Tres

La privacidad de los datos: un reto empresarial técnico-jurídico

Jeimy J. Cano, Ph.D, CFE

Introducción

Considerando los recientes informes internacionales (BURT 2012) sobre seguridad de la información, es evidente que aunque las organizaciones mejoran cada vez más en sus prácticas de seguridad, los atacantes se adaptan mejor a las condiciones de un entorno más asegurado, obligando a que su capacidad creativa se renueve y sus técnicas asimétricas nos vuelvan a sorprender.

De acuerdo con el reporte de la empresa Verizon (2012) y el estudio realizado por el Instituto Ponemon (2012) (patrocinado por la empresa Symantec), confirman que más del 50% de los ataques impactantes son causados por código malicioso o Malware y por atacantes internos. Esta realidad, nos habla de dos condiciones claves para tener en el radar organizacional. Una que nos interroga sobre nuestra capacidad de prevenir y enfrentar las fallas técnicas propias de las plataformas de las aplicaciones que tenemos en la actualidad, y otra, sobre las tendencias e inquietudes humanas frente a las necesidades, juicios sobre los valores y cultura organizacional.

En consecuencia, la información como elemento fundamental de las organizaciones modernas, adquiere cada vez más relevancia en el contexto estratégico de las juntas directivas, toda vez que cualquier atentado contra ella, que la ubique en una situación que vulnere alguno de sus principios como son la confidencialidad, integridad o disponibilidad, será objeto de sanciones o multas que pueden impactar de manera negativa la reputación y/o posición estratégica de la compañía.

Así las cosas, entender la información en un contexto más amplio y multidisciplinario, es advertir un giro importante en su gestión dentro de las organizaciones, que no solamente se preocupa por su calidad, seguridad y conservación, sino que incorpora una condición legal, de corte constitucional, que demanda el cumplimiento de un derecho fundamental, denominado en el ordenamiento jurídico internacional como *hábeas data*.

En este sentido y considerando la próxima formalización de la ley estatutaria de protección de datos personales en Colombia (Congreso de la República 2010), se detallarán algunos aspectos relevantes para desarrollar la función de privacidad de los datos en las organizaciones, para lo cual se tomarán algunos referentes metodológicos y experiencias internacionales, que nos orientan sobre aquellas cosas en las que no nos podemos equivocar, para dar cumplimiento a la exigencia de convergencia de dos mundos: la seguridad de la

información como buena práctica de negocios, y la privacidad, como garantía constitucional de los ciudadanos.

Roles frente a la protección de los datos

Las buenas prácticas internacionales en seguridad de la información señalan que podemos tener diferentes roles frente a los datos. Cada uno de tales roles establece responsabilidades y exigencias que deben ser conocidas, entendidas y aplicadas, toda vez que no hacerlo, significa dar lugar a brechas de seguridad que claramente pueden exponer a la empresa a circunstancias inestables, para dar cumplimiento a las condiciones que la normatividad interna o externa le impone frente a los datos.

Los roles más conocidos son los de creador o dueño, usuario y custodio de los datos. Cuando las organizaciones comprenden lo que significa ejercer cada uno de estos roles, es menos probable que tengamos situaciones inesperadas o amenazas de fuga que no tengan claramente identificados a los responsables y sus roles asociados. Las empresas en la actualidad, al no incorporar este tipo de roles caminan sobre una cuerda floja, sin malla de protección, jugando con las probabilidades de ocurrencia de un hecho, cuando en realidad, lo único necesario es reconocer que la posibilidad siempre está.

El creador de los datos, es aquella persona que genera los mismos, es el individuo que establece las condiciones de uso de la misma y detalla los permisos de acceso y/o actualización, requeridos para mantener la integridad del registro. En este sentido, el creador es el responsable de mantener una vista homogénea de los datos, para que ellos representen y mantengan la realidad que los trajo a la vida.

El usuario, como su nombre lo indica, es el que acoge y cumple las condiciones que el creador ha impuesto sobre los datos generados. El usuario es responsable de conocer y aplicar las condiciones de acceso establecidas por el dueño, teniendo en cuenta que todo atentado contra las reglas establecidas por el creador, serán objeto de sanciones o cierre de acceso, sin perjuicio de acciones disciplinarias, penales o administrativas que se puedan derivar de la gravedad de las acciones del posible atacante.

El custodio, es la entidad o individuo que atiende con claridad las condiciones de conservación y acceso que ha establecido el creador, para crear el ambiente requerido que permita su materialización y monitorización, de tal forma, que cualquier usuario autorizado cuente con las herramientas y el entorno adecuado para acceder a los datos previamente creados. Es claro que el custodio, deberá implementar mecanismos de alerta y seguimiento de accesos no autorizados o actividades no contempladas, para contar con la trazabilidad de las acciones que se han cursado frente a los datos.

Reconocer y aplicar estos roles frente a los datos determina con claridad los compromisos que cada individuo tiene y los impactos que se pueden derivar del incumplimiento de las mismos, lo que necesariamente nos habla del régimen sancionatorio que deben existir, siempre y cuando los datos se encuentren claramente clasificados según su importancia corporativa o su nivel de confidencialidad, condiciones que generalmente son comunes frente a este ejercicio.

Principios de protección de datos y derechos

Sabiendo que la definición y aplicación de roles frente a la(os) información/datos es una condición base para la protección de éstos y siguiendo la experiencia internacional de España frente a su Ley Orgánica de Protección de Datos Personales –LOPD-, revisamos a continuación algunos elementos relevantes del reglamento del desarrollo de esta norma, que leído en clave del ordenamiento jurídico colombiano, se traduce como el decreto reglamentario donde se detalla el proceso de aplicación real de una ley.

De acuerdo con el reglamento de la LOPD, declara los principios fundamentales de la protección de la información personal, que como bien anota García Rambla (2009, pag.48), recogen aspectos asociados a la solicitud, el uso o almacenamiento de datos personales. Los principios establecidos son:

- Calidad de los datos.
- Consentimiento para el tratamiento de los datos y deber de ser informado.
- Responsabilidad y encargado del tratamiento.

La norma citada entiende la calidad de los datos de la siguiente forma:
"Se considera indispensable que el interesado conozca el fin para el cual se recogen sus datos

y por lo tanto que éstos serán sometidos a tratamiento. Cualquier desviación de su utilización original constituye una falta en el uso de la calidad de los datos. En el caso de finalización del tratamiento para el cual fueron recabados, deberán ser cancelados y, por lo tanto, finalizar su utilización. No podrán de esta forma conservarlos, una vez superado el período necesario para los fines originales. Se excluyen de este tratamiento aquellos que puedan proporcionar valor histórico, estadístico o científico. (…)" (García Rambla 2009, pag.26)

De otra parte, el deber de ser informado es declarado por la norma como sigue:
"Cuando sea solicitado un dato, deberá expresarse previamente y de forma clara, el motivo de dicha solicitud y el tratamiento o finalidad para el cual será utilizado. Entre los datos facilitados, se encontrará información respecto de las capacidades del individuo para ejercitar sus derechos, así como la identidad y dirección del responsable del tratamiento o su representante. (…)" (idem, pag.27)

Seguidamente la LOPD establece qué es el consentimiento del interesado:
"Toda manifestación de la voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. (…) Cualquier empresa que utilice datos sin que su dueño haya dado su consentimiento, se encontrará cometiendo una infracción y por lo tanto sujeta a sanción por parte de la Agencia Española de Protección de Datos – AGPD. (…)"

Finalmente, el encargado del tratamiento, la norma lo define como:
"La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento. Cualquier organización que mantenga y trate datos personales, presentará una serie de sujetos físicos y jurídicos encargados de las diferentes operaciones sobre los mismos. Estos encargados del tratamiento estarán sujetos a diferentes normativas por parte de la empresa y dependerán directamente del responsable del fichero que disponga la organización. (…)" (idem, pag.26)

Como podemos ver, la norma citada conjuga una serie de directrices que definen con claridad lo que una empresa debe considerar cuando del tratamiento de un dato personal se requiere. Lo anterior fusiona las necesidades propias del estado para proteger la privacidad de la información personal, con las condiciones necesarias requeridas para su acceso, sumando las condiciones técnicas exigidas para darle cumplimiento a sus definiciones en un contexto conocido de una empresa.

Detallando un programa de privacidad de datos

Para hacer realidad los principios detallados y operacionalizar las definiciones de los roles frente a los datos en el escenario de las empresa, se requiere especificar un programa concreto y sistemático que permita incorporar dentro del ADN corporativo, la función de privacidad de los datos, no sólo como un requisito de cumplimiento, sino como aquel reconocimiento constitucional de la privacidad, principio fundamental para el buen uso de la información de terceros.

De acuerdo con los estudios realizados por el CIO Executive Board (2010), un programa de privacidad de los datos es la base esencial de la incorporación de una distinción extendida de la seguridad de la información, que ahora recae en el escenario corporativo donde se identifiquen fuentes de información de esta categoría (es decir personales asociados con personas jurídicas o naturales), el cual deberá operar al más alto nivel de la empresa, pues es allí donde el compromiso con el respeto a la Constitución y las leyes se debe dar, así como en cada uno de sus empleados en el adecuado tratamiento de los datos personales.

Desarrollar un ejercicio de este tipo, representa para una empresa la disposición de recursos, tiempo y esfuerzo, y es necesario definir una serie de etapas y entregables que permitan avanzar en la formulación de la estrategia, para hacer de la protección de los datos personales, una real consideración corporativa para aumentar la confianza de los terceros frente a la forma en la cual una organización materializa la promesa de valor de su negocio.

Las etapas y entregables propuestas por el CIO Executive Board son:

1. *Establezca una estructura de gobierno*
   Establezca claramente el propietario de la función para el desarrollo e implementación del programa, así como el cargo que va a atender las diferencias y reclamaciones frente a este tema, bien un Oficial en Jefe de Privacidad o un Ombudsman de Privacidad.

2. *Determine las leyes y regulaciones aplicables*
   Establezca un inventario de normativa aplicable, las directrices internas relacionadas con tecnología de información, control de seguridad físicos, entrenamiento monitoreo basado en el tipo de información que se recolecta y sus locaciones geográficas.

3. *Desarrolle un valoración de los datos*
   Establezca un diagnóstico de la información personal recolectada, almacenada y utilizada dentro de la empresa.

4. *Cree y distribuya políticas y procedimientos*
   Establezca el cuerpo fundamental sobre principios y condiciones sobre el manejo de la privacidad en la organización. Defina y detalle políticas y procedimientos para el tratamiento de diferentes tipos de datos personales (clientes, empleados, comunidades y proveedores)

5. *Despliegue el programa de entrenamiento y concientización*
   Desarrolle cursos y capacitaciones en línea sobre los principios de privacidad y respeto por los datos personales, así como entrenamientos dirigidos a segmentos de la población de más alto riesgo en el tratamiento de la información personal.

6. *Verifique los protocolos de seguridad de la información*
   Establezca las medidas de seguridad y control que incluyan entre otros aspectos: almacenamiento, cifrado, autenticación, permisos de acceso, seguridad en bases de datos y redes de computadores.

7. *Desarrolle protocolos para transferencia de datos*
   Detalle en las cláusulas contractuales acuerdos y condiciones para la transferencia de datos personales. Utilice algunas prácticas internacionales como la certificación *Safe Harbor* o reglas corporativas vinculantes que gobiernen la forma como se transfiere información personal entre empresas o dentro de la compañía.

8. *Asegure el cumplimiento de sus prácticas con los terceros involucrados*
   Defina y asegure el cumplimiento de las prácticas de seguridad de la información requeridas con los terceros. Audite y certifique la efectividad de las medidas de seguridad implementadas por los terceros. Incluya en los contratos las consideraciones de privacidad requeridas para el tratamiento de la información personal.

9. *Desarrolle un plan para atención de los incidentes de seguridad de los datos*
   Detalle un plan de acción y el equipo que atenderá los incidentes de seguridad de los datos personales. Documente claramente la investigación y los mecanismos de notificación que aseguren una respuesta clara y oportuna de los mismos.

10. *Monitoree y audite el desempeño del programa*
    Desarrolle métricas concretas y verificables que midan la efectividad del programa. Mantenga un seguimiento interno del programa auditando las prácticas establecidas frente a los requisitos normativos y el cumplimiento de metas propuesto por la alta gerencia.

Si se sigue esta guía metodológica, la función de privacidad de la información tendrá elementos formales que poco a poco se irán incorporando dentro de la dinámica de cumplimiento propia de las empresas, haciendo tanto de la seguridad de la información como de la privacidad, una vista convergente que forme parte del respeto por los datos de los individuos y el aseguramiento de los procesos de la empresa, para alcanzar sus metas corporativas.

Reflexiones finales

Afirma Shaw (pag.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 este contexto, la tentación de encargar el programa de privacidad de la información al área de seguridad de la información se debe desdibujar, toda vez que alcanzar la efectividad del mismo exige un compromiso de la alta gerencia y de las áreas de cumplimiento empresarial, donde se conjugan las responsabilidades y retos de seguimiento para que la organización asuma y encuentre en este programa, una forma de avanzar tanto en las prácticas de seguridad como en el reconocimiento jurídico de la importancia del buen tratamiento de los datos personales.

Aunque la experiencia española nos dice que el proceso de reglamentación de una norma de protección de datos implica necesariamente incorporar nuevas prácticas en las empresas que den cumplimiento a las garantías constitucionales, es importante reconocer que este esfuerzo debe ser acompañado de la sensibilización e interiorización sobre las exigencias de la protección de los datos personales, como esa distinción que verifica que nuestros derechos terminan donde empiezan los de los otros.

Entrar en la era del cumplimiento de la protección de los datos personales, que no es otra cosa que hacer evidente el principio constitucional de la privacidad, es movernos en una esfera multidisciplinaria que, atenta a los cambios y motivaciones tecnológicas de la sociedad, es capaz de entender y confrontar las amenazas de una realidad altamente interconectada, de información instantánea y generalmente almacenada en la nube, para encontrar nuevas estrategias y acciones que permitan vincular los derechos de los titulares de la información, las condiciones de las regulaciones vigentes y las expectativas de la alta gerencia, de manera homogénea, para desarrollar una visión holística en la protección de la información empresarial.

Referencias

[1] VERIZON (2012) 2011 Data breach investigation report. Disponible en: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (Consultado: 25-03-2012)

[2] PONEMON INSTITUTE (2012) 2011 Cost of data breach study. United States. Disponible en: http://bit.ly/xBF6vr (Consultado: 25-03-2012)

[3] BURT, J. (2012) IBM: Security is improving, but cybercriminals are adapting. Eweek Magazine. Disponible en: http://www.eweek.com/c/a/Security/IBM-Security-Improving-but-CyberCriminals-Are-Adapting-757749/ (Consultado: 25-03-2012)

[4] CIO EXECUTIVE BOARD (2010) CEB Guidance: Key components of a data privacy program. Legal and compliance practice. *Compliance and ethics leadership council*. (Requiere suscripción).

[5] CONGRESO DE LA REPÚBLICA (2010) Informe de conciliación al proyecto de ley No.046 de 2010 Cámara, 184 de 2010 Senado. *Gaceta del Congreso. Senado y Cámara*. No. 1101. Año XIX. Diciembre

[6] GARCÍA RAMBLA, J. (2009) *Aplicación de medidas para la implantación de la LOPD (Ley Orgánica de Protección de Datos Personales) en las empresas. Medidas técnicas y organizativas*. Ed. Informática64.

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

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.*