegurar que la organización puede responder con agilidad ante una situación de crisis que pueda estar motivada por diferentes factores, desde una brecha de seguridad hasta una avalancha de solicitudes de cliente a escala (ej. millones de personas).
- **Recuperación ágil:** La organización tiene que ser capaz de minimizar el impacto de cualquier brecha. Ello requiere por un lado realizar análisis de impacto que permitan diseñar las acciones en función de la criticidad. Por otro, tener marcha planes de recuperación, que permitan retomar la actividad con agilidad en caso de una incidencia.

Criticidad mayor que la urgencia (color anaranjado): Redefinir la relación con los clientes

- **Consentimiento e información con clientes:** Revisar el modelo de comunicación con clientes, desde la etapa de consentimiento inicial hasta los cambios que puedan producirse en el uso de los datos o la respuesta a solicitudes de forma ágil.
- **Revisar los contratos de tratamientos de datos:** Asegurar que todos los actores de la cadena de valor, así como los prestadores de servicios externalizados, cumplen con el reglamento dentro como parte de su relación contractual.
- **Nuevo modelo de comunicación:** GDPR debe servir para sentar las bases de un nuevo modelo de comunicación, basada en la transparencia y el valor para ambas partes.

Urgencia y criticidad limitadas (color gris): Estrategia de protección del dato

- **Protección orientada al dato:** Asegurar que los datos personales están identificados, clasificados y monitorizados, sea cual sea su ubicación, dispositivo y uso. Asimismo, cifrar los datos personales en la medida de lo posible. Estas medidas, además de proteger directamente el dato, lo hacen desde el diseño.
- **Automatizar procesos**: Es necesario establecer unas políticas y procesos a lo largo de toda la organización. En la medida de lo posible, estos deben estar automatizados, para poderse realizar con agilidad. Tienen que apoyarse en una tecnología que les permita escalar las acciones (ej. Peticiones múltiples de usuarios).
- **Capacitar usuarios:** El mayor protagonismo del empleado en la transformación digital, junto con las políticas de puesto móvil y flexible, desplazan el riesgo hacia el usuario. Es aconsejable una formación sobre responsabilidades y riesgos que conlleva el uso del dato, que abarque también hábitos y mejores prácticas. Asimismo, el usuario tiene que poderse apoyar en herramientas de gobierno, y no depender únicamente de su buen juicio.

Las actuaciones necesarias son numerosas, y requieren cambios a varios niveles, que abarcan la tecnología, el empleado, los proveedores de servicios o el cliente. Por ello, para hacer realidad el cumplimiento de GDPR es necesario tener claro hasta dónde puede llegar la empresa por sí misma, y dónde necesita ayuda y asesoramiento.

La mayor parte de las empresas van a necesitar apoyarse en uno o más proveedores tecnológicos para este proceso. Es aconsejable compartir con ellos esta matriz de acciones, dado que pueden proporcionar *feedback* valioso, bien sea identificando acciones inicialmente desapercibidas, o sugiriendo cambios en las priorizaciones. Además, si hay varios actores, el gráfico puede servir para conocer dónde encaja cada uno en el proceso, y coordinar mejor las tareas y comunicaciones.