*Conozca las **mejores prácticas** para afrontar la Ley Federal de Protección de Datos Personales.*

IBM le brinda a su empresa un asesoramiento personalizado, poniendo en marcha las mejores prácticas para la implantación y cumplimiento de regulaciones de privacidad de datos.

Un paso más para garantizar un tratamiento seguro de tratar la información y datos personales en su compañía.
La emisión de regulaciones sobre privacidad de información (específicamente, datos personales) en la industria, ha generado implicaciones en el entorno de negocios de las organizaciones. Ahora las entidades deben velar por el cumplimiento de la normativa logrando el nivel de operación requerido.
Es importante destacar que el objeto y alcance de estas regulaciones acarrea muchos beneficios a los individuos, pero para las organizaciones que obtienen y utilizan estos datos, representan un esfuerzo adicional: deben fortalecer el esquema actual de protección de la información en tres instancias fundamentales:

a) Organización.

Implica que se definan roles y responsabilidades sobre la privacidad de los datos personales al interior de la organización. También se deben ampliar los existentes para garantizar que en el cumplimiento natural de los objetivos de cada persona, se logre consolidar una cultura de privacidad de la información.

b) Procesos.

La organización deberá desarrollar todos los procesos y procedimientos que garanticen que la infraestructura tecnológica y de seguridad de la información, esté alineada con la operación del negocio y requerimientos particulares de la normatividad de privacidad.

c) Mecanismos de protección de la información.

Los requerimientos de las regulaciones de privacidad de la información, tienen implicaciones en el marco tecnológico de control y seguridad de la información. Por esta razón, y en función de la existencia de datos personales, debe complementarse y renovarse los procesos de negocio y los recursos informáticos que los soportan.

En un sentido práctico, el desarrollo de las iniciativas para lograr el cumplimiento de las regulaciones en las empresas, puede apegarse a recomendaciones de mejores prácticas que la industria ha aplicado para el cumplimiento de estas regulaciones en diversos países.

Sin embargo, no existe una secuencia universal de actividades o factores que sean obligatorios o mandatarios.

Más allá de todo esto, IBM se basa en su experiencia en este tipo de proyectos y su modelo de privacidad global, para proponer los siguientes grupos de actividades para guiar las iniciativas mencionadas:

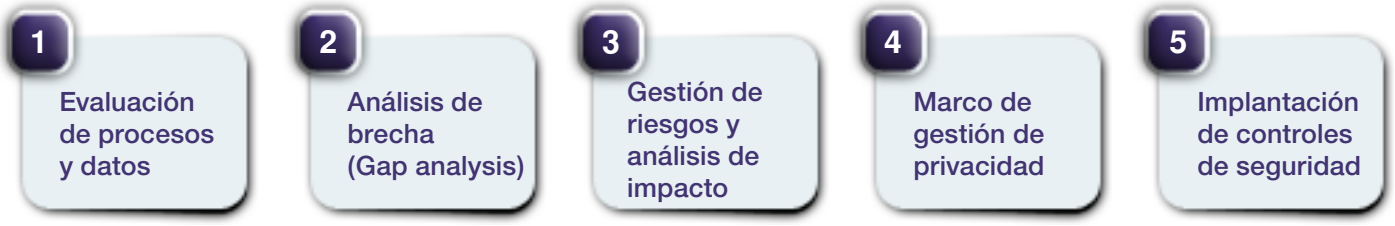
- ***Evaluación de procesos y datos.***

La organización debe obtener un mapa preciso y detallado de todos sus procesos en los que se obtienen, transmiten, utilizan, almacenan y/o procesan datos personales, así como un inventario y relaciones de los recursos de infraestructura tecnológica que soportan dichos procesos. De igual manera, deben identificarse todas las formas y mecanismos de los procesos relativos a datos personales (formatos, solicitudes, notas, papeles físicos).
En esta instancia, también es recomendable realizar una clasificación o identificación inicial de la información y/o datos encontrados en el detalle de los procesos analizados a partir de su propósito de uso.

- ***Análisis de brecha (gap analysis).***

A partir de un entendimiento mínimo de los requerimientos de las regulaciones de privacidad, la organización debe realizar una comparación de los mismos contra sus prácticas actuales de seguridad de la información, así como cada uno de los mecanismos que lo soportan, para lograr

Concientización, capacitación y entrenamiento en privacidad



Mejores prácticas para cumplimiento de regulaciones de privacidad. IBM de México. 2011.

determinar las áreas de oportunidad que deben ser atendidas y el nivel de seguridad, privacidad y operación que demande la naturaleza de su operación.

Gestión de riesgos y análisis de impacto.

La gestión de los riesgos de seguridad y el análisis de impacto permitirá a la organización establecer prioridades de protección en función de su visión y objetivos de negocio. Se deberán evaluar diferentes escenarios de afectación de los niveles de seguridad y privacidad (en la operación, legal/fiscal, económico, imagen) requeridos por la organización, para clasificar la información y seleccionar los mecanismos de control que permitan lograr el nivel de riesgo aceptable más rápido (más impacto, más probabilidades, más costo), con un sentido de negocio.

Marco de gestión de privacidad.

Se deben implantar todos los componentes normativos y de proceso que permitirán operar un modelo de privacidad en todas las actividades del negocio. Se considerará la creación del marco normativo (políticas y estándares) relativo, así como la estructura organizacional que atenderá a este esfuerzo (roles y responsabilidades, considerando la función de datos personales). Luego se considerarán los procesos y procedimientos de administración y gestión técnica. Todo esto para cumplir con los requerimientos de las regulaciones, incluyendo medición de la efectividad de esta gestión.
En el caso específico de las regulaciones mexicanas, en esta fase se debe asignar la función de Datos Personales y la publicación del aviso de privacidad a los dueños de los datos.

Implantación de controles de seguridad.

A partir de las prioridades de aseguramiento y los criterios de clasificación de los datos personales, se deben seleccionar nuevos mecanismos de protección. Para esto es necesario considerar los esquemas tecnológicos que soportan los procesos del negocio (ambientes virtualizados, usuarios móviles, esquemas tercerizados, actividades de usuarios). Así mismo se debe desarrollar un modelo integral ampliando la seguridad en la infraestructura a partir de los requerimientos de las regulaciones y las capacidades de concentrar y organizar la información en los recursos tecnológicos (recursos que puedan generar evidencia en un proceso legal o de investigación).

Concientización y capacitación.

La organización debe iniciar un proceso permanente de concientización, capacitación y entrenamiento para todo el personal interno, externo y socios de negocio. De esta forma podrá informar sobre su modelo de privacidad y los mecanismos técnicos y administrativos, optimizando sus actividades cotidianas. Es importante que este esfuerzo esté relacionado estrechamente con la estructura de reclutamiento y evaluación del desempeño del personal, con el objetivo de establecerlo como un componente de la operación segura.
La secuencia descrita, puede ser adaptada a cada negocio de acuerdo a su nivel de madurez en la gestión de la seguridad y privacidad y a sus propios requerimientos de cumplimiento y decisiones corporativas. Sin embargo, es importante destacar que este esfuerzo debe atenderse con un enfoque interdisciplinario al interior de la organización, donde al menos se encuentra la participación de las áreas: Legal, Operaciones, Recursos Humanos, Áreas Comerciales y Tecnología de la Información.
Las iniciativas que las organizaciones tomen para el cumplimiento de las regulaciones, deben enfocarse en desarrollar una cultura corporativa basada en sus valores y naturaleza de operación, evitando una visión de corto plazo o de cumplimiento aislado.
Es evidente que las regulaciones sobre la seguridad de la información y la privacidad adquieren una gran relevancia. Finalmente, este paso agrega más valor al negocio, desarrolla ventajas competitivas y aumenta la confianza de sus colaboradores, clientes

No deje en manos inexpertas el tratamiento de los datos. **IBM le ofrece las mejores prácticas** y un tratamiento personalizado para implantar un marco de seguridad de la información y privacidad de datos personales en su compañía.

Contacto:
Roque C. Juárez - Consultor de Seguridad de la Información
rjuarez@mx1.ibm.com
ibm.com/software/mx/tivoli/leyprotecciondatos/