Seguridad de la información y privacidad: dos conceptos convergentes

En un mundo interconectado, de información instantánea y servicios en la nube, la sobrecarga de información y la pérdida de privacidad son amenazas inminentes. De ahí que el contenido de esta edición contemple los asuntos más relevantes de ese panorama, a través de las distintas especialidades de los colaboradores. Uno de los temas de mayor alcance es la XII Encuesta Nacional de Seguridad Informática que muestra las tendencias 2011-2012 en Colombia.

Jeimy J. Cano, Ph.D, CFE

En ese contexto, el concepto de privacidad y las tensiones naturales con las exigencias corporativas son elementos que requieren analizarse, para reconocer los límites y balances que deben existir, orientados a mantener una coexistencia para asegurar un adecuado manejo de la información, además de mantener y fortalecer un cuidado estricto sobre la información personal.

Algunos estudios internacionales, entre ellos el de Ernst and Young 2012, señalan que la administración de la privacidad en las organizaciones, se encuentra influenciada al menos por tres elementos claves: el fraude, la economía y las regulaciones. El fraude, generalmente materializado a través de múltiples individuos o eventos, con acceso a información personal con propósitos criminales, políticos o de monitoreo; es una tendencia que revela la fragilidad interna de las empresas frente a los estándares de ética, los valores personales y la cultura corporativa.

De otra parte, la economía internacional, como aspecto complementario al anterior, propone un ambiente de incertidumbre, de inestabilidad, que confronta la seguridad financiera y valores personales atentando contra el balance natural de las necesidades humanas, es otro detonador que revela la necesidad de acceso a información para mantener el seguimiento de los hábitos financieros de los individuos.

Finalmente, las regulaciones que como menciona el estudio *Ernst and Young* son un ejercicio de nunca terminar, demandan un esfuerzo importante por parte de las empresas,

para mantener un ambiente de control conocido y confiable, que permita generar la confianza requerida tanto para la empresa en su relación con los inversionistas, como para los individuos en el contexto del manejo de sus datos.

Así las cosas y como quiera que esta realidad de la privacidad y la seguridad de la información de las personas son un reto propio de una sociedad de la información y el conocimiento, es imperioso encontrar referentes, experiencias y buenas prácticas que nos permitan abordar y sintonizar las garantías constitucionales de los ciudadanos, con las posibilidades y necesidades de los estados para potenciar sus capacidades de seguridad y control.

Privacidad de los datos

Entrar en los terrenos de la privacidad es reconocer los derechos y deberes que los ciudadanos tienen respecto de la información personal. En este sentido, el NIST – *National Institute of Standard and Technology* (2010) define la información de identificación personal (PII – *Personal Identifiable Information*) como "(…) cualquier información acerca de un individuo gestionada por una agencia, incluyendo (1) cualquier información que pueda ser usada para distinguir o seguir la identidad de un individuo, como puede ser su nombre, número de seguro social, fecha y lugar de nacimiento, apellido de la madre o registros biométricos; y (2) cualquier otra información que vincule o asocie a un individuo, como puede ser información médica, educacional, financiera y laboral."

Esta definición establece con claridad la exigencia que cualquier empresa tiene con el manejo y uso de la información, frente a las garantías constitucionales que cada ciudadano tiene, con respecto a su información. Esto es, que cada organización debe atender no sólo las exigencias regulatorias respecto a la información personal, sino desarrollar los mecanismos y estrategias que permitan su adecuada administración, lo que generalmente incluye aspectos como su recolección, uso, procesamiento, almacenamiento y revelación.

Si bien, en el mundo existen diferentes iniciativas relacionadas con la protección de los datos personales, es claro que las organizaciones y los estados están recientemente tomando atenta nota sobre estas consideraciones. El estudio de tendencias en privacidad realizado por la empresa de consultoría antes mencionada (ERNST AND YOUNG 2012), establece que el 73% de las empresas entienden claramente las regulaciones relativas a la privacidad y sus impactos a nivel corporativo; sin embargo, sólo un 30% tiene implementados mecanismos reales que permitan monitorear y mantener los controles relacionados con la privacidad de los datos.

Ante el escenario jurídico colombiano la Corte Constitucional ha venido consolidando jurisprudencia sobre el tema por más de 10 años, lo cual establece el desarrollo de un derecho fundamental denominado *hábeas data*. Dicho derecho, es un reconocimiento de la autodeterminación informática de las personas, cuyo eje fundamental está asociado con conocer, rectificar y actualizar la información del titular en cualquier medio o condición que se encuentre la misma.

Como quiera que la privacidad es un derecho fundamental y que su protección depende de un ejercicio razonable de prácticas de seguridad y control que permita su adecuado tratamiento, es necesario identificar todos aquellos sitios o fuentes donde se pueda tener información de carácter personal, para establecer el marco general de cumplimiento requerido que asegure el compromiso de la gerencia frente a esta realidad.

Seguridad de los datos

De acuerdo con SHAW (2011, págs. 2 y 3) los ejecutivos globales necesitan conocer:

- Las fases y entregables del ciclo de vida de la privacidad y la seguridad de la información.
- Conocer los riesgos e impactos relacionados con la seguridad de la información y la privacidad.
- Las razones fundamentales referentes a la protección de los datos.
- Los costos y otros impactos de las brechas de seguridad y la subsecuente pérdida y revelación de información.
- La relación existente entre seguridad de la información y privacidad.

En este contexto, los ejecutivos corporativos caminan sobre aguas desconocidas, toda vez

que aunque conocen la existencia de mecanismos y prácticas relacionados con la protección de la información empresarial, cuentan con pocos detalles del estado de las mismas y sus impactos frente a la confianza, reputación y relacionamiento internacional con sus socios de negocio.

En consecuencia, SHAW propone un ciclo de vida para la privacidad y la seguridad de la información, como una forma de establecer un tenor concreto de las responsabilidades, exigencias y cumplimiento que las organizaciones deben considerar cuando de atender las obligaciones, riesgos y tratamiento de la información se requiere; no sólo para verificar que se consideran las regulaciones del caso, sino para comprender que tanto la seguridad como la privacidad son disciplinas complementarias, que hacen de su aplicación una forma de elevar la confianza de los grupos de interés frente a sus intereses empresariales.

El ciclo propuesto establece cinco pasos:

1. *Identificar y revisar los estatutos y regulaciones aplicables a la organización*
   Este primer paso demanda que las organizaciones cuenten con un observatorio permanente de regulaciones y leyes de cada una de las regiones o sectores donde opera la empresa, de tal forma que desarrolle un diagnóstico concreto sobre las condiciones actuales de su cumplimiento frente a las prácticas corporativas respecto del tema.

2. *Identificar y analizar las fuentes potenciales de responsabilidad*
   Esta fase pretende que la organización establezca un análisis exhaustivo de activos de información existente, que permita determinar el alcance de las responsabilidades y el ejercicio de controles requerido por la empresa. Esta identificación pasa por el análisis de hardware, software, aplicaciones (am-bientes de pruebas, calidad y producción), redes y facilidades que las empresas utilizan para la transmisión de datos, propietarios y custodios de información.

3. *Aplicación de políticas y valoraciones de riesgos*
   Por un lado esta etapa busca revelar las políticas de seguridad y control de la organización y cómo estas son aplicadas y verificadas en el contexto del inventario de activos de información previamente identificado. De igual forma, este marco de actuación frente a la protección de la información debe contar con un tono claro de la gerencia, que imprima la relevancia del tema en las agendas estratégicas de los ejecutivos de primer nivel, así como en la cultura de sus empleados. Así mismo, las valoraciones de riesgo deben mantener una vista integrada del nivel de exposición de la organización frente a eventos de falla parcial o total, con el fin de mantener una postura proactiva frente a las amenazas y vulnerabilidades que puedan afectar el modelo de generación de valor del negocio.

4. *Diseño, aplicación y validación de los controles de seguridad y privacidad de la información*
   Una vez identificados los riesgos y sus impactos sobre los activos de información relevantes para la empresa, es necesario identificar o diseñar las medidas de mitigación de los mismos y asegurar la efectividad de éstas. En particular, se cuentan con listas de controles generalmente aceptados en documentos como:

   - NIST *Special publication 800-53. Recommended security controls for Federal Information Systems and Organizations*
   - ISO 27002
   - COBIT de ISACA.

   En particular, en esta etapa se requiere una especial coordinación entre los objetivos de los controles seleccionados, de tal forma que se ajusten tanto a las necesidades de privacidad como a las de seguridad, de manera que el mínimo de controles aplicados ofrezcan una vista estandarizada, confiable y verificable del ambiente de control requerido para los datos claves de la empresa.

5. *Asegurar el cumplimiento, los procesos de auditoría y certificación*
   Una vez implementados el conjunto mínimo de controles y su uso en la operación diaria de la empresa, éstos deben ser monitoreados y verificados frente a los objetivos

de seguridad y privacidad de la empresa, así como de los requisitos legales de cumplimiento normativo nacional o internacional. Para ello, esta fase exige un seguimiento y reporte periódico de monitoreo interno de la efectividad de los controles, sin perjuicio de evaluaciones y auditoría externas que se planteen por parte de entes de supervisión y vigilancia para conocer el estado de modelo de seguridad, control y privacidad de la organización.

Si las organizaciones toman este ciclo y lo incorporan como un ejercicio sistemático propio y relevante para los objetivos de negocio de la empresa, habrá menos sorpresas en el futuro inmediato frente a incidentes que afecten la reputación y los planes estratégicos de la empresa, generando un ambiente propicio para consolidar relaciones de confianza con inversionistas y terceros interesados que confirmen como anota GAFF y SMEDINGHOFF (2012), que "la seguridad de la información ya no es solamente una buena práctica de negocio, sino un requerimiento legal".

Algunas consideraciones jurídicas acerca de la privacidad y seguridad de los datos

Considerando los altos costos que implican las brechas de seguridad y la revelación de información sensible, es necesario que las organizaciones adelanten medidas adecuadas y razonables para asegurar el debido cuidado sobre el tratamiento de la información, tanto en medios digitales como físicos. En este sentido, se extienden obligaciones legales que las empresas deben atender, so pena de enfrentarse a demandas o sanciones que impacten su flujo de caja, reputación o posición preferente en un sector de la economía.

Por tanto, afirma SHAW (pág.16, 2011) que para el desarrollo de un debido cuidado en la protección de la información en las empresas modernas se requiere un esfuerzo multidisciplinario conjunto, con el concurso de al menos tres grupos de profesionales:

- Profesionales de la seguridad de la información para evaluar los impactos relevantes de las amenazas y vulnerabilidades de la información.
- Profesionales en tecnologías de información, para implementar las soluciones adecuadas en los ambientes técnicos establecidos.
- Profesionales de las ciencias jurídicas para analizar y recomendar frente a las obligaciones legales y contractuales, así como de los aspectos de cumplimiento requeridos frente a ordenamientos nacionales e internacionales.

En consecuencia, no podemos comprender el fenómeno de la privacidad sólo desde la perspectiva técnica, sino como un referente holístico que, a partir de la esfera personalísima del individuo, es capaz de extenderse y reclamar su protección, a través de diversos ambientes empresariales, para conducir el cumplimiento legal de un derecho que es tan antiguo y tan nuevo como la humanidad.

Habida cuenta de lo anteriormente detallado, la Corte Constitucional de Colombia, ha venido ilustrando su punto de vista y consideraciones al respecto donde establece su posición frente a la información reservada como se advierte en la sentencia c-334 de 2010:

"*La información reservada es aquella que sólo interesa al titular en razón a que está estrechamente relacionada con la protección de sus derechos a la dignidad humana, la intimidad y la libertad; como es el caso de los datos sobre la preferencia sexual de las personas, su credo ideológico o político, su información genética, sus hábitos, etc. Estos datos, que han sido agrupados por la jurisprudencia bajo la categoría de "información sensible", no son susceptibles de acceso por parte de terceros, salvo que se trate en una situación excepcional, en la que el dato reservado constituya un elemento probatorio pertinente y conducente dentro de una investigación penal y que, a su vez, esté directamente relacionado con el objeto de la investigación. (…)*"

En atención al concepto previo y considerando que legalmente tenemos una definición concreta de lo que se debe entender por información sensible, los responsables de la seguridad de la información deben señalar con claridad este tipo de información en los análisis de riesgos que se adelanten frente al riesgo de pérdida y/o fuga de información, conociendo los impactos legales que pueden enfrentar las empresas, teniendo en cuenta que no sólo se

está en presencia de una brecha o incidente de seguridad de la información, sino frente a la vulneración de un derecho constitucional que define un bien jurídico que el Estado desea proteger como lo es la dignidad, el buen nombre o la privacidad, como garantía constitucional de los ciudadanos.

Reflexiones finales

Cuando desarrollamos modelos de seguridad de la información en las organizaciones, la identificación de activos de información se adelanta alrededor de aquellos objetos claves de negocio, con el fin de entender la generación de valor de la empresa y cómo protegerlo, pero por lo general, no toma en consideración elementos propios de las obligaciones legales propias de la información, sino sólo aquellas que le son pertinentes para sus relaciones con los socios del negocio.

Esta postura algo desafiante y arriesgada, ignora la relevancia constitucional que el tema tiene y la necesidad formal que el Estado requiere para dar cuenta de derechos fundamentales que los ciudadanos tienen respecto de su información. En este sentido, la Corte Constitucional Colombiana en su sentencia c-1011 de 2008 confirma nuevamente el derecho de hábeas data "*como aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales.(…)*" lo que inmediatamente amplía el espectro de actuación del modelo de seguridad de la información y sus prácticas, para dar cum-plimiento a las expectativas naturales de las personas frente a la privacidad a su información.

En este sentido, cuando hablemos de seguridad de la información o privacidad, no debe existir una separación de prácticas en el tratamiento de la información, sino el reconocimiento de una vista convergente entre derechos y principios de protección, que buscan establecer un referente natural de confesión de deberes y derechos de los individuos frente a la recolección, uso, retención, transferencia y disposición final de la información. Esto es, construir un marco general de controles mínimos que permitan darle tranquilidad a la gerencia frente a los requisitos de cumplimiento legal y normativo, así como de disponer de mecanismos de verificación que permitan que los individuos puedan hacer uso efectivo de sus derechos constitucionales.

Si bien las redes sociales y el paradigma de la movilidad pondrán nuevamente a prueba el hábeas data, se requiere que los ejecutivos de seguridad de la información, consideren dentro de los diseños de seguridad y control corporativos, elementos propios que aseguren los datos personales, que bien pudieran ser aquellos propuestos por la doctora Cavoukian en su modelo denominado "privacidad por diseño", el cual consta de siete principios fundamentales para proteger la información personal: (CAVOUKIAN 2011)

- Sea proactivo y preventivo.
- Haga de la privacidad una configuración por defecto en los sistemas de tecnología de información.
- Incorpore la privacidad entre los diseños y arquitectura de los sistemas de tecnología de información.
- Tome un enfoque de suma positiva, en lugar de uno de suma cero (privilegie la protección del dato personal, y no sólo el cumplimiento normativo).
- Incorpore la privacidad de principio a fin dentro del sistema de seguridad del sistema de tecnología de información.
- Provea visibilidad y transparencia.
- Respete la privacidad del usuario.

Como quiera que el reto de la privacidad en nuestra sociedad actual requiere un entendimiento mucho más elaborado del que actualmente tenemos, es preciso continuar incorporando dentro de los ordenamientos jurídicos los aspectos técnicos requeridos para darle un sentido efectivo a los derechos fundamentales que cada persona tiene frente a la información y de igual forma, nutrir las prácticas de seguridad de la información con los componentes constitucionales para repensar la protección de la información más allá de los aspectos de cumplimiento, sino en el contexto del perfeccionamiento del estado social y democrático de derecho.

No sabemos en qué momento una falla de seguridad de la información se puede presentar, ni bajo qué condición ésta puede poner a tambalear nuestros más elaborados pronósticos; pero sí debemos conocer cómo vamos a responder y mantener la operación de las empresas, no sólo para cumplir con un requisito legal o exigencia corporativa, sino para entender que en la práctica de aseguramiento y control corporativo, la información es la savia que sostiene la competitividad corporativa y la fuente natural de un derecho propio de cada ser humano.

Referencias

[1] ERNST AND YOUNG (2012) Privacy trends 2012. The case for growing accountability. *Insights on IT Risk*. January. Disponible en: http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2012/$FILE/Privacy-trends-2012_AU1064.pdf (Consultado: 24-03-2012)

[2] GAFF, B. y SMEDINGHOFF, T. (2012) Privacy and data security. *IEEE Computer*. March.

[3] SHAW, T. (2011) *Information security and privacy. A practical guide for global executives, lawyers and technologists*. American Bar Association. ABA Section of Science & Technology.

[4] CORTE CONSTITUCIONAL DE COLOMBIA (2008) Sentencia C-1011. Revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) *"por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."* Magistrado Ponente: Jaime Córdoba Triviño. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2008/c-1011-08.htm (Consultado: 24-03-2012)

[5] CORTE CONSTITUCIONAL (2010) Sentencia C-334. Demanda de inconstitucionalidad contra el artículo 16, inciso 1º (parcial) de la ley 1142 de 2007 y contra el artículo 245, inciso 2º, de la Ley 906 de 2004 (Código de Procedimiento Penal). Magistrado Ponente: Juan Carlos Henao Pérez. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2010/c-334-10.htm (Consultado: 24-03-2012)

[6] NIST (2010) Guide to protecting the confidentiality of Personally Identifiable Information. April. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (Consultado: 24-03-2012).

[7] CAVOUKIAN, A. (2011) Privacy by design. Disponible en: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf (Consultado: 24-03-2012).

***Jeimy J. Cano, Ph.D, CFE**. Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor Distinguido de la misma Facultad. Universidad de los Andes. Colombia. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D in Business Administration de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management, Boston. USA. Egresado del programa de formación ejecutiva Leadership in 21st Century. Global Change Agent, de Harvard Kennedy School of Government, Boston. USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. jjcano@yahoo.com*