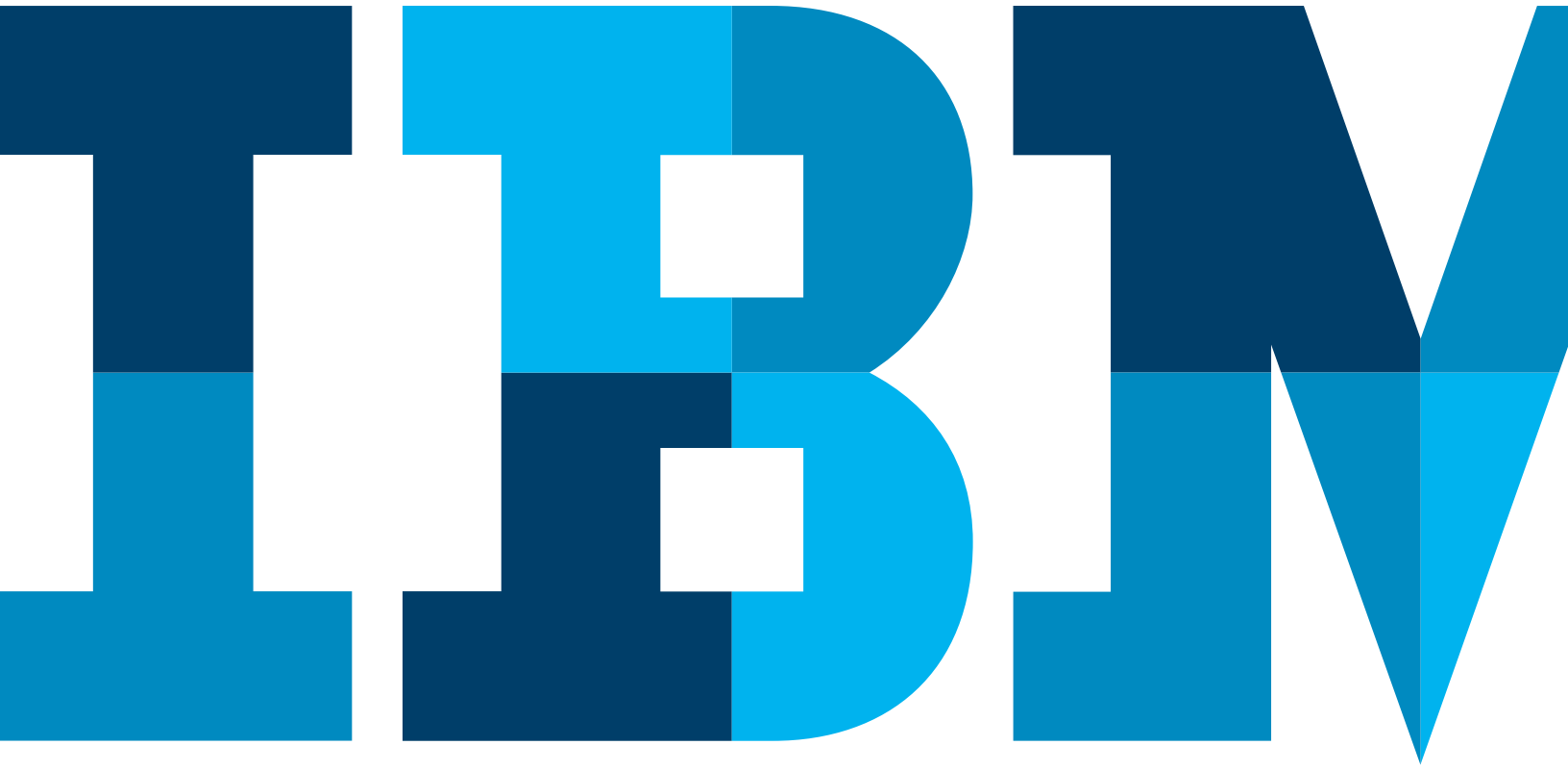
IBM
Documento técnico

Las vías de IBM para prepararse para el GDPR

Prepare a su empresa para los nuevos requisitos de protección de datos en la Unión Europea



IBM

Contenido

Introducción

Si su empresa opera en la Unión Europea (UE), probablemente ya sabe que se le complicará la vida a partir de mayo del 2018, fecha en la que entrará en vigor el Reglamento General de Protección de Datos (GDPR) para la Unión Europea.

El objetivo de este nuevo reglamento más estricto es el de armonizar al máximo las distintas reglas de protección de datos de los 28 estados miembros de la UE. En algunos casos, simplemente reforzará o mejorará derechos específicos que ya se garantizan en muchos reglamentos locales, mientras que otros derechos se introducirán por primera vez.

La UE cuenta con más de 500 millones de ciudadanos y 20 millones de empresas activas, todos ellos directamente afectados por el GDPR. Además, muchas de las normativas se aplicarán a ciudadanos de varios países no miembros de la UE, incluyendo Suiza, Noruega, Islandia y Liechtenstein, para homogeneizar con estos países las reglas incluidas en el GDPR cuando se incorpore al Acuerdo EEE de 1992 (actualmente es una ley aprobada bajo el escrutinio del EEE-AELC.)

Asimismo, el nuevo reglamento se declara explícitamente extraterritorial en determinadas circunstancias. Esto significa que, aunque su organización no tenga una presencia física en el mercado de la UE, se regirá por el GDPR si se cumplen las siguientes condiciones:

- Ofrece bienes o servicios de pago o gratuitos a ciudadanos de la UE
- Gestiona o procesa los datos personales de los ciudadanos de la UE, o supervisa su comportamiento

Además, si trabaja con socios que operan en la UE, estos probablemente confiarán en que cumpla con el GDPR para limitar su propio riesgo. Dicho de otro modo, el cumplimiento del GDPR se considerará un requisito para cualquier organización que quiera lucrarse en Europa.

¿Cuáles son las posibles repercusiones del incumplimiento del GDPR?

Las sanciones económicas derivadas del incumplimiento del GDPR se definen claramente: por cada caso de incumplimiento, las organizaciones pueden enfrentarse a una sanción de hasta 20 millones de euros o el 4% de la facturación anual, el que sea de importe superior. A ello hay que sumarle el daño que dicha multa —o más específicamente las acciones que han provocado la multa— puede causar a su reputación de cara a sus clientes y empleados.

Incluso podría suponerle perder cuota de mercado ante competidores que se han preparado mejor. Algunos clientes de IBM ya se están posicionando para prepararse para el GDPR y obtener una ventaja competitiva. La implementación proactiva de medidas de seguridad y privacidad de datos permite a estas organizaciones mejorar su reputación, además de presentar un valor adicional para atraer a nuevos clientes.

Todos los indicadores apuntan que el GDPR se aplicará de forma estricta desde el primer día. Las empresas no deben confiar en que dispondrán de un periodo de gracia. De hecho, la Information Commissioner's Office (ICO) del Reino Unido ha confirmado que las organizaciones que no cumplan corren el riesgo de ser sancionadas inmediatamente.[1] Sin embargo, también ha declarado que aplicarán un enfoque pragmático basado en el sentido común para los principios del reglamento, permitiendo que las organizaciones expliquen las medidas tomadas para prepararse.

Además, los reguladores podrán interrumpir el negocio si sospechan que la organización no cumple con el GDPR. La investigación que realicen puede concluir que dicha organización dista aún más de cumplir con el reglamento de lo que el regulador —o la propia empresa— pensaba inicialmente.

Por tanto, podemos afirmar que la amenaza que supone es a su vez un incentivo, ya que su cumplimiento aporta beneficios, aparte de los riesgos de su incumplimiento. La implementación del GDPR puede ser el detonante para que establezca una estrategia de datos más sólida, que le permita seguir generando ingresos.

Un uso más inteligente de los datos en sus sistemas —esto es protegerlos sin limitaciones, controlarlos de forma efectiva, comprenderlos y ponerlos a disposición de los usuarios— le permitirá identificar oportunidades de innovación y nuevas fuentes de ingresos que de otro modo no habría detectado. Un método proactivo de preparación para el GDPR puede ser el primer paso hacia una mejora de la rentabilidad de sus datos.

¿Qué implica prepararse para el GDPR?

Además de ser más sólido que los reglamentos de protección de datos existentes en los estados miembros de la UE a nivel individual, el GDPR es también un reglamento mucho más estricto que muchos de los establecidos en Estados Unidos. Muchas organizaciones estadounidenses perciben los datos como un mero recurso de mercado; el GDPR les forzará a tener en cuenta la privacidad y la seguridad de los datos. El reglamento cubre la seguridad, la privacidad y el gobierno de los datos, por tanto, cualquier estrategia de preparación que establezca deberá abordar estas tres cuestiones para que sea efectiva.

Si se fija en los temas principales de las medidas técnicas y organizativas del GDPR, queda claro que la estrategia de preparación para el GDPR debe englobar personas, procesos y tecnología. La mayoría de las organizaciones podrá conservar algunos de sus procesos, o basarse en ellos para cubrir las carencias que tenga.

Uno de los objetivos finales que debería considerar es el desarrollo de una estrategia de gobierno integral y unificada. Si se implementa adecuadamente, esta estrategia le ayudará a cumplir con el GDPR, además de posicionarle mejor para cumplir con cualquier otro reglamento de protección de datos que sea aplicable, ahora o en el futuro.

Cinco conceptos principales

Desde nuestro punto de vista, existen cinco conceptos principales que debería conocer para comprender sus obligaciones con el GDPR, como se muestra en la Figura 1:

1. Derechos de los ciudadanos de la UE
2. Seguridad de los datos personales
3. Legalidad y consentimiento
4. Responsabilidad de cumplimiento
5. Diseño y predeterminado

Principales deberes, obligaciones y sanciones

Figura 1: Desde el punto de vista de IBM, existen cinco conceptos principales que debería conocer para comprender sus obligaciones con el GDPR.

1. Derechos de los ciudadanos de la UE

Los derechos que se aplicarán a todos los ciudadanos de la UE en circunstancias adecuadas incluyen el derecho a la información, acceso, rectificación, borrado, restricción de tratamiento, portabilidad y objeción. Su organización también deberá informar a los clientes sobre sus derechos en referencia a los datos personales, además de cumplir rápidamente con todas las solicitudes de derechos que presenten.

Un paso importante que puede dar para cumplir estos requisitos es mantener la calidad de los datos. Identificar datos redundantes, obsoletos y triviales (ROT) y eliminarlos puede reducir costes y riesgos, además de ayudarle a prepararse para el GDPR. Todos los datos que se mantengan tras la eliminación deben ser accesibles en un formato usable, en orígenes de datos estructurados y no estructurados. Esto está ligado a sus responsabilidades establecidas en el GDPR, como la minimización de los datos y la limitación del almacenamiento.

2. Seguridad de los datos personales

Su organización debe proporcionar un nivel de seguridad de los datos adecuado a los riesgos que afronta. Uno de los requisitos del GDPR es, cuando proceda, notificar infracciones de datos en un plazo de 72 horas. Por tanto, es aconsejable implementar herramientas de seguridad de datos que aceleren la respuesta, ayudando a su vez a minimizar el daño sobre la reputación.

Asimismo, debería considerar aplicar medidas pre-incidente para impedir que se produzcan infracciones. Las técnicas adecuadas para ello se indican específicamente en el GDPR, e incluyen minimización, seudonimización y cifrado. También sería conveniente aplicar disciplinas de gobierno de la información, incluyendo la eliminación justificable, para reducir la cantidad de datos personales que podrían estar en riesgo.

3. Legalidad y consentimiento

Bajo los términos del GDPR, asegurar el consentimiento resultará mucho más difícil para su organización, ya que para que el consentimiento sea válido, debe otorgarse libremente, de forma específica, informada e inequívoca. En casos como la asistencia sanitaria, donde es más frecuente el manejo de categorías especiales de datos, también debe ser explícito. Además, el interesado puede retirar su consentimiento en cualquier momento.

Sea cual sea el proceso que utilice para obtener el consentimiento, debe realizarse teniendo en cuenta los fundamentos legales para el tratamiento de datos personales. La ICO ha elaborado unas directrices de regulador según las cuales el consentimiento solo debe utilizarse cuando proceda y cuando no se apliquen otros fundamentos legales.

El consentimiento debe obtenerse con total transparencia, sin inducir a error o confusión al interesado. Para abordar todas estas cuestiones, su organización puede adoptar un sistema de gestión de consentimientos, basado en actividades que podrían considerarse mejores prácticas, como la implementación del seguimiento del flujo de trabajo o el establecimiento de una única fuente de verdad.

Además del consentimiento, existen otras cuestiones referentes a la legalidad que debería tratar, incluyendo la necesidad y el interés legítimo. Es muy importante que sepa exactamente qué datos tiene y por qué los tiene. La correlación y el descubrimiento de datos son dos medidas relevantes que pueden ayudar a su organización a alcanzar este objetivo, así como obtener asesoramiento legal y contratar un director de protección de datos corporativos (DPO), el cual incluso aunque no lo necesite estrictamente, puede resultar útil.

4. Responsabilidad de cumplimiento

No basta con que una organización trabaje para cumplir con el GDPR, sino que debe ser capaz de demostrarlo o documentar su progreso hacia el cumplimiento. Algunas de las medidas que puede tomar incluyen registros, evaluaciones, códigos de conducta o certificaciones proactivas.

El artículo 30 del GDPR especifica los registros de actividades de tratamiento, que normalmente se reconocen como una forma de correlacionar datos específica del GDPR, y puede ayudarle con la responsabilidad. Estos registros deberían gestionarse de forma proactiva con las herramientas adecuadas, evitando hojas de cálculo estáticas, que tienden a ofrecer información limitada y pueden quedar desfasadas rápidamente.

5. Diseño y predeterminado

El concepto de protección de datos por diseño y de forma predeterminada requiere que los controladores de datos implementen medidas técnicas y organizativas que demuestren el cumplimiento con los principios del GDPR.

En el elemento del diseño, el principio de la minimización de los datos forma parte de la integración de las garantías necesarias en el tratamiento, a fin de proteger los derechos de los interesados y cumplir con el GDPR. De modo similar, en el elemento predeterminado, solo deberían tratarse los datos personales necesarios para una finalidad específica. Bajo este precepto, estos datos se controlan en todo su ciclo de vida, desde la recopilación hasta la eliminación, prestando especial atención a limitar la accesibilidad a personas que no sean los interesados.

La clave de este concepto es tener siempre presentes los datos personales. Para los datos no estructurados, las organizaciones deberían sindicar, instrumentar y aplicar políticas referentes a la correlación, la gestión y la seguridad de los datos personales, mejorando la rentabilidad de la información y reduciendo riesgos. Del mismo modo, para los datos estructurados, podrían implementar la gestión de metadatos y políticas, así como explorar y gestionar el linaje de datos, para crear información que se adhiera a los principios del GDPR.

Vías para prepararse para el GDPR

Muchas organizaciones son conscientes de que ya tienen que empezar a tomar medidas para prepararse para el GDPR; pero no saben bien cómo empezar. La verdad es que no hay una única respuesta correcta; por dónde empezar depende de su situación actual. Por ello, IBM ha analizado nuestros compromisos de clientes y ha identificado varías vías comunes que han sido prioritarias para la mayoría de las organizaciones que se están preparando para el GDPR, así como otras vías que podrían tratar en el futuro.

Vías del GDPR que requieren atención inmediata

Evaluación de la preparación para el GDPR

Si aún no lo ha hecho, el primer paso debería consistir en determinar el estado actual de madurez de la protección de datos en su organización, así como los riesgos del GDPR a los que expondría a su organización si no empieza a tomar medidas ya. Lo ideal sería incluir un inventario de resumen de datos, que le daría una idea básica de la ubicación de los datos personales en su organización. Irá ampliando el resumen durante los siguientes pasos.

Un aspecto clave de la evaluación de la preparación para el GDPR sería trazar una hoja de ruta para evitar las fuentes de riesgo que ya ha identificado, incluyendo reconocer iniciativas de la compañía en las que basarse, así como carencias específicas del GDPR que deberían cubrirse. Una vez trazada la hoja de ruta priorizando los pasos a seguir, puede asignar a los encargados de dirigir estas tareas.

Descubrimiento de datos personales

El descubrimiento de datos personales, que puede completarse durante o después de la evaluación de preparación de riesgos, le permite conocer mejor sus orígenes de datos y lo que contienen.

Muchas organizaciones controlan donde están sus orígenes de datos estructurados y lo que contienen, pero no suele ser así en los orígenes de datos no estructurados. Los orígenes de datos como antiguos usos compartidos de archivos, unidades compartidas, SharePoint y repositorios de contenido se olvidan fácilmente, y a menudo contienen datos personales que no se tratan adecuadamente.

A veces incluso sabiendo que tiene datos personales que debe proteger, quizá no sabe todo lo que debería sobre el volumen de dichos datos, exactamente a qué interesados implica o cualquier otra clase de detalles. Para prepararse para el GDPR, hemos concluido que es de vital importancia limpiar todos los datos antiguos, moviendo los datos que necesite para introducirlos en el programa de seguridad y gobierno de la información y así garantizar su comprensión y protección.

IBM ofrece a sus clientes un acuerdo de preparación para el GDPR rápido y efectivo que se basa en el potencial de herramientas como IBM® Information Analyzer, IBM Information Governance Catalog e IBM StoredIQ®, y trata orígenes de datos estructurados y no estructurados. Está diseñado para generar un plan claramente definido que le ayudará a que sus esfuerzos de preparación para el GDPR tengan una duración de entre cuatro y seis semanas de análisis.

Como parte del compromiso de preparación para el GDPR, su organización se expondrá a rutinas establecidas en procesos repetibles y estandarizados que ayudarán a identificar todos los datos personales. Además, IBM trabajará con usted para minimizar los datos personales en almacenes de datos identificando datos que su negocio ya no necesita mantener. Al minimizar estos datos—limitando lo que almacena y por cuánto tiempo—reducirá los riesgos del GDPR.

Podrá empezar con el descubrimiento de los datos personales que maneja su organización en tan solo dos meses desde la implementación.

Inventario de datos

En base a los principios establecidos durante la evaluación de preparación de riesgos, el inventario de datos es donde consolidará todo lo que ha aprendido sobre sus datos personales, incluyendo los orígenes de dichos datos y su ubicación física. Esta medida debe tomarla como parte del requisito de registrar las actividades de tratamiento, según lo establecido en el Artículo 30 del GDPR.

En IBM, creemos que la mejor manera de crear un inventario de datos actualizado consiste en combinar un método ascendente (con herramientas de inventario de datos) con un método descendente (realizando entrevistas a usuarios técnicos y de negocio para conocer de primera mano dónde residen los datos, y qué valor de negocio extraen los usuarios de dichos datos). Este proceso debería ser iterativo en el tiempo, para actualizar los cambios que se vayan produciendo.

Herramientas de IBM como Information Analyzer y StoredIQ ayudan a acelerar y mejorar el proceso de correlación de datos,

ya sean estructurados o no estructurados. Mediante el análisis y la clasificación rápida del contenido de sus almacenes de datos, estas herramientas y las actividades de correlación descendente que realice—trabajando junto con IBM Information Governance Catalog—le ayudarán a crear un catálogo detallado de almacenes de datos personales, ubicaciones, finalidades, propietarios, tipos de interesados, etc., y al mismo tiempo podrá reducir las tareas manuales.

Un inventario de datos completo y preciso establece la base para una estrategia integral de gobierno de la información, cuyos beneficios no solo se limitan a la preparación para el GDPR, sino que le ayudan a cumplir con otros reglamentos y normativas que podrían afectarle, ahora o en un futuro. Es a su vez el primer paso para obtener resultados de negocio más informados, poniendo datos valiosos a disposición de los usuarios de negocio en toda la organización.

Enmascaramiento, cifrado y transformación (redaction)

Entre las soluciones de IBM que le ayudan a prepararse para el GDPR se incluye IBM Optim™ para el enmascaramiento y la transformación, así como IBM Guardium® para el cifrado. Juntas, estas herramientas garantizan la disponibilidad de los datos cuando y donde los necesite, minimizando el riesgo de que se acceda a los datos inactivos.

Optim asegura a las organizaciones el principio de la minimización de los datos. La información se des-identifica siempre que sea posible, y solo se conservan los puntos de datos necesarios para actividades de tratamiento, como la analítica y las pruebas.

A través de diversas técnicas de enmascaramiento, Optim ayuda a proteger datos como números de tarjetas de crédito, direcciones de correo y números de identificación, sin perder el significado contextual subyacente. Por ejemplo, un número de tarjeta enmascarado tiene el formato de un número de tarjeta de crédito real y funciona como tal en pruebas, sin poner al propio número en riesgo de exposición.

El enmascaramiento se realiza en cargas de trabajo en cloud y local, con reglas y clasificaciones de privacidad de datos predefinidas, diseñadas para acelerar la implementación y simplificar los informes. Aunque los datos que ya no son necesarios para el tratamiento pueden redactarse directamente, la organización puede seguir obteniendo valor de los datos enmascarados, representando una de las muchas maneras en que la preparación para el GDPR ayuda a hacer un mejor uso, y más sensible, de sus datos.

Los servicios de cifrado de datos de Guardium GDPR Accelerator, combinados con funcionalidades de cifrado de hardware y almacenamiento, pueden ayudar a asegurar que solo las personas con buenos motivos para ello puedan acceder a la información personal sensible. A fin de cumplir con los requisitos del GDPR, este cifrado cubre todo el ciclo de vida de los datos, desde que se introducen por primera vez en la organización hasta que se eliminan o se enmascaran.

Las organizaciones también pueden aprovechar las soluciones de IBM Enterprise Content Management para gestionar y transformar contenido no estructurado en función de los roles de usuario. Los usuarios verán los datos que necesitan para realizar sus trabajos, y nada más.

El entorno para GDPR de IBM

IBM ha creado un entorno para el GDPR que destaca cinco fases para la preparación, como se muestra en la Figura 2: Evaluar, Diseñar, Transformar, Operar y Adherirse. El objetivo del entorno es ayudar a los clientes a gestionar eficientemente la seguridad y la privacidad desde una perspectiva de riesgo para reducir los riesgos y, por tanto, los incidentes.

Evaluar, Diseñar, Transformar, Operar y Adherirse

Fase	Evaluar	Diseñar	Transformar	Operar	Adherirse
Actividad	• Realice evaluaciones del GDPR de privacidad, gobierno, personas, procesos, datos, seguridad • Desarrolle la hoja de ruta de preparación para el GDPR • Identifique los datos personales	• Diseñe los estándares de gobierno, formación, comunicación y procesos • Diseñe los estándares de privacidad, gestión de datos y gestión de la seguridad	• Desarrolle e integre procedimientos, procesos y herramientas • Ofrezca formación para el GDPR • Desarrolle estándares con privacidad por diseño, seguridad por diseño y políticas de gestión de datos	• Ejecute todos los procesos de negocio relevantes • Supervise la seguridad y la privacidad mediante TOMs • Gestione los derechos de consentimiento y acceso de los interesados	• Supervise, evalúe, realice auditorías y notifique la conformidad con los estándares del GDPR
Resultado	**Evaluaciones y hoja de ruta**	**Plan de implementación definido**	**Procesos y mejoras completados**	**Entorno operativo establecido**	**Creación de informes y supervisión continua**
	Identifique el impacto del GDPR y planifique Medidas Organizativas y Técnicas (TOM)	Incluye controles, procesos y soluciones de protección de datos para implementar	TOMs establecidas: descubrimiento, clasificación y gobierno de datos personales	Aplicar la nueva forma de trabajar del GDPR	Supervisar la ejecución de TOMs: presentar pruebas de cumplimiento

Figura 2: El entorno para GDPR de IBM

Vías adicionales a considerar en un futuro

Aunque estamos convencidos de que las vías descritas en la sección anterior son los puntos de partida más lógicos para la mayoría de las organizaciones que se preparan para el GDPR, existen otras áreas a explorar que le pueden reportar beneficios después de realizar los primeros pasos básicos.

Plan de protección de datos críticos: Identifique y clasifique los activos de GDPR más importantes para su organización, incluyendo las joyas de la corona y otra información protegida.

Gestión de datos maestros: Obtenga una perspectiva completa de quiénes son los interesados, qué datos suyos retiene y dónde están ubicados dichos datos.

Solicitudes de Derechos de Acceso de los Interesados (SAR): Proporcione a los interesados un modo simple y efectivo de ejercer sus derechos de consulta, corrección y eliminación.

Gestión del consentimiento: Ofrezca el tratamiento de datos específicos y utilice los requisitos de consentimiento para cada uso y cada ciudadano.

Implementación de seguridad y remediación: Despliegue funcionalidades de seguridad de la información en todas sus funciones de tratamiento de datos personales.

Gestión de incidentes: Despliegue funcionalidades de preparación, gestión y creación de informes proactivas ante incidentes con las soluciones IBM Resilient®.

Eliminación de datos: Elimine los datos que ya no son de utilidad para el negocio, en todos los sistemas.

Gestión de cambios de procesos y personas: Cree una cultura de la organización que complemente todos los cambios técnicos descritos en este documento.

Comprender sus obligaciones con el GDPR

El objetivo de este documento es demostrar que la preparación para el GDPR no es sencilla, sino que es un proceso complejo, exigente y costoso, pero a su vez necesario. Además del simple hecho de que le ayudará a evitar serias sanciones, la preparación para el GDPR se puede considerar un coste de hacer negocios cuando implican interacciones con la Unión Europea.

Además, creemos que la implementación del GDPR es el primer paso hacia un único mercado digital en toda Europa. Las organizaciones que actúen ahora estarán mejor posicionadas en esta nueva realidad.

El cumplimiento del GDPR también generará confianza entre sus clientes y empleados, incrementará su visibilidad y comprensión del negocio, pondrá a disposición de los usuarios de negocio datos de calidad, aumentará su eficiencia y le permitirá identificar nuevas oportunidades para generar ingresos. Los beneficios que aporta la preparación para el GDPR por sí mismos ya son un buen motivo para actuar, no solo los riesgos de su incumplimiento.

Ahora que comprende la urgencia de prepararse para el GDPR, así como algunas formas de empezar, cuente con las personas, los procesos y la tecnología de IBM para avanzar. Si necesita ayuda para identificar los pasos a seguir o si está preparado para establecer una plataforma completa de gobierno de la información, estamos aquí para prestarle la asistencia necesaria.

Información adicional

Para conocer mejor la perspectiva de IBM sobre la preparación para el GDPR, póngase en contacto con su representante de IBM, o bien visite **ibm.com**/es-es/gdpr/.

IIBM España
Santa Hortensia 26
28002 Madrid

Producido en España
Junio de 2017

Este documento se considera actualizado en la fecha inicial de su publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

LA INFORMACIÓN PROPORCIONADA EN ESTE DOCUMENTO SE DISTRIBUYE "TAL CUAL", SIN GARANTÍA ALGUNA, YA SEA EXPRESA O IMPLÍCITA, INCLUYENDO TODA GARANTÍA DE COMERCIALIZACIÓN, IDONEIDAD PARA UN FIN CONCRETO O INFRACCION DE DERECHOS DE TERCEROS. Los productos IBM están garantizados de acuerdo con los términos y condiciones de los contratos con arreglo a los cuales son facilitados.

Aviso: Los clientes son responsables de garantizar el cumplimiento con las leyes y normativas aplicables, incluyendo el Reglamento General de Protección de Datos de la Unión Europea. Los clientes son los únicos responsables de obtener asesoramiento legal competente referente a la identificación y la interpretación de cualquier ley relevante que pudiera afectar a su negocio, así como cualquier medida que debieran tomar para su cumplimiento. Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetas a disponibilidad. IBM no proporciona asesoramiento legal, de contabilidad ni de auditoría, ni representa ni garantiza que sus servicios o productos son garantía de que los clientes cumplan con las leyes o normativas vigentes.

Declaración de buenas prácticas de seguridad: La seguridad de los sistemas de TI implica proteger sistemas e información mediante la prevención, detección y respuesta a un acceso indebido desde dentro o fuera de su empresa. Un acceso indebido puede tener como consecuencia la alteración, destrucción o apropiación indebida de información o bien provocar daños o un uso inadecuado de sus sistemas, lo que incluye ataquesa terceros. Ningún sistema o producto de TI debe ser considerado completamente seguro y ningún producto o medida de seguridad puede ser por sí solo plenamente efectivo para prevenir accesos indebidos. Los sistemas y productos de IBM han sido diseñados para ser parte de una estrategia de seguridad completa y legal, lo cual conlleva necesariamente procedimientos operativos adicionales y puede requerir otros sistemas, productos y servicios para ser realmente efectiva. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O VAYA A HACER SU EMPRESA INMUNE FRENTE A, LA CONDUCTA MALITENCIONADA O ILEGAL DE PARTE ALGUNA.

1 The Privacy Advisor, *ICO's Wood: GDPR grace period? No way.* https://iapp.org/news/a/icos-wood-gdpr-grace-period-no-way/

Recicle este documento