Deloitte.

# Riesgo intensivo, valor elusivo
# Guía sobre seguridad y privacidad, dirigida al ejecutivo inteligente frente al riesgo

Serie Inteligencia de Riesgos
No. 15

# Prefacio

Esta publicación es la 15ª entrega de la serie de documentos de Deloitte sobre *Inteligencia frente al riesgo.*

La serie incluye documentos que se centran en roles (director ejecutivo jefe, junta de directores, etc.), industrias (energía, ciencias de la vida, etc.) y problemas (responsabilidad social corporativa, incertidumbre global, etc.). En www.deloitte.com/RiskIntelligence usted puede tener acceso gratis a las versiones electrónicas de todos los documentos de la serie. Para copias impresas de cortesía, contacte a su profesional de Deloitte. (Vea la información de contactos que aparece en la página 17).

La comunicación sin barreras es una característica clave de la *Risk Intelligent Enterprise*™ Empresa inteligente frente al riesgo. Considere compartir este documento con otros ejecutivos, miembros de junta y administradores clave de su organización. Los problemas que aquí se resaltan le servirán como punto de partida para el diálogo crucial para aumentar la *Inteligencia frente al riesgo* de su organización, al tiempo que fortalece su enfoque frente a la seguridad y la privacidad.

# Contenidos

# ¿Quién debe leer este documento?

Si usted es un ejecutivo que pertenece a la c-suite o es miembro de la junta de directores, ha visto reportes de medios de comunicación sobre las últimas violaciones a la seguridad o a la privacidad y se ha preguntado, “¿Podría esto ocurrirle a nosotros?,” este documento es para usted.

Si usted no es un profesional de TI pero tiene responsabilidades importantes de gobierno o de administración ejecutiva, y si usted tiene la sensación de que su organización puede no estar del todo en la parte superior de sus problemas de seguridad y privacidad, este documento es para usted.

Si usted es un ejecutivo de TI y necesita algún respaldo logístico y lógico para ayudarle a alinear el pensamiento y permitirle al resto de la organización acelerar la velocidad en lo que se refiere a seguridad y privacidad, este documento es para usted (para pasarlo personalmente a otros que se puedan beneficiar de él).

Si usted encaja en alguna de las categorías anteriores y si usted está intentando decidir si tiene sentido que su organización refuerce las cerraduras o abra la jaula de sus datos, información y activos de propiedad intelectual, este documento puede ofrecerle la clave que usted está buscando.

# Parte uno: entendiendo el presente

## Nosotros y ellos

Las personas que se encuentran en estados de hipnosis, cerca a la muerte o espirituales, algunas veces pierden su capacidad para identificar dónde termina el “yo” y dónde comienza el “no-yo.”

El mismo fenómeno puede aplicarle a su organización. Entre los acuerdos de tercerización y deslocalización, cadenas de suministro, alianzas, sociedades y otros entrelazados, ha cambiado la definición misma de empresa.

Usted puede tercerizar su nómina, recursos humanos, almacenamiento, fabricación y cumplimiento de órdenes. Al hacerlo, usted está exponiendo datos vitales, desde la información personalmente identificable de sus empleados hasta los secretos de la propiedad intelectual de sus productos.

Incluso sus clientes, en el momento de la separación, se encuentran atrapados por una crisis de identidad: usted comparte sus datos, ellos comparten los suyos.

La nueva realidad es: Ya no hay “nosotros” y “ellos”. Solamente hay “nosotros.”

Esta eliminación de las fronteras puede tener implicaciones profundas para su organización. Los datos y la información, que son las joyas de la corona de su empresa, ya no se pueden defender a la manera de un castillo rodeado de agua, con medidas de seguridad aplicadas alrededor del perímetro. Hoy, el foso se ha agotado, los muros han sido derribados y los activos están esparcidos por todo el campo.

# Migración y mutación

Con todas las clases de propiedad intelectual convertibles en unos y ceros, no es extraño que defender la empresa se haya vuelto más difícil que nunca.

La información se mueve libremente y en el camino es replicada, combinada y modificada. Cada día, innumerables terabytes de datos son transferidos desde los servidores corporativos hacia computadores portátiles, unidades USB y teléfonos inteligentes. La información es absorbida en hojas de cálculo; copiada en bases de datos; transmitida por correo electrónico. Es transmitida por mecanismos inalámbricos; migra fuera de las redes corporativas, VNP (virtual prívate network = redes virtuales privadas) y otros entornos controlados; y es almacenada – de manera apropiada y de manera inapropiada.

El riesgo puede variar, dependiendo de múltiples factores, incluyendo la posibilidad de distinguir los datos (qué tan fácilmente los datos pueden ser vinculados a un individuo particular), el contexto del uso, y su localización y acceso.

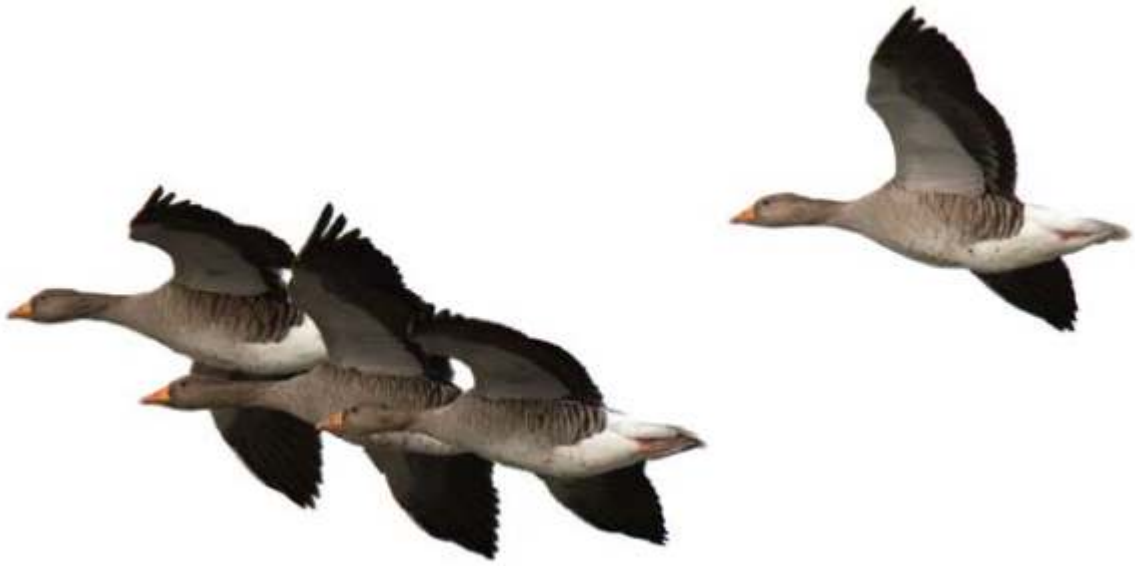
Considere, por ejemplo, la amenaza que genera la agregación de los datos. Normalmente, un solo registro contenido en un solo conjunto de datos – digamos, el nombre de una persona – conlleva poco riesgo. Pero cuando el nombre se asocia con otra parte de información – como un número de cuenta o el número de seguridad social – el nivel del riesgo crece de manera considerable.

En muchos países, las leyes y regulaciones sobre la privacidad se basan en combinaciones de datos, no en una parte aislada de datos. Las organizaciones enfrentan problemas cuando no tienen salvaguardas contra, por ejemplo, la capacidad del empleado para extraer y combinar datos provenientes de varias fuentes tales como archivo maestro de clientes, base de datos de las transacciones de cuentas, y reporte de seguro médico. Cuando ello ocurre, datos relativamente inofensivos pueden de pronto convertirse en una amenaza importante.

Datos e información: la diferencia

Si bien en este documento usamos los términos “datos” e “información” de una manera intercambiable, de hecho hay diferencia.

- Datos = técnico / nivel más bajo de abstracción
- Información = datos transformados / nivel medio de abstracción
- Conocimiento = inteligencia de negocios / nivel más alto de abstracción



# El enfoque de la mitad de los activos

En una época en la cual se supone que el conocimiento es el rey, el abuso con y el abandono de la información son las reglas del reino. Muchas organizaciones no etiquetan, identifican, hacen inventario o clasifican sus datos – o lo hacen al azar.

Imagine que su compañía compra un edificio grande de oficinas, con más del doble de espacio que se necesita para acomodar de manera cómoda a su fuerza de trabajo. Usted tiene que servir la deuda de este espacio innecesario. Usted necesita mantenerlo, asegurarlo y pagar impuestos por él. Usted no obtiene beneficio de ser propietario de espacio extra, pero usted paga generosamente por ello.

Tal medida sería pura locura, ¿verdad?

De manera sorprendente, muchas organizaciones se encuentran en una situación análoga en términos de sus datos. Nosotros postulamos que la mitad de los activos de información que las compañías mantienen y defienden no se quieren, necesitan o usan.

Esos datos superfluos conllevan un precio importante por obtención, almacenamiento y mantenimiento. Más importante aún, conllevan costos ocultos potenciales en términos de responsabilidad legal y *accountability*. Muchas compañías han pagado caro – en dinero y reputación – por el uso equivocado y la pérdida de datos que en primer lugar nunca quisieron o usaron. Considere el caso reciente que implica a una compañía global de servicios financieros: cintas de respaldo que fueron robadas contenían datos de valor marginal para la compañía – pero de valor potencialmente alto para los ladrones.

Por otro lado, muchos activos digitales que las organizaciones poseen tienen valor intrínseco. El problema es que la mayoría no conoce la diferencia.  En una época en la cual se supone que el conocimiento es el rey, el abuso con y el abandono de la información son las reglas del reino. Muchas organizaciones no etiquetan, identifican, hacen inventario o clasifican sus datos – o lo hacen al azar. Fallan en manejarlos de manera apropiada en términos de almacenamiento, administración, retención, recuperación o destrucción. No explotan su valor inherente, ni mitigan su riesgo latente. Tienen un entendimiento limitado de si lo que poseen vale la pena guardarlo y defenderlo.

En otras palabras: muchas compañías no conocen los activos que tienen en sus codos.

# La paradoja de las personas

¿Dónde se esconde más su riesgo de seguridad? Contrario a los reportes de los medios de comunicación sensacionalistas, la amenaza principal no son los hackers, los huracanes o los terroristas. Son las personas que están en su círculo de "confianza" – sus empleados y los de su empresa extendida de contratistas, clientes, socios y afiliados[1].

La amenaza no está limitada al fraude. Además, el mayor problema es relativamente mundano: sus empleados y contratistas son humanos. Y, como todos los humanos, están propensos a error y descuido, fatiga, aburrimiento y distracción. Son susceptibles a phishing y otros ataques de ingeniería social. Tal y como se observa en una encuesta reciente sobre seguridad global, realizada por Deloitte, "las infracciones son resultado tanto de comportamiento involuntario y negligente como de mala intención[2]."

Adicionalmente, algunas personas que tienen acceso al sistema de TI no entienden las restricciones, los derechos y las obligaciones que están asociados con los datos, de manera que de manera rutinaria le pasan información a otros en la organización – los cuales pueden no tener los mismos derechos a permiso – originando fuga de datos. Este fenómeno es, en esencia, un problema de "utilidad" – grandes intenciones que conducen a malos resultados.

Para ayudar a resolver el problema de las personas, muchas compañías imponen restricciones al nivel de acceso a la red de computación, bajo la premisa de que usted no puede usar mal los datos a los cuales usted no tiene acceso. Aún así las actividades rutinarias del personal de contratación, promoción y desvinculación pueden ofrecer complicaciones. Por ejemplo, cuando las personas cambian de funciones de trabajo, a menudo ganan nuevos derechos de acceso sin renunciar a sus antiguos permisos. Como resultado, quienes extienden sus cargos en la organización eventualmente acumulan privilegios amplios, carentes de monitoreo.

La encuesta de seguridad realizada por Deloitte[13] observó que el control del acceso requiere vigilancia y diligencia de la cual a veces de carece. "Si bien en la práctica la administración del acceso parece simple, en la práctica no lo es. Dadas las cambiantes responsabilidades de trabajo, la fuerza de trabajo más móvil, la rotación de los empleados, y las reorganizaciones y fusiones corporativas, esto es una tarea difícil." La encuesta adicionalmente observa que los auditores y los reguladores han mostrado interés en esta área.

En resumen: usted enfrenta la paradoja de la seguridad: las personas son, simultáneamente, su mayor activo y su mayor riesgo.

¿Dónde se esconde más su riesgo de seguridad? Contrario a los reportes de los medios de comunicación sensacionalistas, la amenaza principal no son los hackers, los huracanes o los terroristas. Son las personas que están en su círculo de "confianza" – sus empleados y los de su empresa extendida de contratistas, clientes, socios y afiliados.


[1] Para más información, vea "Building a Secure Workforce: Guard Against Insider Threat," Deloitte Development LLC, 2008. Disponible en http://www.deloitte.com/dtt/article/0,1002,sid%253D7021%2526cid%253D225950,00.html.
[2] "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. Disponible en http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html.
[3] Ibid.

# Carros de bomberos vs detectores de humo

Es tan predecible como la temporada de gripa. Cuando los medios de comunicación reportan otra violación de la seguridad o de la privacidad, los ejecutivos se motivan repentinamente. Rápidamente buscan un grupo de expertos. Piden reportes. Buscan aseguramiento. “Esto no nos puede pasar, ¿verdad?”

La respuesta corta es: “Sí, puede pasar.” De acuerdo con una encuesta reciente del Ponemon Institute[4], las violaciones a los datos le costaron a las organizaciones de los Estados Unidos un promedio de $6.65 millones por incidente en el año 2008. La investigación realizada por Deloitte en colaboración con el Ponemon Institute señala que el 32.1 por ciento de quienes respondieron reportan más de 20 incidentes por año; el 45.5 por ciento reporta más de 5 incidentes[5]; y el 5.7 por ciento reporta entre 1 y 5 incidentes. Tal y como lo sugieren los datos, los costos pueden aumentar rápidamente.

Considere, por ejemplo, la reciente pérdida de datos importantes sufrida por una compañía multinacional. Para manejar el evento, enviaron notificaciones por correo a varios millones de clientes cuya información personalmente identificable había sido comprometida; compraron varios meses de monitoreo de los reportes de crédito para cada consumidor afectado; pagaron importantes honorarios legales; y sufrieron pérdidas de clientes y erosión de la reputación que fueron incuantificables pero probablemente importantes.

Todo ello hace que la dilación y la pasividad sean difíciles de entender. La mayoría de los ejecutivos están motivados y son proactivos cuando se trata de incrementar ingresos ordinarios, atraer talento y buscar oportunidades de crecimiento. Aún así, en lo que se refiere a la seguridad y la privacidad, muchos de esos mismos ejecutivos esperan que ocurra un evento externo – sea una crisis espectacular o una regulación más rutinaria – antes de tomar acción.

Las compañías que manejan desechos peligrosos nunca contemplarían esperar un accidente antes de invertir en medidas de seguridad. Los agricultores no esperan que sus cultivos sean diezmados por insectos antes de aplicar pesticidas. Sin embargo, en relación con la seguridad y la privacidad, muchas compañías todavía llaman al carro de bomberos antes que instalar un detector de humos.

Muchos ejecutivos esperan que ocurra un evento externo – sea una crisis espectacular o una regulación más rutinaria – antes de tomar acción.

[4] Ponemon Institute, “U.S. Cost of Data Breach Study,” 2009. Disponible en www.ponemon.org.

[5] “Enterprise@Risk:2009 Privacy & Data Protection Survey,” Deloitte Development LLC, publicación pendiente.

# Parte dos: previendo el futuro

## La promesa de la era de la información

En un mundo ideal, las organizaciones y las personas disfrutan de la entrega perfecta de información de alta calidad, transmitida de manera segura dónde, cuándo y a quién la consideró valiosa y que la necesitaba. Esta red ayudaría a crear personas más informadas, más productivas, y permitiría la entrega confiada, eficiente y efectiva de productos y servicios.

Esta es la promesa de la era de la información, todavía no realizada, pero alcanzable. ¿Qué nos llevará hasta allí? Unos pocos pre-requisitos:

- Una estructura internacional que tenga en cuenta los derechos y obligaciones asociados con los activos de información.
- Implementación de las leyes, las regulaciones y los estándares de la industria, que sean apropiados.
- Enfoques efectivos y eficientes para la administración del riesgo.
- Uso eficiente de los recursos de información de la administración.
- Inventario y valuación exactos de los activos de información.
- Inversión suficiente en tecnología de la información, basada en esta valuación.
- Disponibilidad de soluciones probadas, aceptadas, que permitan la entrega segura de información.
- Mitigación y administración proactivas de las amenazas que de manera creciente son más específicas y sofisticadas.

# Parte tres: construyendo el puente

## Forje los vínculos que faltan

La política y las operaciones del día-a-día tienen que estar vinculadas de manera inextricable, mezcladas de una manera práctica. De manera creciente, los reguladores (y los juristas) no aceptarán menos.

¿Cómo algunas compañías manejan los problemas relacionados con la seguridad? De manera simple: el personal legal elabora la política de privacidad y la arroja por el travesaño. ¿Seguimiento? ¿Entrenamiento? ¿Monitoreo? A menudo ello no ocurre.

¿Cómo otras organizaciones manejan los asuntos relacionados con la seguridad? De manera similar: las vierten en el regazo del grupo de TI. ¿Colaboración? ¿Consulta? ¿Coordinación? Algunas veces simplemente no ocurren.

Esas no son fallas de intención, sino de conexión. Lo que falta es un vínculo entre las políticas y la realidad operacional. Las reglas se elaboran para satisfacer un requerimiento regulatorio o legal, prestándole poca consideración a las necesidades de negocio que tiene la organización. ¿El resultado? Políticas que no se pueden aplicar y que no se pueden hacer cumplir de manera forzosa. O, quizás peor aún, irrelevantes.

Para que sean verdaderamente efectivas, la seguridad y la privacidad tienen que trascender la elaboración de políticas y convertirse en problema de todos. Las amenazas y las oportunidades tienen que ser ampliamente entendidas; las prioridades y las responsabilidades compartidas tienen que ser comunicadas; el mensaje transmitido a los *stakeholders* hacia-arriba, hacia-abajo y a través de las organizaciones central y extendida.

La junta y los ejecutivos de nivel-*c* tienen roles cruciales por desempeñar, dado que la dirección se establece desde arriba hacia-abajo. Desafortunadamente, las tendencias recientes sugieren que en este nivel pueden estar menguando el respaldo y la participación. De acuerdo con la encuesta de seguridad realizada por Deloitte, la actual "agitación financiera ha forzado a que los ejecutivos en Norteamérica comiencen a quitarle prioridades a las iniciativas relacionadas con la seguridad…" La encuesta mostró "una caída importante en el 2008 en el número de quienes respondieron que sentían que la seguridad había subido a la administración ejecutiva y/o a la junta como un imperativo clave (63% en el 2008 versus 84% en el 2007)."[6]

Se tienen que restaurar esos vínculos perdidos. Las organizaciones no pueden solamente redactar la política y pensar que ella funciona. Más aún, la política y las operaciones del día-a-día tienen que estar vinculadas de manera inextricable, mezcladas de una manera práctica. De manera creciente, los reguladores (y los juristas) no aceptarán menos.

[6] "Protecting What Matters: The 6th Annual Global Security Survey," Deloitte Development LLC, 2009. Disponible en http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html.

# Resuelva el acertijo de la TI

Durante los últimos años, muchos departamentos de TI se han encontrado en una situación de no-ganadores en términos de seguridad y privacidad. Dos factores contribuyeron al actual acertijo:

Primero, la gente de tecnología ha sido cargada con la esparcida concepción equivocada de que la seguridad y la privacidad son principalmente un problema de TI. De acuerdo con la encuesta de Deloitte, realizada entre los principales ejecutivos de las compañías de Fortune 1000, 9 de cada 10 que respondieron expresaron este punto de vista.[7]

Segundo, TI se ve dificultada por expectativas poco realistas: dado que seguridad y privacidad son percibidas como exclusivamente un problema de TI, muchos consideran que sin ayuda TI debe aportar la solución.

Este es un punto de vista peligrosamente limitado. Imagine si pensamiento similar gobierna, digamos, el departamento de recursos humanos. En la mayoría de las compañías, las políticas y la documentación relacionadas con el empleo son manejadas por recursos humanos. Pero por necesidad logística, la supervisión del día-a-día, las evaluaciones del desempeño, las asignaciones de trabajo y otras responsabilidades tienen que ser llevadas a cabo por otros. Sin la participación de toda la organización, recursos humanos simplemente no podría funcionar de manera apropiada.

Igual ocurre con los problemas de seguridad y privacidad. En los años recientes, esta área se ha vuelto crecientemente más compleja, necesitando un enfoque multidisciplinario, que reúne varios grupos de trabajo. El CIO[8] puede asumir el rol de liderazgo, pero tiene que trabajar estrechamente con legal, cumplimiento, recursos humanos y otras funciones, así como también con las cabezas de las unidades de negocio.

En su núcleo, seguridad y privacidad es un problema de negocios, no un problema de tecnología, y si usted se focaliza principalmente en la tecnología, el progreso será laborioso. De otro modo, si usted mira a seguridad y privacidad como un problema de negocios, un problema de clientes, o un problema de *stakeholders*, entonces serán mucho más fáciles de conseguir el consenso, la colaboración y las soluciones.

[7] Ibid.
[8] CIO = Chief Information Officer = Director de información jefe. Para más información sobre el rol del CIO, vea “The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World.” Disponible en www.deloitte.com/RiskIntelligence.

# Gane visibilidad

Consiga darle luz a su información mediante el desarrollo de un inventario de datos. Iniciado antes de su próximo evento adverso, el proyecto sobre el inventario de datos puede ser completado de acuerdo con sus propios términos, sin dureza.

Esta pregunta puede no dejarle dormir en la noche – pero quizás debería: ¿Sabe usted dónde están sus datos?

Desafortunadamente, muchos ejecutivos tienen poca visibilidad respecto de los activos de información corporativos. No saben quién tiene acceso a ellos y los modifica; ni si están apropiadamente archivados y asegurados.

Estar en la oscuridad puede ser peligroso si su organización es golpeada con una demanda legal. En los Estados Unidos, reglas que fueron modificadas en el año 2006 gobiernan el descubrimiento de la información por ambos lados. Quienes litigan tienen que poner rápidamente en la mesa la lista de fuentes de información potencialmente relevante. Si su organización tiene una extensa infraestructura de TI, hacer el inventario de sus correos electrónicos, archivos compartidos, sistemas de transacción, unidades portátiles y similares, puede probar ser logísticamente imposible bajo la estrechez de tiempo ordenada por una corte.

Entonces, consiga darle luz a su información mediante el desarrollo de un inventario de datos. Iniciado antes de su próximo evento adverso, el proyecto sobre el inventario de datos puede ser completado de acuerdo con sus propios términos, sin dureza.

Y el corolario de beneficios puede ser importante. Usted puede:
- Desarrollar un entendimiento pleno de sus activos de datos
- Valorar el verdadero riesgo y el valor neto
- Fortalecer las protecciones o las restricciones perdidas, así como las garantizadas
- Mapear su inventario de activos de acuerdo con las leyes aplicables, las regulaciones y las expectativas del mercado.

Probablemente usted necesitará una persona dedicada al esfuerzo. Algunas organizaciones grandes designan un director de datos jefe (CDO = chief data officer) para que supervise la tarea.[9] Las compañías que no se pueden dar el lujo de tener un CDO pueden contar con auditoría interna, sistemas de información, o relevar a otro empleado de sus obligaciones normales.

Las metas son simples, si bien el proceso es laborioso. El equipo examinará las estructuras y las prácticas de administración de los datos; hará inventario de la información existente; valorará y asignará el riesgo y el valor. Determinará cómo usted maneja sus propios datos, así como lo hacen sus clientes y vendedores. Examinará sus prácticas de obtención y retención de datos. Responderá las preguntas: ¿Por qué estamos obteniendo este dato? ¿Qué estamos haciendo con él? ¿Estamos obteniendo información superflua o innecesaria que represente riesgo potencial sin la oportunidad de obtener recompensa?

[9] En las organizaciones más grandes la posición del director de datos jefe todavía es un relativamente rara, pero está creciendo. Para más información sobre esta tendencia, vea “The Role of the Chief Data Officer” en: http://www.deloitte.com/dtt/cda/doc/content/us_consulting_ti_roleofchiefdataofficer_250108.pdf

# Acoja la naturaleza dual de los datos

Si el título de su trabajo comienza con “jefe,” respecto de los controles a la información de su organización usted deben pensar de dos maneras:

(1) cómo aprovecharlos para crecimiento del negocio
(2) cómo evitar que dañen el negocio.

Se requiere este punto de vista bifurcado porque los datos son simultáneamente el pasivo más sobre-expuesto y el activo más sub-explotado en toda la empresa.

Su pasivo es potencialmente inmenso. Considere: ¿Quién posee sus datos? ¿Quién tiene acceso a ellos? ¿Qué controles están en funcionamiento? ¿Cuál sería el impacto en su organización si llegan a manos equivocadas? ¿Está usted gastando suficiente para mantenerlos y protegerlos?

Al mismo tiempo, los datos valiosos están invariablemente sub-apreciados. ¿En cuáles activos de datos se apoya usted? ¿Usted entiende su verdadero valor? ¿Está usted maximizando su valor en su inversión? ¿Sus esfuerzos para salvaguardarlos son proporcionales con su valor?

Esos puntos de vista opuesto crean una tensión dinámica que se tiene que resolver: entre un enfoque de Fort Knox y un enfoque de *laissez faire*; entre profesionales que buscan restricción y personas de negocio que desean liberación; entre aplastar el valor con demasiadas restricciones o despilfarrarlo con muy pocas.

Cuando las compañías se dan cuenta del verdadero valor de sus datos, su inclinación natural a menudo es defenderlos con mayor vigor. Pero la pregunta se tiene que contestar de manera franca: ¿Este dato podría tener más valor si quitamos las restricciones sobre él?

De acuerdo con nuestra experiencia, muchas compañías todavía no han conciliado el problema: están ya sea sobre-protegiendo o no-protegiendo.

Cada *stakeholder* tiene la expectativa legítima de que se maximice el valor de los datos de la organización – y cada ejecutivo tiene la clara responsabilidad de hacer que ello sea una realidad. Focalice su programa de seguridad en agregar valor a sus transacciones de negocio y a sus productos, no en agregar valor a la seguridad que los rodea.

Se requiere este punto de vista bifurcado porque los datos son simultáneamente el pasivo más sobre-expuesto y el activo más sub-explotado en toda la empresa.

# Desenrede el nudo regulatorio

A nivel conceptual, la privacidad es una noción simple. En la aplicación, sin embargo, los problemas se vuelven significativamente más complejos, especialmente cuando entran en juego consideraciones geográficas y políticas.

Tome, por ejemplo, los 50 estados de los Estados Unidos. En la colcha de retazos regulatoria en América, incidentes similares que implican la pérdida de datos de clientes puede requerir respuestas significativamente diferentes dependiendo de en cuál estado reside el consumidor afectado. Aún algo tan fundamental como la definición de PII (personally identifable information = información personalmente identificable)  varía de estado a estado.

Los estándares regionales e internacionales complican adicionalmente la descripción. Por ejemplo, ciertos países de Asia requieren que las compañías de seguros conserven físicamente los datos en el país de acogida. Como resultado, los aseguradores que operan en múltiples países de Asia tienen que mantener un centro de datos independiente en cada uno, más que consolidarlos en una instalación centralizada.

Claramente, los problemas de seguridad y privacidad constituyen un atolladero de información que se ahonda dependiendo del tamaño de su huella corporativa. Peor aún, no hay una manera simple para salir del lío.

Tradicionalmente, frente al problema las compañías han asumido un enfoque orientado exclusivamente al cumplimiento, haciendo un compromiso importante de recursos, implicando al consejero corporativo y a asesores externos, revisando las leyes y regulaciones aplicables y mapeándolas en el negocio de acuerdo con la geografía. Este método de fuerza bruta, si bien completo, puede ser costoso y consumidor de tiempo.

De manera creciente, las organizaciones están adoptando un enfoque basado-en-riesgos que mira el común de los requerimientos y luego desarrolla estrategias y programas para tomar ventaja de las similitudes, incluyendo simplificación y consolidación de los procesos. El desafío es importante, pero el esfuerzo puede prevenir que sus esfuerzos de seguridad y privacidad se vuelvan inconexos y heterogéneos.

Siga completa y conscientemente un plan en funcionamiento que cubra no solo dónde usted opera sino también donde residan sus datos. Entonces, la próxima vez que un computador portátil sea robado en Bangkok o una cinta de datos se caiga de un camión en Berlín, usted no estará esforzándose por obtener una respuesta oportuna, apropiada y legal.

# Descubra las delicias de la destrucción

Hace unas décadas, los expertos en eficiencia cantarían las alabanzas de la herramienta favorita: la cesta. (A veces llamada afectuosamente el “archivo circular.”). Hoy, la tecla de borrar y la papelera de reciclaje del computador sirven a un propósito similar.

A la máxima “las cosas suceden” podemos añadirle un corolario: “los datos se acumulan.” Crecen sin límites, de manera similar a una forma de vida independiente. La capacidad de almacenamiento siempre se las arregla para conservarlos, de manera que es improbable que sus servidores se ahoguen en ellos – pero podrían hacerlo su director de privacidad jefe, su CIO o su consejero corporativo.

Por lo tanto, ahora podría ser un tiempo oportuno para descubrir las ventajas de la destrucción. Muchas compañías se deshacen de problemas potenciales de seguridad y privacidad (y de los problemas legales relacionados) justamente limpiando la casa. Si usted no los conserva, usted no necesita asegurarlos y no tiene que preocuparse respecto de si caen en las manos equivocadas.

Si usted ha iniciado el análisis del inventario de datos que se le recomendó anteriormente, entonces usted puede tener un buen manejo de lo que es prescindible. Solicítele a su director de datos jefe o a otra persona de seguridad de la información que desarrolle la política para la destrucción de los datos. Confirme con el consejero corporativo la legalidad de sus planes propuestos para la retención y la destrucción. Cree rutinas automatizadas de purga de clases específicas de información. Luego verifique que sus planes se estén llevando a cabo de manera correcta (y continúe verificando).

Al mismo tiempo, usted no debe destruir los datos a menos que de manera clara entienda su valor para su organización. Además, el potencial requerimiento legal de conservar datos durante períodos especificados de tiempo debe ser la causa de una pausa antes de realizar la purga.

El almacenamiento es barato, pero la protección de los datos no lo es. Recuerde: la destrucción de los datos no puede ser comprometida.
(Recuerde también que la letra de borrar no siempre borra. Asegúrese de adoptar técnicas seguras de destrucción.)

# Resuelva el problema de las personas

Un cuestionario rápido: ¿Cuál organización tenía un “problema de personas”?

- ¿La ciudad americana importante que fue literalmente encerrada por un personal de TI descontento?
- ¿El banco europeo grande que sufrió una pérdida de cerca de €5 billones a manos de un vendedor pícaro?
- ¿La compañía de análisis de datos cuyos empleados fueron engañados para que revelaran información personal de cerca de 150,000 personas contenida en la base de datos de la compañía?

La respuesta, por supuesto, es todas ellas.

Sorprendentemente, en una época de mayor conciencia respecto de la seguridad, a menudo se carece de sentido común. Por ejemplo, ningún banco que se auto-respeta le daría las claves de la bóveda a un empleado nuevo de una sucursal. Sin embargo, sin pensarlo dos veces la misma institución entregará las claves virtuales de la empresa a una red o al administrador de TI, recientemente contratados.

Por supuesto, la mayoría de sus empleados son honestos, diligentes y leales. Usted puede maximizar esos atributos mediante proporcionarles entrenamiento efectivo respecto de seguridad y privacidad. Aumente la conciencia en áreas tales como seguridad de datos y manejo de actividades sospechosas. Involucre a los empleados en la refinación de los procesos y en el llenar los vacíos de seguridad. Y proporcione entrenamiento para los empleados recientemente promovidos que ahora puedan tener diferentes derechos de acceso a los datos.

Cuando se llega al entrenamiento,[10] es importante evitar la trampa de la generalidad. En los planes de estudio pueden existir algunos elementos comunes, pero la mayoría de los empleados necesitará ayuda con situaciones especializadas. Por ejemplo, el entrenamiento que necesita el cajero del banco diferirá del requerido por un banquero de inversión o por un vendedor de valores en la misma institución financiera.

Desafortunadamente, el entrenamiento representa una brecha importante en los programas de seguridad y privacidad de muchas compañías. De acuerdo con la encuesta “Enterprise@Risk” de Deloitte,[11] solamente el 35 por ciento de las compañías encuestadas ofrece anualmente entrenamiento en privacidad. El 43 por ciento lo ofrece solamente una vez durante la carrera del empleado. Mientras tanto, el 40 por ciento ofrece anualmente entrenamiento en seguridad; con el 37.5 por ciento ofreciéndolo solamente una vez durante la carrera.

Sin embargo, abordar las necesidades de su gente puede ser el paso más importante que usted puede dar. De acuerdo con la encuesta de seguridad realizada por Deloitte, “la mejor defensa de una organización contra las violaciones internas y externas… es la cultura de seguridad dentro de la organización – la manera de pensar por parte de cada individuo, de modo que las acciones en respaldo de la seguridad de la información se vuelvan automáticas e intuitivas.”[12]

**El enfoque de la aerolínea**

Considere tomar el “enfoque de la aerolínea” para la seguridad y la privacidad. En la mayoría de las aerolíneas importantes, la seguridad es la preocupación primordial, con el mensaje y el pensamiento inmersos en la cultura corporativa. Cada empleado en la aeronave, desde los asistentes de vuelo hasta el piloto, está entrenado para pensar primero en la seguridad, y cada uno de ellos entiende que una de sus obligaciones primarias es la de un “funcionario de seguridad.” Cuando un avión de US Airways hizo un aterrizaje de emergencia en el Hudson River en enero del 2009, ese alto nivel de entrenamiento se hizo dramáticamente evidente.

[10] Vea la publicación de Deloitte, “The People Dimension of Security & Privacy: Eight Training and Awareness Habits of Highly Effective Organizations,” Deloitte Development LLC, 2009. Disponible en: http://www.deloitte.com/dtt/article/0,1002,sid%253D26554%2526cid%253D266196,00.html.

[11] “Enterprise@Risk: 2009 Privacy & Data Protection Survey,” Deloitte Development LLC, publicación pendiente.

[12] “Protecting What Matters: The 6th Annual Global Security Survey,” Deloitte Development LLC, 2009. Disponible en: http://www.deloitte.com/dtt/research/0,1015,sid%253D2212%2526cid%253D245909,00.html.

# Adopte un modelo viable

¿Qué tipo de estructura debe respaldar su programa de seguridad y privacidad? Muchas compañías globales grandes adoptan un modelo federal. Emulando la estructura de gobierno, el modelo federal tiene un grupo centralizado a cargo de establecer estándares comunes y realizar funciones de coordinación, con las unidades de negocio administrando la ejecución "local."

El modelo federal es un híbrido de centralizado y descentralizado, las otras dos formas predominantes. La encuesta de seguridad realizada por Deloitte encontró que el uso de los modelos federales está en aumento, con el 22 por ciento de quienes respondieron en el 2008 (comparado con el 13 por ciento en el 2007) señalando que seguían este modelo.[13]

El modelo federal promueve la responsabilidad distribuida por los problemas de seguridad y privacidad, lo cual puede hacer que más personas se involucren y se responsabilicen por la seguridad y la protección de los activos de información. Según el modelo, la supervisión del gobierno tiene lugar a nivel de la junta; desde el nivel ejecutivo se desarrollan y despliegan herramientas, políticas y procedimientos comunes; y la propiedad del riesgo y la aplicación de las herramientas de administración del riesgo residen a nivel de la unidad de negocios.[14] El monitoreo y el hacer forzoso el cumplimiento ocurre en cada nivel del modelo.

Por supuesto, la mayoría de las compañías alinean sus programas de seguridad y privacidad con su estructura corporativa general, y es improbable que renueven su modelo de negocio únicamente para ajustarse a las preocupaciones relacionadas con seguridad y privacidad. Para una organización estrictamente centralizada y jerárquica, por ejemplo, puede no tener sentido adoptar el modelo federal. Por lo tanto, las prácticas relacionadas con seguridad y privacidad usualmente funcionan dentro de los límites de la estructura organizacional existente.

Cada modelo tiene sus fortalezas y debilidades; escoja la estructura que de mejor manera se alinee con las necesidades de su negocio. La simple existencia de una estructura de seguridad y privacidad es más importante que las particularidades del diseño.

El modelo federal promueve la responsabilidad distribuida por los problemas de seguridad y privacidad, lo cual puede hacer que más personas se involucren y se responsabilicen por la seguridad y la protección de los activos de información.

[13] Ibid.
[14] Para elaboración, vea "Putting risk in the comfort zone: Nine principles for building the Risk Intelligent EnterpriseTM", en: www.deloitte.com/RiskIntelligence.

# Un poco de comida para llevar

Si bien ciertos problemas de seguridad y privacidad se pueden resolver con cifrados, claves fuertes o reingeniería de procesos, tales pasos son tácticas y no se deben confundir con la estrategia de negocios

Alguna comida para llevar, relacionada con seguridad y privacidad:

- Es difícil restringir el acceso si usted en primer lugar no controla.
- Tanto en moda como en seguridad, “un tamaño se ajusta a todo” raramente funciona.
- Su mayor desafío puede estar en asegurar la inversión antes que la catástrofe golpee. (Naturalmente, luego que surge el problema los fondos fluyen libremente.) Por lo tanto, explique el problema en términos de negocio – no en términos técnicos – a quienes controlan los cordones de la bolsa.
- Cualesquiera horas que usted gaste documentando el ROI de sus programas de seguridad y privacidad será tiempo bien gastado.
- Cambiar las prioridades – a nivel organizacional, pero también su mismo programa de seguridad y privacidad – puede menoscabar sus objetivos. Asegúrese que tiene un *CIO inteligente frente al riesgo*,[15] que tenga una silla en la mesa ejecutiva.
- Cambie su manera de pensar respecto de los roles y las responsabilidades; ya no se trata de departamentos y divisiones; se trata que pueden y que no pueden hacer las personas con los activos de información.
- No acepte alegremente que terceros traspasen los datos. Limite su responsabilidad aceptando solamente los datos que usted quiere y necesita.
- Los datos deben ser tratados como un activo – con su valor, riesgos y ROI esperado identificados, y con recursos aplicados de acuerdo con ello.
- Viva en el presente y anticípese al futuro. Las amenazas evolucionan de manera continua. Las amenazas de ayer no necesariamente serán las del mañana.
- Considere la demografía de los empleados. La generación Y lleva al trabajo a una persona digital, junto con sus teléfonos inteligentes y sus reproductores de MP3 que pueden almacenar cientos de gigabites. Sus capacidades de correo electrónico y mensaje de texto, basadas en la red, pueden eludir las salvaguardas de la seguridad. Sus blogs y sus anuncios en Facebook pueden contener información sensible o desconcertante.
- Adopte una buena perspectiva de conjunto. La seguridad y la privacidad son un problema de negocios complejo. Si bien ciertos problemas de seguridad y privacidad se pueden resolver con cifrados, claves fuertes o reingeniería de procesos, tales pasos son tácticas y no se deben confundir con la estrategia de negocios.
- Evite el enfoque minimalista. Considere cuáles salvaguardas se necesita tener en funcionamiento, más que las mínimas que usted puede conseguir. Trate la seguridad y la privacidad como si se tratara de la salud y seguridad en una industria peligrosa – tome precauciones mayores.
- No piense respecto de la seguridad y la privacidad como un proyecto con un comienzo y un final. Tiene que ser un proceso sostenido, disciplinado, metódico. Comprende no solo políticas y procedimientos, sino también presupuestación, entrenamiento, implementación técnica, monitoreo, cumplimiento y gobierno.

[15] Vea “The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World,” en: www.deloitte.com/RiskIntelligence.

# Contactos

**Contactos en los Estados Unidos**


**Ted DeZabala**
Managing Principal
Security & Privacy Services
Deloitte & Touche LLP
+1 212 436 2957
tdezabala@deloitte.com

**Rena Mears**
Partner
Security & Privacy Services
Deloitte & Touche LLP
+1 415 783 5662
renamears@deloitte.com

**Henry Ristuccia**
Managing Partner
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

**Bruce Murphy**
Principal
Deloitt e & Touche LLP
+1 973 602 6020
brmurphy@deloitte.com

**Bill Kobel**
Principal
Security & Privacy Services
Deloitte & Touche LLP
+1 214 840 7120
bkobel@deloitte.com


**Contactos internacionales**


**Adel Melek**
Partner, Global Leader
Security & Privacy Services
Deloitte Canada
+1 416 601 6524
amelek@deloitte.ca

**Simon Owen**
Lead Partner
ERS - Information & Technology Risk
Deloitte United Kingdom
+44 20 7303 7219
sxowen@deloitte.com


Mediante el desarrollo de estrategias de seguridad y privacidad, Deloitte le ayuda a sus clientes a:

- liberar el valor de la información
- proteger los activos de información que sean críticos para la entrega de productos y servicios
- establecer y mantener relaciones de negocio basadas en la confianza
- aprovechar eficiente y efectivamente los recursos de administración de la información.

Para la discusión de sus problemas de negocio o para más información sobre nuestros servicios, contacte a cualquiera de los profesionales que se listan arriba.

Esta es una traducción al español de la versión oficial en inglés de **Intensive risk, elusive value. A Risk Intelligent executive's guide to security and privacy – *Risk Intelligence Series Issue No. 15***, publicada por Deloitte Development LLC, 2009. Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

Deloitte se refiere a Deloitte Touche Tohmatsu -asociación suiza- y a su red de firmas miembro, cada una como una entidad única e independiente. Deloitte presta servicios profesionales en auditoría, impuestos, consultoría y asesoramiento financiero a organizaciones públicas y privadas de diversas industrias. Con una red global de firmas miembro en 140 países, Deloitte brinda su experiencia y profesionalismo de clase mundial para ayudar a sus clientes a alcanzar el éxito desde cualquier lugar del mundo en el que éstos operen.

Los 168.000 profesionales de la firma están comprometidos con la visión de ser modelo de excelencia; están unidos por una cultura de cooperación basada en la integridad y el valor excepcional a los clientes y mercados, en el compromiso mutuo y en la fortaleza de la diversidad. Disfrutan de un ambiente de aprendizaje continuo, experiencias retadoras y oportunidades de lograr una carrera en Deloitte. Sus profesionales están dedicados al fortalecimiento de la responsabilidad empresarial, a la construcción de la confianza y al logro de un impacto positivo en sus comunidades.