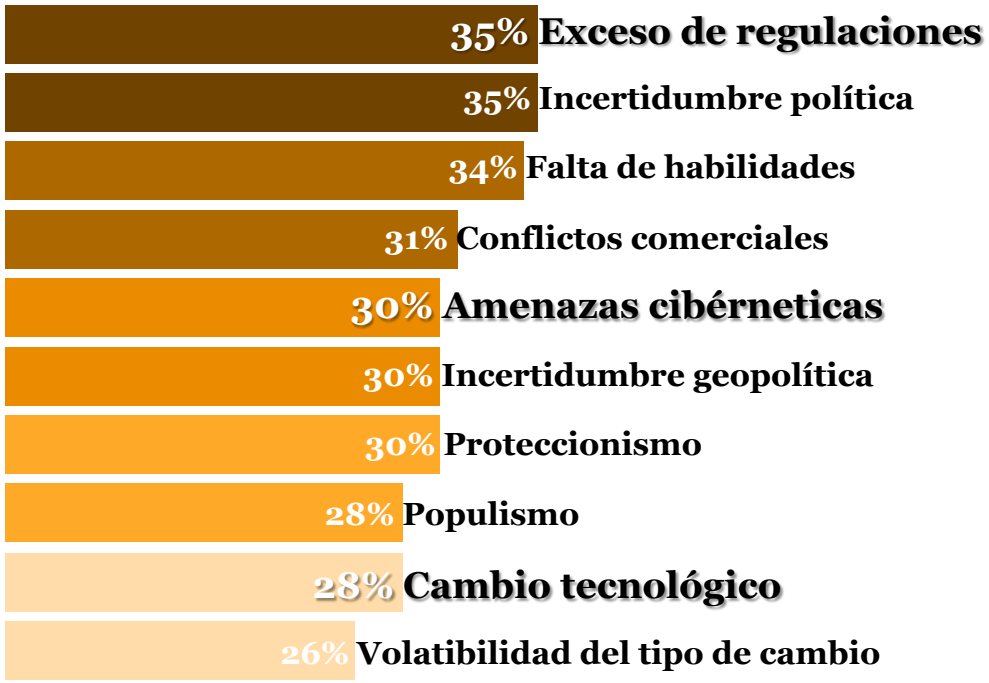
ASUGMEX

Asociación de Usuarios de SAP en México A.C.

- ***GDPR, implicaciones para el mercado mexicano***

Preocupaciones CEOs Ranking

De acuerdo al *Global CEO Survey México 2019*, actualmente los líderes de negocios en el mundo han externando sus preocupaciones, las cuales se resumen en el siguiente ***Top Ten***:



México se encuentra en el tercer lugar en el ranking de países con más ciberataques (1) a nivel mundial, sólo por detrás de Estados Unidos y Reino Unido, respectivamente. Entre los casos más importantes en el pasado, destacan, en mayo de 2017, Wannacry, con el que México se convirtió en una de las naciones más afectadas por el virus (2) y, en abril de 2018, cuando cinco entidades bancarias mexicanas fuer(3)on hackeadas a través de su plataforma SPEI. Asimismo, en los últimos días UpGuard Cyber Risk anunció que encontró expuestos públicamente en Internet un conjunto de datos almacenados por el medio mexicano Cultura Colectiva (3), los cuales contienen 540 millones de registros con comentarios, gustos, reacciones, nombres de cuentas e identificaciones de la red social Facebook.

(1) Fuente: Expansión, 9 de enero de 2019.
(2) Fuente: El Economista, 15 de mayo de 2017.
(3) Fuente: El Economista 3 abril de 2019 y El Financiero 3 de abril de 2019

Los datos como estrategia empresarial

- Saber como integrar de manera efectiva los conocimientos sobre la protección y tratamiento de datos personales en toda la empresa es un desafío importante para los CEOs.
- Las empresas recaban una gran cantidad de datos personales, por lo cual su transferencia incrementa rápidamente debido a la facilidad de la comunicación móvil y los servicios en la nube.
- *El 50% de los CEOs indican que los consumidores confían en compartir los datos personales con las empresas*
- En la actualidad, los datos personales se utilizan principalmente para mejorar partes del negocio orientadas hacia el cliente, como el servicio al cliente (el 85% de los CEOs siempre o con frecuencia utilizan los datos del cliente para mejorar este proceso), ventas (84%) y marketing (81%)
.

Los datos personales son utilizados principalmente para las siguientes funciones.

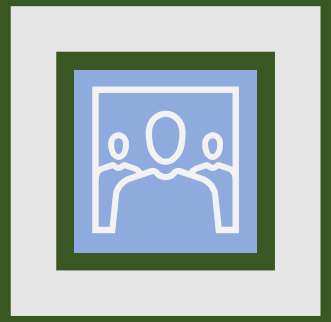
PwC CEO pulse on Data Privacy Survey

Digital Trust

Actualmente la tecnología busca resolver problemas y la vez crear experiencias únicas, por lo cual el crecimiento de los riesgos de ciberseguridad y privacidad va en aumento.

La conectividad por medio de dispositivos personales entre las personas, empresas y el gobierno incrementa día a día.

Sólo el **44%** **(53%)** de las empresas indican que las medidas proactivas de gestión de riesgos de ciberseguridad y privacidad están integradas desde el inicio ante la ejecución de algún proyecto.



96% **(91%)** compañías que implementan estrategias de transformación digital incluyen personal de seguridad y privacidad como *stakeholders.*

* pwc.com/mx/digitaltrust

Los siguientes sectores incluyen una estrategia de ciberseguridad y privacidad al inicio del proceso de transformación digital.

Servicios Financieros

66% México

63% Global

Telecomunicaciones & Tecnología

58% México

58% Global

Servicios de Salud

65% México

57% Global

Mercados de consumo

49% México

51% Global

Productos Industriales

55% México

50% Global

Energía y Minería

53% México

48% Global

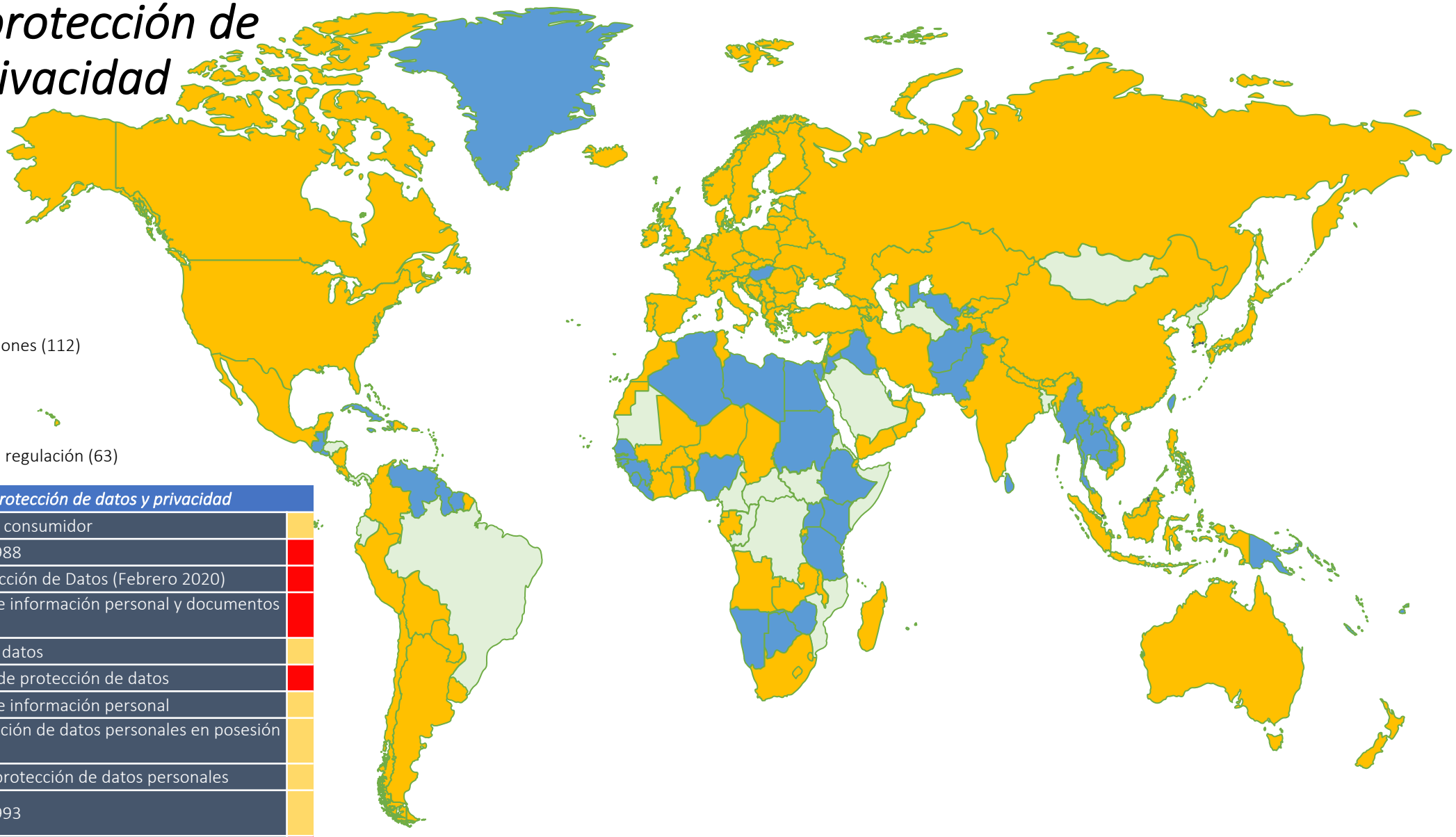
En México solo el **48%** de las organizaciones cuenta con un *CISO* en funciones

Leyes de protección de datos y privacidad

194 países

- *58%* Leyes y regulaciones (112)
- *10%* Draft (19)
- *32%* No cuentan con regulación (63)

País	*Leyes de protección de datos y privacidad*	
Argentina	Acta de protección al consumidor	
Australia	Acta de privacidad 1988	
Brasil	Ley General de Protección de Datos (Febrero 2020)	
Canadá	Acta de protección de información personal y documentos electrónicos	
China	Ley de protección de datos	
UE	Reglamento general de protección de datos	
Japón	Acta de protección de información personal	
México	Ley federal de protección de datos personales en posesión de particulares.	
Moroco	Ley No. 09-08/2009 protección de datos personales	
Nueva Zelanda	Acta de privacidad 1993	
Corea del Sur	Acta de protección de información personal	
EUA	Privacy Act.	



** United Nations Summary of Adoption of E-Commerce Legislation Worldwide*
*** DLA PIPER Data Protection Laws Of The World*

General Data Protection Regulation (GDPR)

Oficiales de protección de datos, estrategia de privacidad, gobernanza y gestión de riesgos

Evaluaciones del impacto de la protección de datos

Inventario de datos y registro de todo el procesamiento interno y de terceros

Derechos para acceder, corregir, portar, borrar y oponerse al procesamiento de sus datos

Notificación de violación de datos a reguladores y a personas cuya información este comprometida

Ene 2012

El Parlamento Europeo publica la propuesta legislativa GDPR

Dic 2015

Aprobación GDPR

Abr 2016

GDPR adoptada por la Unión Europea

2016-2017

Fase de implementación

May 2018

GDPR entra en vigor

Mar 2019

Solo un 20% de las empresas cumple en su totalidad con los requisitos de GDPR

** GLOBBIT. Your IT Channel*

Requisitos clave de GDPR

01 Inventario obligatorio de datos y mantenimiento de registros de todo el procesamiento interno y de terceros de datos personales europeos.

02 Notificación obligatoria de violación de datos a los reguladores y a los individuos cuya información se ve comprometida tras fallas en la seguridad de la información.

03 Los derechos individuales de ARCOP para acceder, corregir, portar, borrar y oponerse al procesamiento de sus datos.

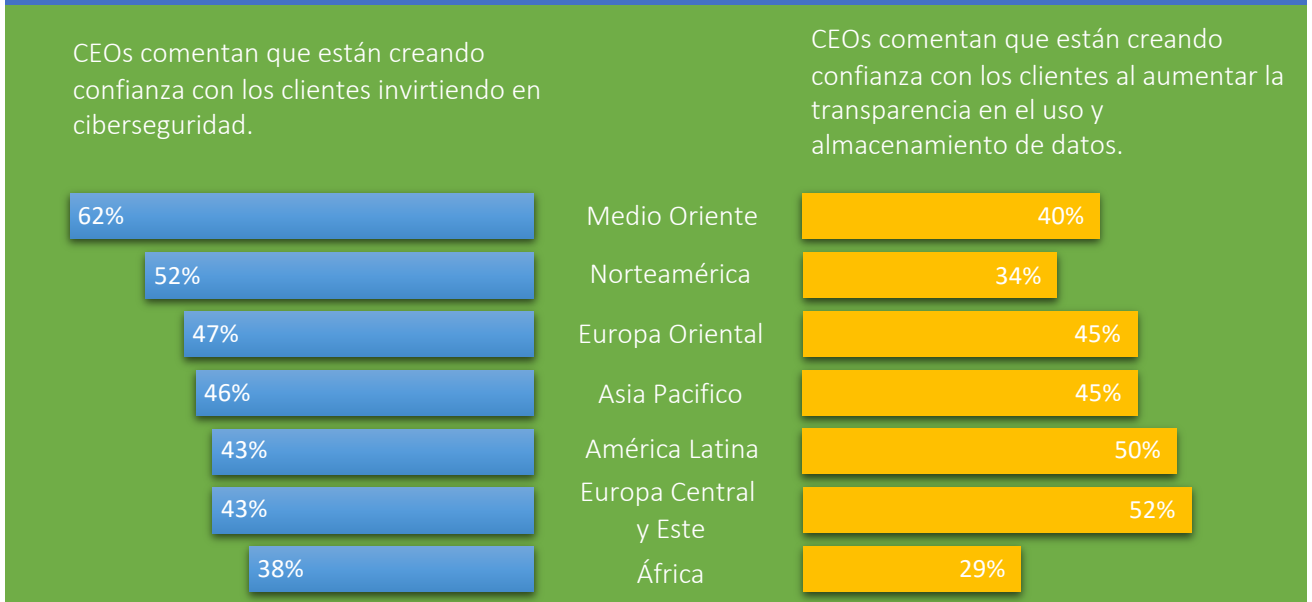
04 Evaluación rutinaria del impacto de la protección de datos para la tecnología y el cambio de negocio.

05 Funcionarios de protección de datos obligatorios y un replanteamiento general de la estrategia de privacidad, la gobernanza y la gestión de riesgos.

06 Contar con una visión de la ubicación y resguardo de los datos en servicios de cómputo en la nube, lo cual le permitirá identificar los datos almacenados y las medidas de seguridad aplicables.

El "GDPR" es la nueva ley de la Unión Europea (EU) que prevé un reglamento uniforme de protección de datos en toda la EU. Entró en vigor el 25 de Mayo de 2018 y representa el más alto estándar de protección de datos en el mundo, creando una base legal consistente, global y unificada para la protección de datos, requerida a ser aplicada por los estados miembros (EU), además de contemplar multas de hasta *20 millones de euros o 4% del ingreso total anual global del negocio* por incumplimiento o violaciones a los datos personales. EL GDPR reemplazó a la Directiva de Protección de datos de la UE existente, la cual tuvo una vigencia durante casi 20 años (desde 1998).

Los CEOs de todo el mundo cuentan con oportunidades para crecer en ciberseguridad y privacidad.



Source: PwC, 21st Global CEO Survey, 2018. Base: Middle East respondents (52): North America (148); Western Europe (274); Asia Pacific (464), Latin America (136), Central & Eastern Europe (139), Africa (80)

¿Cuándo aplica GDPR?

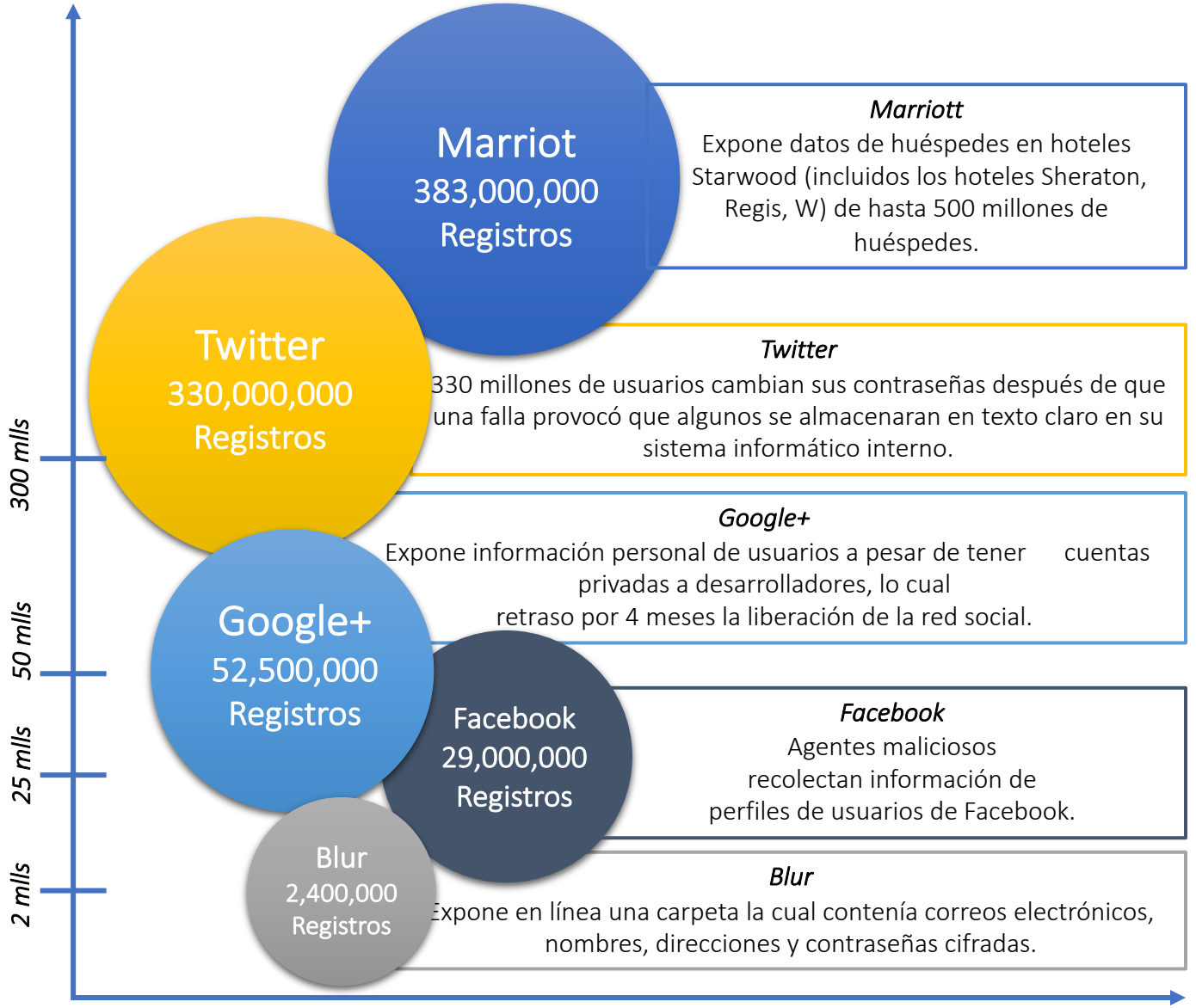
GDPR aplica si:

- ✓ Su empresa procesa datos personales y tiene su sede en la UE, independientemente del lugar donde se realice el procesamiento real de los datos;
- ✓ Su empresa está establecida fuera de la UE, pero procesa datos personales en relación con la oferta de bienes o servicios a individuos en la UE, o controla el comportamiento de los individuos dentro de la UE;

GDPR no se aplica si:

- ✓ El sujeto de datos esta muerto;
- ✓ El interesado es una persona jurídica;

Estadísticas de fuga de información y multas GDPR



https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/

Multas

1 — Google
Multa de 50 millones de euros otorgada por la autoridad francesa de protección de datos a Google ya que la empresa procesó datos personales con fines publicitarios sin una autorización válida o consentimiento del interesado.

2 — Knuddels *(Primer multa)*
Multa de 20 mil euros impuesta por Alemania, debido a una fuga en julio de 2018 de 808,000 correos electrónicos y más de 1,8 millones de nombres de usuario y contraseñas de la plataforma de chat en línea.

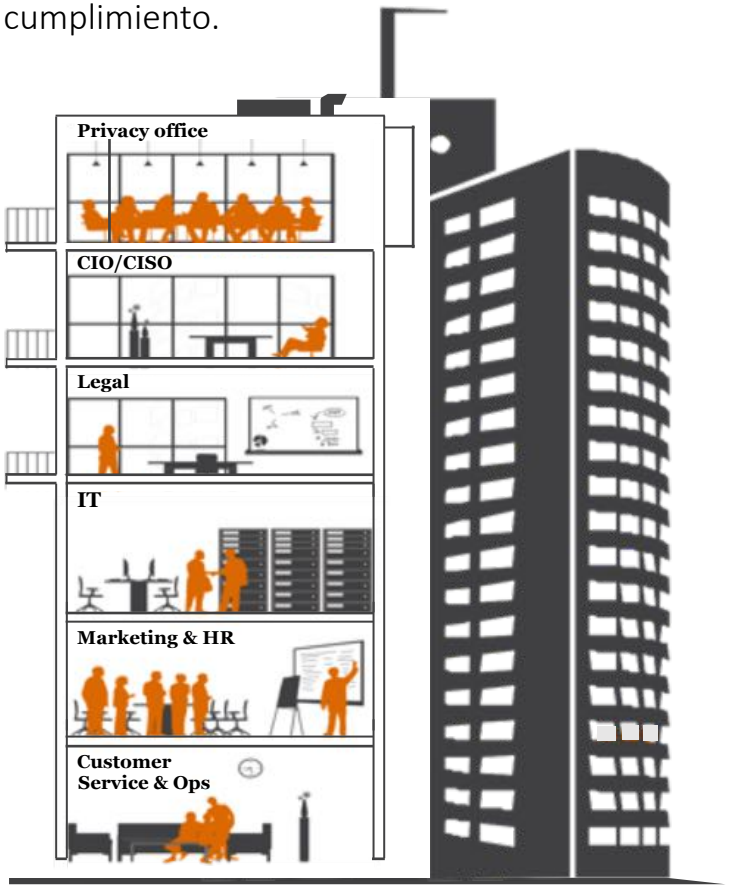
3 — Uber
Multa de 1 millón 385 mil euros por la fuga de 57 millones de usuarios e información de cuentas de 600 mil conductores.

4 — Hospital Barreiro
Multa de 400 mil euros por la violación de los principios de integridad, confidencialidad, acceso a los datos.

https://pideeco.be/articles/eu-gdpr-list-sanctions-fines-penalties-2019/

Roles para el cumplimiento de GDPR

Los requerimientos de GDPR impactan la organización entera, y necesitará un soporte funcional a lo largo de la organización, así como, actividades de remediación que sean identificadas e implementadas para su cumplimiento.



Delegado de Protección de Datos

Nombrar a un Delegado de Protección de datos (DPO) es uno de los requisitos más importantes de GDPR. Entre otras tareas, DPOs ayudan con el aviso y la transparencia al consumidor; Privacidad por diseño; y conducir las evaluaciones de impacto de privacidad (PIAs), así como a mantener actualizado el registro de actividades de tratamiento; mantener la interlocución con el regulador.

CIO/CISO

El cumplimiento de GDPR requerirá considerables recursos e inversiones. Muchos CIOs ya han incorporado este renglón a sus presupuestos. CISOs estarán encargados de promover los requisitos de seguridad para GDPR durante todo el ciclo de vida de datos; y asistir en la notificación de brechas de datos (requeridos por incumplimiento) y respuesta a incidentes.

Servicio al Cliente y Ops

Servicio al cliente y Ops pueden tener la tarea de implementar estrategias y sistemas para la remediación del cumplimiento de los derechos de acceso de clientes y empleados. Esto incluye las consultas asociadas con el "derecho a ser olvidado".

Las empresas consultarán al área legal (OGC) para ayudar en la implementación de mecanismos de transferencia de datos; registro de actividades de tratamiento, análisis objetivo de impacto en la privacidad y PIA's; definición de responsables y encargados del tratamiento de los datos; y la gestión de las cláusulas y modelos de contratos, políticas y protocolos internos; ; derechos ARCOP, análisis y regularización de las bases legitimadoras del tratamiento. El OGC también ayudará a conducir notificaciones de brechas de datos, requerido en GDPR.

Legal

Una buena parte del cumplimiento de los requisitos de portabilidad de los datos recae en IT. Además de permitir la portabilidad de los datos, colaborará en la ejecución de los derechos de acceso; autenticación; mejora del ciclo de desarrollo; y gestionar los indicadores de consentimiento y registros.

TI

Marketing y RRHH pueden ayudar a mantener el negocio conforme con los requerimientos de privacidad de empleados y clientes de GDPR, incluyendo: adherencia a las pautas de consentimiento; capacitar a los empleados en privacidad; y limitar el acceso a los datos. Marketing y RRHH también se encargarán de automatizar los procesos de toma de decisiones.

Marketing y HR

GDPR Framework

Protección de Datos

- Estrategia de Seguridad
- Recuperación ante Desastres, Continuidad del Negocio y Gestión de Respaldos

Estrategia, Gobierno y Responsabilidad

- Estrategia
- Oficial de Protección de Datos
- Gobierno
- Capacitación y Concientización

Gestión de riesgos y cumplimiento

- Supervisión de Cumplimiento Normativo
- Identificación, mitigación y Notificación de Riesgos
- Evaluación de Impacto Relativa a la Protección de Datos (DPIA)

Gestión de Riesgos de Terceros

- Transferencia Cross-Border
- Evaluación de terceros

Respuesta a Incidentes y Gestión de Brechas

- Identificación y notificación de brechas
- Respuesta a Incidentes

Derechos del Interesado y Tratamiento de Datos

- Derecho de Rectificación / Derecho al olvido
- Decisiones Automatizadas
- Retiro del Consentimiento
- Derecho de Oposición / Derechos de Limitación del tratamiento
- Derecho de Acceso
- Consentimiento
- Portabilidad de los Datos

Avisos de Privacidad y Gestión de Políticas

- Gestión de avisos de privacidad y políticas de privacidad
- Comunicación de políticas.

Ciclo de vida del dato

- Identificación y notificación de brechas
- Respuesta a Incidentes

Siguientes pasos para las compañías

"Existen muy pocas empresas que están implementando correctamente la gestión de riesgos cibernéticos y de privacidad en su transformación digital".

– Sean Joyce, PwC's US Cybersecurity and Privacy Leader

Gestión del Riesgo

La ciberseguridad, la privacidad y la confianza se entrelazan cada vez más dentro y fuera de la organización. Los CEOs deben liderar y no simplemente delegar la protección de datos y los problemas de privacidad a otros que no son totalmente responsables de dirigir el negocio y establecer el apetito de riesgo. Además, el aumento de la comunicación con la junta sobre estos asuntos debe ser una prioridad. La actualización de las estrategias de continuidad del negocio, por ejemplo, es importante para mantener el acceso a datos precisos en una crisis.

Compromiso de la Alta Dirección

Cinco preguntas que la Alta Dirección se deberá hacer sobre la privacidad de los datos:
¿Cuál es la exposición total al riesgo de privacidad de datos?
¿Qué tan efectiva es la estrategia de privacidad de datos?
¿Qué tan preparada está la compañía para proporcionar evidencia de cumplimiento a los reguladores de privacidad?
¿Los planes de la compañía para adoptar nuevas tecnologías y análisis de datos están sincronizados con las nuevas regulaciones de privacidad globales?
¿El área o departamento de privacidad de la compañía cuenta con los recursos suficientes para dar cumplimiento?

Gobierno de Datos

Las empresas deben equilibrar el uso de datos con los controles adecuados para mantener un adecuado nivel de protección de datos, además de comprender los riesgos más comunes, por ejemplo, la falta de conocimiento sobre la recopilación de datos y las actividades de retención.

GDPR, una oportunidad

Los líderes deben ver a GDPR como una oportunidad para alinear a la compañía, no sólo para el cumplimiento sino para la gestión estratégica de riesgos.

Riesgos de la regulación en el extranjero en un contexto estratégico

Las compañías se enfrentarán cada vez más la presión de gobiernos extranjeros para proporcionar acceso a propiedad intelectual. Las decisiones sobre cómo responder a tal presión deben ser informadas considerando los riesgos cibernéticos y de privacidad que podrían surgir al divulgar dicha información confidencial a funcionarios de gobiernos extranjeros.

El cumplimiento de GDPR no se trata de la tecnología, se trata de cómo se usa.

Existen casos de uso y aplicaciones compatibles con GDPR

Yonathan Parada
Socio, Cybersecurity & Privacy
PwC México
yonathan.parada@pwc.com
+81 8881 4106

asug.mx

ASUG México (empresa)

ASUG México

@ASUGMEX

contacto@asug.mx

¡Vive la #ExperienciaASUGMEX!