



Asuntos relevantes sobre privacidad para 2010

Presentación

El mundo en general está enfrentando cambios y retos importantes por una transformación profunda en la forma de hacer negocios y operar organizaciones, como resultado de eventos específicos o fenómenos globales de los que hemos sido testigos en los últimos años.

Entre estos cambios está la postura que el mundo ha adoptado frente al tema de Privacidad, al que le hemos dado seguimiento con la elaboración de este análisis global desde 2001. En el estudio anterior, que publicamos en mayo de 2009, comentamos sobre la relevancia que el tema tenía para nuestro país ya que en ese entonces podían verse las primeras leyes que tocaban el tema, ejemplo específico puede ser la Ley de Protección de Datos Personales en el Distrito Federal; sin embargo, hoy la historia es distinta y afortunadamente lo es para bien.

La Constitución Política de los Estados Unidos Mexicanos fue reformada en sus artículos 6, 16 y 73 para dar al derecho a la protección de datos personales una dimensión diferente. Así, hoy este derecho ha sido elevado al nivel de garantía individual. Los cambios específicos incluyen lo siguiente:

- ▶ El artículo 6 en su fracción I, se concentra en indicar que la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal es pública, aunque muestra la siguiente precisión en su fracción II: "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes".
- ▶ El artículo 16 en su segundo párrafo especifica lo siguiente: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".
- ▶ El artículo 73 da al Congreso Mexicano a través de su fracción XXIX-O la facultad: "Para legislar en materia de protección de datos personales en posesión de particulares".

Estos elementos han constituido el marco para que hoy podamos ver dos logros significativos para el desarrollo de las medidas asociadas a la protección a la privacidad en nuestro país:

- ▶ La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental incluye en el capítulo cuarto de su título primero un apartado de protección de datos personales que está integrado por los artículos 20 al 26. En ellos se establecen los cuidados que los sujetos obligados al cumplimiento de lo allí dispuesto (los sujetos obligados son especificados en la fracción XIV del artículo 1 y se refieren prácticamente a cualquier órgano federal) deben poner en el manejo de datos personales, incluyendo además en el capítulo único de su título cuarto, la especificación de las responsabilidades y sanciones a las que un servidor público se hace acreedor al incumplir lo dispuesto en general por esta ley.

- ▶ La Ley Federal de Protección de Datos Personales en Posesión de los Particulares entró en vigencia el 6 de julio de 2010, presentando las obligaciones de los particulares (excepto las sociedades de información crediticia, que tienen su propia regulación al respecto) acerca de los cuidados que deben tener en la recolección, uso, almacenamiento, mantenimiento y desecho de datos personales. Especifica igualmente las sanciones que se aplicarán por las acciones de incumplimiento que se manifiesten.

Estas legislaciones reconocen la trascendencia de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de los ciudadanos sobre los datos personales de los que ellos son titulares y dan al derecho a la privacidad un peso que antes no tenía.

Hoy nos encontramos en el tiempo en el que el reglamento de cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares habrá de ser definido en la antesala de la posibilidad de ejercer los derechos ARCO como ciudadano, ante la oportunidad de que la efectividad de los mecanismos de seguridad de la información se vean reforzados al interior de las organizaciones como resultado de la puesta en marcha de las acciones para cumplir con una legislación que se esperaba desde hace tiempo y que hoy por fin está viendo la luz.

¿Qué hay que hacer hoy en México? Comprender la ley, estudiarla y entender la forma en la que cada organización debe definir las acciones de cumplimiento con lo allí dispuesto, hay tiempo pero no deberemos confiarnos. Con esta publicación nuestra firma procura reforzar el conocimiento necesario para poder hacer frente al cumplimiento de esta importante disposición. Próximamente compartiremos también con ustedes el desarrollo de otras iniciativas que nos permitirán tener contacto directo con nuestros amigos para incrementar nuestra aportación en la adopción de esta regulación. Nos complace incluso haber sido invitados por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), así como por diferentes y prestigiadas personalidades de la comunidad española de la protección de datos a participar en la elaboración de un compendio analítico pormenorizado que al momento ha sido titulado "La Ley Federal de Protección de Datos en Posesión de los Particulares Comentada", proyecto que se concibe con la idea de cubrir la necesidad existente del conocimiento profundo de esta normatividad y facilitar así su cumplimiento.

Esto es lo que ocurre en nuestro país; nos motiva ver el surgimiento de este tipo de regulaciones y nos honra poder ser parte de este cambio. Sin embargo, el mundo continúa viendo además de éstos otros aspectos igualmente trascendentes en torno a este tema.

Es esto lo que como firma nos lleva a poner en sus manos la edición de este año de los asuntos más relevantes en materia de privacidad a nivel mundial. Le invitamos a leerlo, revisarlo, reflexionarlo y poner en marcha las acciones necesarias para atender este tema.

Agradecemos su interés en este material. Esperamos tener en breve la oportunidad de conversar en persona con usted sobre el tema.

Ernst & Young México
Servicios de Asesoría



Antecedentes

La información constituye un elemento integral de la mayoría de los procesos de negocios; las organizaciones no pueden sobrevivir sin información y sin los sistemas de apoyo, sin los terceros y las actividades manuales para recabar, obtener, procesar, almacenar, y dejar disponible la información. Las organizaciones dependen de la información y, por consiguiente, están en riesgo cuando esta información se distorsiona. A menudo, la información impone obligaciones a las organizaciones, ya sea porque una ley o cierto reglamento requiere la información, o porque el deber fiduciario así lo exige.

El gobierno, riesgo y cumplimiento corporativo (GRCC) representa las acciones que una organización lleva a cabo para cumplir con sus objetivos de desempeño y administración de riesgos. Esto incluye los riesgos de la información y las obligaciones de la organización con respecto a la información que posee, produce, utiliza y deja disponible para terceros. Las organizaciones utilizan diferentes tipos de información: financiera, de negocios, propiedad intelectual, etc., cada uno con sus propias consideraciones sobre gobierno, riesgos y cumplimiento. Los datos personales pueden considerarse en una de dichas categorías y este documento se concentra en analizar más de cerca los riesgos de privacidad a los que éstos se exponen.

Introducción a la administración de riesgos de privacidad y cumplimiento

Este documento presenta los temas relacionados con la administración de riesgos de privacidad y cumplimiento, describe cómo deben ser atendidos integralmente para lograr una administración eficaz, establece también cómo ésta puede generar mayor valor para una organización y presenta un marco para administrar los riesgos de privacidad y cumplimiento de forma holística. El marco de privacidad permite a las organizaciones administrar los riesgos, mantener los niveles de cumplimiento y apoyar las iniciativas del negocio relacionadas con datos personales. Presentar los principales asuntos dentro del contexto del marco de privacidad permite conocer la dirección y el enfoque que las organizaciones deberían tomar para atender estos asuntos.

Asuntos relevantes sobre privacidad para 2010

Toda organización que maneja datos personales, ya sea de consumidores, clientes, empleados o socios de negocios, se enfrenta a un gran número de obligaciones relacionadas con la privacidad y protección de esa información.

Desde 2001, cuando Ernst & Young publicó su primera actualización anual sobre las inquietudes respecto a la privacidad y los principales problemas que las organizaciones enfrentarían en el año siguiente, un punto quedó claro, y es que muchos problemas persisten y no desaparecen al concluir el año. Dicho lo anterior, estos problemas cambian y se manifiestan de diferente manera para adaptarse a las circunstancias actuales de los acontecimientos. Este documento detalla dichos acontecimientos a la luz de los cambios constantes en el entorno de la privacidad y protección de datos.

Mientras que hace algunos años la privacidad era considerada como un “gancho” de mercadotecnia enfocada en las preferencias del cliente, actualmente, está asociada con la posibilidad de que ocurran abusos; es decir, acceso inapropiado o revelación de información que podría resultar en el robo de identidad y fraude. Este año hemos decidido agregar a estos alarmantes asuntos los cambios reglamentarios en todo el mundo, así como los persistentes efectos de la crisis económica.

El reto clave de la administración de riesgos y cumplimiento con respecto a los datos personales en dicho ambiente, es el gobierno del uso y la protección de esa información de manera completa y constante entre las empresas cada vez más complejas y distribuidas. Aquí es donde el marco de privacidad adquiere mayor importancia. Nos enfocamos en aquello que la organización debe hacer y que, de hecho, debe hacer bien a nivel corporativo, de unidades de negocios y afiliadas, para lograr una administración eficaz y gobierno de riesgos de privacidad y cumplimiento en toda la organización.

El marco de privacidad

Nuestro marco de privacidad explica lo que una organización debe hacer bien para administrar eficazmente los riesgos de privacidad y cumplimiento. El nivel de desempeño del negocio describe el uso de datos personales por parte de la organización en todos sus procesos de negocios y contempla la infraestructura de sistemas y terceros. El nivel de administración de riesgos y cumplimiento define la gente, los procesos y la tecnología requeridos para proteger y regular el uso de datos personales en toda la organización. En la parte superior, el nivel de gobierno define cómo todo esto debe ser administrado.

A continuación presentamos la representación gráfica de nuestro marco de privacidad, seguido de una definición de cada uno de los tres componentes que lo integran: Gobierno, Gobierno (parte alta), Desempeño a nivel del negocio (parte baja) y Administración de riesgos y Cumplimiento (parte media).



Gobierno

El nivel de gobierno define los roles y las responsabilidades requeridas para administrar el uso y la protección de datos personales a nivel corporativo y de las unidades de negocio. A menudo, el término *gobierno* puede ser considerado como la asignación formal e informal de responsabilidades, obligaciones y funciones auxiliares de las diferentes partes dentro de la organización y entre los terceros que participan en el procesamiento de la información. Asimismo, podría incluir regímenes formales de gobierno corporativo, de TI o de datos, así como procesos informales basados en la ejecución de prácticas recurrentes dentro de una unidad de negocios específica.

Desempeño a nivel del negocio

El desempeño a nivel del negocio describe cómo una organización entiende, o cómo determina dónde y cómo procesa datos personales, incluyendo la rendición de cuentas de los procesos, sistemas, bases de datos y terceros relacionados con el procesamiento de datos personales. Este nivel está compuesto de la infraestructura que proporciona datos personales a los procesos del negocio. Esto podría reflejarse en listados, bases de datos u otra información a nivel corporativo (por ejemplo: lista de aplicaciones de TI, información de proveedores del departamento de compras), y a nivel de las unidades de negocio (por ejemplo: documentación del proceso operativo).

Administración de riesgos y cumplimiento

Administración de riesgos

La administración de riesgos incluye el enfoque utilizado para manejar los temas que pueden fallar, incluyendo aquellos relacionados con privacidad en toda la organización. La función de administración de riesgos podría ser formal o informal, independiente o integrada a otras áreas de riesgo del negocio (por ejemplo: a través de un programa de administración de riesgos empresarial), a nivel corporativo, mediante un programa de administración de riesgos de TI, o a nivel de la unidad de negocio.

Cumplimiento

El cumplimiento es definido por los programas, herramientas y otros facilitadores de la organización que aseguran la observancia de políticas, reglamentos y otras obligaciones relativas al uso y protección de datos personales. A menudo, este aspecto del marco incluye las funciones de los departamentos de auditoría interna, cumplimiento, legal, seguridad de la información, el comité de auditoría y otras partes de la organización que participan en la supervisión. El cumplimiento y monitoreo pueden realizarse a nivel corporativo; sin embargo, este aspecto se refiere también a los procesos específicos de cumplimiento y monitoreo establecidos dentro de los procesos de negocio de la organización.

Políticas, procedimientos y controles

Este elemento del marco se enfoca en el cuerpo normativo de políticas existente en la organización, ya sea que se cuente con ellas a nivel corporativo, al de la unidad de negocios o ambos. Considera también procedimientos y normas relativos a la privacidad, seguridad de la información, administración de registros, uso autorizado de tecnología, administración de recursos humanos, servicio al cliente, y otras funciones relacionadas con el procesamiento de datos personales. Esto puede incluir también los procesos y controles utilizados para asegurar el cumplimiento con políticas y obligaciones, y el monitoreo de dichos procesos y controles para asegurar que se mantengan intactas y sean eficaces. Estas políticas, procedimientos o controles pueden ser administrativos, técnicos, físicos, contractuales, reglamentarios o incluso otras medidas. Pueden establecerse a nivel corporativo (por ejemplo: un proceso de autorización común, un proceso de desarrollo de productos, un ciclo de vida de desarrollo de un sistema) o específicamente a nivel de función de una unidad de negocio (por ejemplo: pasos a seguir en el proceso de contacto a clientes en mercadotecnia, controles técnicos relativos a la transferencia de información, protección física de instalaciones específicas). Con gran frecuencia, esto representa el programa de seguridad de información a nivel corporativo o de unidad de negocio y los controles de seguridad de la información específicos establecidos para el procesamiento de información (por ejemplo: a nivel de red, sistema operativo, *software* intermedio, base de datos y aplicaciones). También incluiría controles de seguridad en dispositivos y tecnología de cómputo para el usuario final, tales como en PDAs, otros dispositivos de cómputo y medios portátiles.

Administración de terceros

La administración de riesgos de terceros abarca procesos que responden por la protección de datos, incluyendo realizar un *due diligence* durante el periodo de selección, implementar controles (tanto contractuales, como para la transferencia segura de la información) y construir una base sólida confiable que asegure que los terceros que utilizan datos personales, tienen los medios para protegerlos y regular su uso. Este aspecto del marco de privacidad puede implicar procesos a nivel corporativo o de unidad de negocio en los departamentos de compras, en el área legal y en otros grupos de apoyo, junto con los procesos operativos específicos a nivel de la unidad de negocio apoyados por el tercero. Utilizamos el término *tercero* (s) de manera más generalizada que *proveedor* o *proveedor de servicios*. El término *terceros* se refiere a cualquier entidad que procese datos personales por parte de, o junto con, una organización, o con la cual la organización intercambia datos personales.

Administración de incidentes

La administración de incidentes incluye el proceso, documentado en un plan integral, que da respuesta de manera eficaz y ordenada a circunstancias actuales o posibles acontecimientos que afecten la seguridad de los datos personales, incluyendo ciertos requisitos reglamentarios relacionados, tales como una notificación de infracción. Más allá de ser sólo un programa de reacción de los equipos de seguridad de la información o de especificar las acciones para notificar la presencia de un evento inesperado, un programa de administración de incidentes efectivo debería incluir las fases de detección o descubrimiento, análisis, respuesta, escalación, reporte y remediación de un incidente.

Para cada uno de estos elementos, la organización deberá determinar no sólo qué hacer, sino cómo y hasta qué punto dicho elemento es atendido al considerar lo siguiente:

- ▶ ¿Deben formalizarse o basta con soportarlos en prácticas recurrentes? ¿Qué implicaciones trae cada una de estas opciones?
- ▶ ¿Deben integrarse uno o varios de estos elementos a otros esfuerzos de cumplimiento y/o administración de riesgos o deben de manejarse de forma independiente?
- ▶ ¿Deben administrarse y operarse estos elementos a nivel corporativo, a nivel de las unidades de negocio o al de las afiliadas?

Tomar en cuenta estas consideraciones permitirá a la organización sentar las bases para administrar la privacidad a un nivel razonable de acuerdo con los riesgos, y cumplir con las obligaciones y los procesos de cumplimiento más específicos, establecidos por los reglamentos y contratos.

Asuntos relevantes sobre privacidad para 2010

Entorno reglamentario



Los asuntos relevantes sobre privacidad para 2010 abarcan una amplia gama de temas, cada uno de ellos es atendido por los distintos elementos del marco de privacidad, según se indica en el gráfico anterior con los recuadros que hemos marcado en amarillo.

Aunque en los Estados Unidos no impera una ley general de privacidad, un conjunto de leyes federales complejas y de leyes estatales aún más complejas, regulan el uso de datos personales en diferentes industrias y contextos.

Los cambios derivados de la Ley de Tecnologías de la Información de Salud para Salud Económica y Clínica (HITECH¹, por sus siglas en inglés, que forma parte de la Ley para la Recuperación y Reinversión promulgada en febrero de 2009, ARRA², por sus siglas en inglés) aún mantienen ocupadas a muchas compañías en 2010. Esta Ley modificó la Ley de Portabilidad y Responsabilidad de Seguros Médicos³, y ha establecido ciertos requisitos que abarcan más allá de la industria de la salud al establecer las responsabilidades relativas a la protección de datos de los socios comerciales y proveedores que manejan información protegida de salud (PHI, por sus siglas en inglés) por parte de organizaciones de la salud. Otras disposiciones de la Ley HITECH ponen de relieve la existencia de ciertos requisitos de la HIPAA (Health Insurance Portability and Accountability Act) y detallan las mejoras relacionadas con su implementación. Asimismo, la Ley

1. Ley de Tecnologías de la Información de Salud para Salud Económica y Clínica (HITECH, por sus siglas en inglés)
 2. Ley de Recuperación y Reinversión Estadounidense (ARRA, por sus siglas en inglés)
 3. Ley sobre Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés)

HITECH agrega requisitos relativos a la notificación de infracción sobre información protegida de salud, que representa una nueva consideración, y que contempla más allá de las reglas de notificación de infracción existentes que se enfocaban en el robo de información financiera e identidad. El proceso de implementación, al cual las organizaciones se someterán para atender estos nuevos requisitos, continuará después de 2010 a medida que el Departamento de Salud y Servicios Humanos de los Estados Unidos (HHS, por sus siglas en inglés) y la Comisión Federal de Comercio continúen estableciendo los lineamientos y requisitos finales de las distintas disposiciones.

Fuera de los Estados Unidos, las leyes nacionales de protección de datos están bien establecidas en Europa, Canadá y en algunos países de la Cuenca del Pacífico. A pesar de que las autoridades responsables de la protección de datos han identificado la necesidad de elaborar normas de privacidad congruentes (tal como se ha especificado en el cuerpo de los Estándares Internacionales Sobre Protección de Datos y Privacidad, conocidos también como la Resolución de Madrid, emitida hace pocos meses), las leyes varían enormemente con respecto a muchos temas. Los reglamentos sobre privacidad continúan cambiando en muchos países. Los requisitos de notificación de infracción se encuentran en diferentes etapas de consideración y desarrollo en el mundo. De igual forma, otros reguladores (distintos de los comisionados de privacidad, tales como los reguladores de la industria financiera) se involucran cada vez más en hacer cumplir las reglas sobre el manejo de datos personales. Esto significa que la seguridad y protección de datos personales es generalmente un requisito sin importar dónde se guarda y a quién se le transfiere.

En el caso de México, nos encontramos hoy en el momento en el que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ha entrado en vigor con una fuerza interesante, que deriva de un enfoque renovado frente a otras legislaciones, al haber tenido la oportunidad de tomar en cuenta en su diseño las consideraciones presentadas por la Resolución de Madrid, que aglutinan experiencias tomadas en diferentes países en el tiempo, al definir sus propios modelos regulatorios de protección de datos.

Hoy es tiempo de que su organización comprenda cómo esta Ley debe ser cumplida y cómo sus procesos deben transformarse para favorecer este cumplimiento al mantener un equilibrio sano que tome ventajas de los controles derivados de esta implantación, los cuales den una fuerza competitiva al negocio de manera que le permita trascender en su ámbito de operación.

Al atender las consideraciones reglamentarias de su país en materia de protección de datos, nos permitimos preguntarle lo siguiente:

- ▶ ¿Ha revisado recientemente los cambios reglamentarios en las jurisdicciones en las que opera su negocio, y ha evaluado su cumplimiento respectivo?
- ▶ ¿Ha actualizado sus políticas para que reflejen los cambios en los reglamentos que afectan a su organización?

Administración de incidentes



La necesidad de contar con una administración eficaz y oportuna de eventos e incidentes de privacidad continúa siendo un problema fundamental para todas las organizaciones. Frecuentemente ocurren intrusiones potenciales, incluso en las organizaciones mejor administradas. En los Estados Unidos la necesidad de contar con una administración de incidentes eficaz adquiere mayor relevancia debido a los requisitos de notificación de infracción que aplican de manera más amplia. Anteriormente, un incidente daba lugar a una notificación si ciertos datos confidenciales tales como el número de seguridad social o cuenta bancaria se extraviaban o eran robados. Bajo la Ley HITECH, una notificación de infracción se emite de manera más expedita cuando la información protegida de salud, una categoría de información más extensa, es potencialmente expuesta.

En Europa, los cambios reglamentarios afectarán directamente a la industria de las telecomunicaciones; sin embargo, en Francia, los reglamentos más generalizados que afectan todas las industrias han encontrado terreno conocido, y se está implementando un régimen de requisitos de notificación de infracción más generalizado. En el caso de México, el artículo 20 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares indica que las vulneraciones que se presenten en cualquier fase del ciclo de tratamiento de datos y que afecten de forma significativa los derechos patrimoniales o morales de los titulares de los datos personales afectados, deberán informarse de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos. Las autoridades responsables de la protección de datos en general abogan por una notificación voluntaria a falta de reglas estrictas. Con estos antecedentes, queda claro que las organizaciones deberían planear cuidadosamente sus enfoques sobre administración de incidentes, incluso cuando las reglas en algunas jurisdicciones no estén establecidas de manera precisa.

Actualmente, los procesos de administración de incidentes requieren de un mayor nivel de sofisticación en las organizaciones, no sólo para determinar qué información estuvo potencialmente expuesta, sino también, en el caso de información protegida de salud, para determinar el posible impacto que esto tendrá en las personas. Por lo consiguiente, contar con procesos normales, eficaces y repetitivos para determinar la naturaleza de una eventualidad, así como los pasos a seguir, resulta esencial.

La capacitación del personal es también fundamental para que ellos sepan qué constituye un “incidente” o “eventualidad” que merezca la atención de la administración. En otros casos, reaccionar incorrectamente a eventualidades podría exponer a la organización a mayores daños que lo que merecía la situación en particular. Contar con procesos bien planeados que sean administrados por ejecutivos competentes es una obligación.

Al pensar en el establecimiento del modelo de administración de incidentes de su organización nos permitimos preguntarle:

- ▶ ¿Ha establecido procesos para administrar incidentes y eventualidades relacionados con datos personales, y para abordar los reglamentos aplicables al ámbito de operación de su organización?
- ▶ ¿Ha atendido los posibles riesgos de información mediante la implementación de procedimientos eficaces y controles para evitar que ocurran incidentes?

Computación en nube



La función tradicional de los servicios de *outsourcing* o tercerización y las empresas extendidas se amplían aún más como resultado de la creciente popularidad que ha adquirido la computación en nube, que así como otros servicios públicos de computación, pone a prueba nuestros enfoques tradicionales en la medida en que el control y la custodia de los datos personales se cede cada vez más.

En el pasado, las organizaciones quizá elegían evitar las tecnologías en nube y los posibles desafíos en cuanto a la privacidad y seguridad que éstas conllevan; sin embargo, en este clima económico, los beneficios relativos a la reducción de costos que estas soluciones brindan, han causado que muchas organizaciones reconsideren si estas tecnologías de transformación son correctas para ellas.

Existen tres modelos comunes de entrega de servicios en nube: la infraestructura como servicio (IaaS, por sus siglas en inglés), plataforma como servicio (PaaS, por sus siglas en inglés), y el *software* como servicio (SaaS, por sus siglas en inglés). Existen cuatro modalidades comunes de consumo y despliegue de servicios en nube: privada, pública, administrada e híbrida. La combinación del modelo de entrega del servicio con el modelo de despliegue de servicios, es la que define el perfil básico de riesgo de los servicios de computación en nube.

Primeramente, las organizaciones deben atender algunas de las consideraciones clave antes de contratar a un proveedor de estos servicios. La computación en nube representa un nuevo tipo de tercerización para las organizaciones que podría no encajar perfectamente en su enfoque actual de compra y administración de proveedores.

La capacidad de mantener dichos servicios bajo las actuales expectativas de protección de datos resulta clave, y deberá conservarse. Asegurarse de que las partes interesadas clave de la organización se sientan conformes con el margen de riesgo y beneficio (por ejemplo, la reducción de costos mediante la tercerización de personal, *software* y almacenamiento de información) es esencial para la adopción eficaz de dicho enfoque a largo plazo. Evidentemente, no todos los procesos ni toda la información deberán utilizar estas nuevas tecnologías; por lo tanto, la toma de decisión sobre cuáles datos se pasarán a estas nuevas soluciones es un paso que las organizaciones deben considerar cuidadosamente, sobre todo cuando existen limitantes en el nivel de supervisión y seguridad por parte del proveedor de servicios.

En el caso de México, es importante tomar en cuenta que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares dispone que quien colecta los datos personales será responsable de su protección durante todo su ciclo de vida, sin importar que en ese ciclo intervengan terceros que soporten toda o una parte del tratamiento de datos. Esto quiere decir que en caso de que los datos personales sean vulnerados, las posibles sanciones o infracciones a las que un responsable se hace acreedor, se le aplicarán a él directamente aun cuando una parte o todo el proceso de tratamiento de datos esté tercerizado. Por este motivo, las organizaciones requieren definir cláusulas contractuales que, al celebrar relaciones con terceros, les permitan estar protegidas ante la posibilidad de que se presente una vulneración causada por el proveedor.

Si piensa mandar su información a "las nubes", considere lo siguiente:

- ▶ ¿Ha realizado un inventario de sus procesos y sistemas, y evaluado cuáles de éstos serían los mejores candidatos para subirse a la nube de acuerdo con su exposición a riesgos de privacidad?
- ▶ ¿Ha considerado las implicaciones de la transferencia transfronteriza de su información en la nube?
- ▶ ¿Ha identificado qué tipo de consideraciones de privacidad y seguridad aceptaría su organización antes de subir datos personales a la nube?

Auditorías a los proveedores de servicios



Este 2010 marca un cambio importante en la manera en que los proveedores de servicios garantizarán la seguridad de sus procesos y ambientes de control a sus clientes y socios comerciales. El ahora omnipresente informe SAS 70 será sustituido por un estándar de orden internacional: ISAE 3402 (International Standard on Assurance Engagements). Este informe constituye una herramienta de aseguramiento que los auditores utilizan para soportar su revisión de procesos de negocio que pudieran afectar los estados financieros de aquellos que dependen de los mismos. Sin embargo, en los últimos años, el SAS 70 se ha convertido, indebidamente, en la herramienta de aseguramiento en la que muchas compañías han puesto su confianza, con respecto a la manera en la que sus proveedores de servicios protegen datos personales. No obstante, el cambio está por llegar y la emisión de los reportes SAS 70 pronto será sustituido. La nueva herramienta de aseguramiento ISAE 3402 permitirá la incorporación de controles cuyo alcance va más allá de asegurar

la integridad de la información financiera, de tal forma que el informe incluirá información sobre los controles de protección de datos y privacidad, entre otros.

La prevalencia del SAS 70 y la existente dependencia de este informe para las consideraciones generales en la administración de proveedores sugieren que la nueva norma de presentación de información tendrá un impacto significativo para muchas organizaciones.

Éstas reconsiderarán los tipos de auditorías que realizan y los tipos de estructuras de controles que esperan que adopten sus proveedores. El AICPA ha elaborado criterios de privacidad llamados Principios de Privacidad Generalmente Aceptados (GAPP por sus siglas en inglés). Muchas organizaciones han utilizado los GAPP para elaborar sus programas de privacidad, y algunas ya han auditado sus programas con base en dichos criterios. Lo más probable es que los GAPP sean los que se utilizarán como los criterios de protección de datos y privacidad bajo las nuevas normas de presentación de información relativa a las organizaciones de servicios.

- ▶ ¿Ha evaluado su dependencia actual de los informes SAS 70 en su proceso de administración de proveedores para fines de asegurar una mayor protección de los datos?
- ▶ ¿Ha identificado el alcance de los controles de seguridad y privacidad que desearía haber podido evaluar como parte de las auditorías que se les realizan?

Encriptación



La protección de datos personales debe aplicarse a todo el contenido, independientemente de cuál sea su ubicación actual o futuro destino. Hoy en día la encriptación de dispositivos portátiles, comunicaciones electrónicas y medios portátiles (incluidos los correos electrónicos y sus archivos adjuntos) es bastante común en diferentes regiones del mundo. Si bien esta práctica era considerada como una idea vanguardista o una práctica líder hace apenas uno o dos años, en 2010, la encriptación de datos personales almacenados y en tránsito debe ser un procedimiento operativo estándar.

En ciertos nuevos reglamentos, como los de Massachusetts y Nevada en Estados Unidos, ciertos datos personales deben ser cifrados bajo circunstancias específicas, es el caso del envío de dichos datos personales vía correo electrónico a través de Internet. Cuando no existe un requerimiento directo, bajo la mayoría de las leyes sobre notificación de infracción, la información encriptada extraviada generalmente no requiere de notificación alguna. En 2010, esta exclusión aplica también a los requerimientos de notificación de la Ley HITECH acerca de la información protegida de salud. Ésta es otra de las razones por la cuales muchas organizaciones, incluidas las que no pertenecen propiamente al sector salud, pero que manejan esta clase de información entre sus participantes, podrían optar por la encriptación en casos en que la protección deba estar garantizada.

Para muchas organizaciones, el uso de la encriptación no es una práctica nueva. De hecho ha sido un elemento básico de la protección de sistemas y procesos específicos, y ha dado lugar a una amplia gama de herramientas, tecnologías y soluciones. A pesar de su variedad, cada nueva herramienta representa un nuevo reto con respecto a la administración de claves de encriptación y tendrá limitantes técnicos respecto a su aplicación en diferentes sistemas y operaciones. Para muchas de estas organizaciones, hoy en día la meta ya no es sólo agregar la encriptación cuyo objetivo es contar con una mejor protección de los datos personales, sino que se busca el uso eficaz de esta tecnología.

La encriptación permitirá también perfeccionar y optimizar sus procedimientos y soluciones existentes, lo que implicará la identificación de herramientas específicas que deberán ser aplicadas congruentemente, que llevará incluso a cambiar la encriptación de medios portátiles de nivel de carpeta a nivel disco duro para lograr una mayor cobertura. Finalmente, las organizaciones deberán utilizar de manera menos reactiva la tecnología de encriptación basada en un enfoque de caso por caso, y más de manera holística, con mayor atención en los requerimientos de la administración de riesgos y cumplimiento de las organizaciones.

En el caso de México, la Ley Federal de Protección de Datos Personales dice en su artículo 19 que los responsables de llevar a cabo tratamientos de datos personales deben establecer medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o usos indebidos. Si bien esto no habla específicamente de encriptación y habrá que esperar a que se publique el reglamento para conocer más detalles al respecto, debe reconocerse que un mecanismo de protección que puede favorecer lo dispuesto por este artículo es precisamente la encriptación, por lo que habrá que esperar en México un incremento en el interés por este tipo de tecnologías.

Con respecto a la encriptación:

- ▶ ¿Ha identificado soluciones de encriptación para proteger las comunicaciones y los medios portátiles que contienen datos personales?
- ▶ ¿Ha identificado oportunidades de implementar dichas soluciones de manera más eficaz de modo que la encriptación sea más generalizada y a bajo costo?
- ▶ ¿Ha realizado un inventario de sus sistemas e información para identificar en dónde las soluciones de encriptación serían más eficaces para la administración de riesgos y cumplimiento?

El costo del incumplimiento



Los delitos y fraudes relacionados con datos personales son cada vez más numerosos. Dada la mayor incidencia de robos de identidad, fraudes financieros e, incluso, robos de identidad médica, los reguladores buscan y, a menudo, obtienen mayores facultades de cumplimiento de los reglamentos respectivos. En los Estados Unidos, la Ley HITECH ha aumentado drásticamente el costo del incumplimiento relacionado con la información protegida de salud. El HHS ha manifestado claramente su intención de realizar un mayor número de auditorías a las compañías después que este departamento fuera criticado en un informe general de inspección por no hacer lo suficiente al respecto. Asimismo, la Ley HITECH ahora somete a los socios comerciales al cumplimiento exigido por el HHS, ya que un número significativo de organizaciones que anteriormente estaban fuera del alcance del HHS ya están sujetas a sus reglamentos. Además, la Ley HITECH exige a la FTC y a los procuradores generales estatales asumir un papel proactivo en el cumplimiento con la seguridad y privacidad de la información de salud.

En otros países, algunos reguladores como las autoridades nacionales responsables de la protección de información y los reguladores del sector de las telecomunicaciones y finanzas han realizado más actividades de investigación, auditoría y cumplimiento. En algunas ocasiones, estas actividades son el resultado de las quejas interpuestas por parte de clientes y empleados, aunque, en otras ocasiones, forman parte de iniciativas proactivas por parte de los reguladores, muchos de los cuales han buscado obtener mayores facultades para exigir su cumplimiento y multas más altas. Por ejemplo, en el Reino Unido, el Comisionado de Información ha aumentado el nivel de vigilancia para iniciar acciones legales, y ha sido facultado para imponer multas de hasta 800 mil dólares estadounidenses por casos severos de incumplimiento a la privacidad.

2010 traerá consigo un número mayor de auditorías reglamentarias y multas que tendrán que ser pagadas por las organizaciones que no implementen controles de privacidad eficaces. El cada vez mayor número de industrias y jurisdicciones sujeto a requerimientos de notificación de infracción probablemente sea el impulso de dicho aumento. La Ley HITECH exige que las organizaciones informen los incidentes directamente al HHS o a la FTC, y algunos de los modelos legislativos de notificación de infracción incluyen dicha notificación a los reguladores como un requisito clave.

En el caso de México, si bien hoy el IFAI aún no realiza inspecciones de esta naturaleza, después del 2012 podremos comenzar a ver ejercicios de revisión en los que se confirme que las organizaciones mexicanas están cumpliendo con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Además, hay que reconocer que si bien el IFAI podría en el futuro realizar estas revisiones, en muchos casos éstas podrían originarse por un requerimiento ciudadano de protección de los derechos ARCO. Las infracciones y sanciones incluyen multas que pueden llegar a ser de montos considerables y penas carcelarias de varios años, por lo que es importante considerar con seriedad el cumplimiento con esta regulación.

Bajo expectativas de un mayor cumplimiento y multas más severas por incumplimiento:

- ▶ ¿Ha revisado su nivel de cumplimiento con respecto a los reglamentos que afectan sus operaciones en distintas jurisdicciones?
- ▶ ¿Ha actualizado sus procesos y controles para cumplir debidamente con los requisitos de cumplimiento que su organización debe atender?

Gobierno



Muchas organizaciones han establecido departamentos de privacidad para administrar sus riesgos y cumplir con sus obligaciones sobre datos personales, y no debemos perder de vista que, de acuerdo con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en México esta función debe crearse al interior de las organizaciones privadas antes del 6 de julio de 2011. En algunos casos, estos departamentos han crecido para incluir a varios profesionales de la privacidad. Debido a que el manejo eficaz de la privacidad depende de muchos profesionales en toda la organización, la red de aquellos involucrados en la protección de la información profesional, seguramente ya ha crecido y se ha formalizado con el paso del tiempo.

Los cambios en la economía y en el panorama de la administración de la privacidad afectan las consideraciones relativas al gobierno de muchas organizaciones, aunque, en algunos casos, en sentidos opuestos. Mientras que el riesgo de mal uso de los datos personales aumenta en la medida que crece el uso fraudulento de ellos, algunas organizaciones están llevando a cabo reestructuraciones y reducciones de su fuerza laboral que afecta la privacidad. Estos cambios organizacionales pueden incluir la rotación del personal del departamento de privacidad, o de modo menos directo, la modificación o eliminación de los puestos que tienen alguna función en la administración de la privacidad (p.ej. en el departamento legal, de TI o de seguridad).

A medida que las organizaciones realizan adquisiciones, los retos relativos a la administración de la privacidad se incrementan ya que la organización combinada tiene que trabajar con un alcance más amplio, con respecto a la responsabilidad de los datos personales, y optimizar el uso de información que pudiera tener diferentes compromisos asociados con la misma. Las organizaciones fusionadas representan un desafío mayor cuando existen políticas y procedimientos distintos que deben ser estandarizados.

Al adaptar su organización a estos tiempos financieros desafiantes:

- ▶ ¿Ha evaluado el impacto que genera sobre la administración de privacidad de su organización la eliminación o modificación de puestos?
- ▶ ¿Ha considerado si su departamento de privacidad está todavía estructurado adecuadamente para manejar los riesgos clave y las obligaciones de cumplimiento de su organización?

Uso de tecnología GRC



La creciente complejidad de los marcos de trabajo GRC (Governance, Risk and Compliance), incluidos aquellos diseñados para fines de la privacidad, han dado como resultado que ahora se requiere la automatización de actividades comunes de GRC, como la administración, medición y presentación de información. Normalmente, mediante el uso de herramientas de *software*, las organizaciones pueden alinear sus riesgos específicos, sus requisitos legales y reglamentarios, sus objetivos de cumplimiento, y sus estrategias de negocios a sus propios procesos y controles de negocios, con el fin de que las actividades relativas a la administración de riesgos y cumplimiento estén estructuradas y sean integrales, y que éstas no sean dejadas a la suerte. Actualmente, el software GRC listo para usar tiene un alcance limitado para cualquier organización; la personalización y configuración de estas herramientas es lo que realmente permite que una organización administre sus requisitos y actividades específicos.

Las actividades GRC comunes apropiadas para el uso de esta tecnología incluyen la identificación y administración de riesgos, organización de requisitos de cumplimiento, el mapeo de controles y de requisitos a cumplimiento de procesos de negocios específicos. También incluyen la administración de incidentes y el monitoreo y la presentación de información. El uso de las herramientas GRC puede dar lugar a actividades GRC más sólidas, reducción de costos, información más precisa, y una postura de cumplimiento reglamentario más sólida.

En 2010, un número mayor de departamentos de privacidad utilizarán las herramientas GRC para monitorear sus controles y analizar áreas específicas de riesgo y cumplimiento. A medida que el uso de las herramientas GRC se expande dentro de cualquier organización, un mayor número de áreas dedicadas a la administración de la privacidad serán monitoreadas y, en consecuencia, estas áreas presentarán mejor información sobre el avance y las deficiencias de los procesos. A medida que los otros grupos dentro de la organización responsables de desempeñar funciones de administración de privacidad integren el GRC a sus operaciones, la visibilidad del departamento de privacidad aumentará, así como se incrementa la capacidad de respuesta a problemas específicos.

Antes de integrar las herramientas GRC a sus operaciones de administración de privacidad:

- ▶ ¿Ha identificado en qué áreas pueden mejorar el monitoreo de riesgos y el cumplimiento en todas áreas operativas críticas?
- ▶ ¿Ha contemplado cómo estandarizar la elaboración de los informes y registros relacionados con el GRC en todas las operaciones y procesos?

Tecnologías de la transformación



La tecnología continúa transformando los negocios, esto no es nuevo. Sin embargo entender la nueva tecnología que está transformando los negocios es fundamental para que las organizaciones puedan cambiar la manera en que deben administrar la privacidad.

El uso de dispositivos que contienen información es cada vez más frecuente; éstos son utilizados en el trabajo y hogar, de tal manera que se han eliminado paulatinamente la división entre ambos entornos y se ha cedido el control sobre el uso de estos dispositivos y la información a los empleadores y proveedores de servicios, entre otros. Su manejo a través de redes es cada vez mayor, lo cual ha generado una mayor atención a dispositivos que anteriormente no estaban conectados. Con mayor frecuencia, éstos se vuelven “inteligentes” e interactivos.

Además de estos dispositivos, los sitios de Internet de almacenamiento de datos personales proliferan y la red también ofrece muchas nuevas modalidades que permiten la interconectividad e interacción. Esto significa que existen más datos personales en ubicaciones bajo el control de un mayor número de diferentes entidades.

Se prevé que se emitirán nuevas reglas relacionadas con técnicas y tecnologías específicas, tales como monitoreo de comportamiento y publicidad en Internet, el uso de aplicaciones de identificación de radio frecuencia (RFID por sus siglas en Inglés), y la implementación de la Smart Grid. Estas tecnologías emergentes darán lugar a requisitos reglamentarios y autoreglamentarios específicos que registrarán su implementación.

Finalmente, la computación y los servicios públicos en nube permiten contar con nuevas formas de manejar los costos y lograr mayor eficiencia en el procesamiento de información, pero a la vez lleva el resguardo y el control de datos personales más allá de los límites tradicionales. El resultado de esto es que los datos personales se almacenan o almacenarán en una variedad de objetos lógicos y físicos, y es controlada por varias entidades. Estas tecnologías no sólo han cambiado los negocios, sino quién (y qué) resguarda y controla los datos personales. Estas tecnologías han cambiado la manera en la que las organizaciones manejan la privacidad.

A medida que su organización expande el uso de las nuevas estructuras tecnológicas:

- ▶ ¿Ha determinado cómo adaptará sus procesos para la administración de riesgos sobre privacidad para responder a la pérdida de control y resguardo directo de los datos personales?
- ▶ ¿Ha atendido activamente el cumplimiento reglamentario y los impactos de los controles sobre los dispositivos móviles y la computación en nube?

Ver hacia el futuro

Estos temas no deben ser tratados como un simple ejercicio de revisión, ya que cada aspecto deberá abordarse como parte de la administración integral y deliberada del riesgo de la privacidad y cumplimiento. Fundado en el gobierno y desempeño a nivel del negocio, un programa eficaz depende de controles, monitoreo, actividades de cumplimiento y otros aspectos de aseguramiento para poder asegurar que se cuente con una operación eficaz.

La privacidad tiene un impacto en los riesgos del negocio y en el cumplimiento de cada empresa, y aún más en las entidades globales. La administración y los consejos de administración de las empresas deberán asegurarse que sus organizaciones están posicionadas adecuadamente para administrar la privacidad en toda la empresa.

En México, la segunda parte del año 2010 y el primer semestre de 2011 constituyen un periodo de trabajo intenso para definir medidas de cumplimiento con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Pareciera que el tiempo es mucho, pero el reto también es grande, por lo que el inicio inmediato es inminente.

Ernst & Young dará seguimiento a estos temas y continuará trabajando con personas como usted, que se preocupan por atender estos nuevos retos en la forma de hacer negocios.

Contactos:

Lic. Sylvia Martínez

Socia Asesoría Legal

Tel: (55) 1101 6416

sylvia.martinez@mx.ey.com

Lic. Carina Barrera

Gerente Asesoría Legal

Tel: (222) 237 9922 Ext. 2106

carina.barrera@mx.ey.com

LI Carlos Chalico

CISA, CISSP, CISM, CGEIT

Socio Asesoría en TI

Tel: (55) 1101 6414

carlos.chalico@mx.ey.com

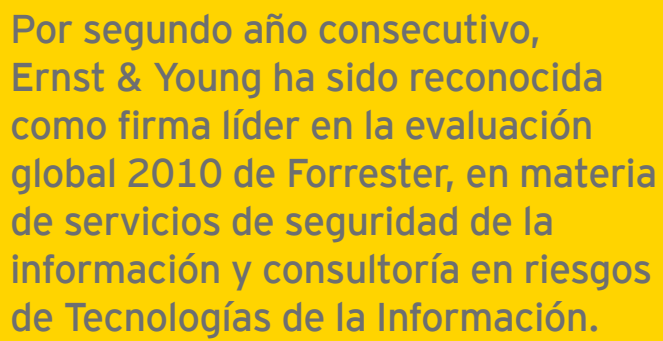
IEC Ricardo Lira

M. en C. CISSP, PMP

Gerente Senior Asesoría en TI

Tel: (55) 5283 1459

ricardo.lira@mx.ey.com



Por segundo año consecutivo, Ernst & Young ha sido reconocida como firma líder en la evaluación global 2010 de Forrester, en materia de servicios de seguridad de la información y consultoría en riesgos de Tecnologías de la Información.





Acerca de los Servicios de Asesoría de Ernst & Young

La relación entre la mejora en el desempeño y los riesgos es un reto cada vez más complejo y primordial para los negocios, ya que su desempeño está directamente relacionado con el reconocimiento y manejo eficaz del riesgo. Ya sea que su enfoque sea en la transformación del negocio o en mantener los logros, contar con los asesores adecuados puede marcar la diferencia. Nuestros 18,000 profesionales en asesoría forman una de las redes globales más extensas de cualquier organización profesional, la cual integra a equipos multidisciplinarios y experimentados que trabajan con nuestros clientes para brindarles una experiencia poderosa y de gran calidad. Utilizamos metodologías comprobadas e integrales para ayudarles a alcanzar sus prioridades estratégicas y a efectuar mejoras que sean sostenibles durante un mayor plazo. Entendemos que para alcanzar su potencial como organización requiere de servicios que respondan a sus necesidades específicas; por lo tanto, le ofrecemos una amplia experiencia en el sector y profundo conocimiento sobre el tema para aplicarlos de manera proactiva y objetiva. Nos comprometemos a medir las ganancias e identificar en dónde la estrategia está proporcionando el valor que su negocio necesita. Así es como Ernst & Young marca la diferencia.

Para mayor información por favor visite www.ey.com/mx

© 2010 Mancera, S.C.
Integrante de Ernst & Young Global
Derechos reservados
Clave ARPO01

Ernst & Young se refiere a la organización global de firmas miembro conocida como Ernst & Young Global Limited, en la que cada una de ellas actúa como una entidad legal separada. Ernst & Young Global Limited no provee servicios a clientes.

