EFECTIVIDAD EN LA GESTION DE DATOS PERSONALES [(1)]

Por: Ing. Gustavo Vicioso Simmonds, Consultor de Gestión Humana & Gobierno Corporativo, marzo 14 de 2018

"Los datos son el problema de polución de la era de la información, y la protección de la privacidad es el desafío ambiental.": Bruce Schneier

Hace un par de meses leía un artículo de uno de mis autores / especialistas favoritos en materia de Cumplimiento, Kristy Grant Hart; el fabuloso escrito versaba sobre las nuevas y exigentes normas de la UE contenidas en el Reglamento General de Protección de Datos (de su sigla en inglés GDPR), tema ciertamente muy sobre el tablero en nuestro país, habida cuenta de la entrada en pleno rigor del último paso de la normatividad sobre Protección de Datos Personales, con el registro de las bases de datos ante la demandante Superintendencia de Industria y Comercio (SIC).

En relación con el artículo en mención, claramente me he sentado muchas veces frente a un escritorio a tratar de leer una política de una compañía y me he declarado impedido de entender el genuino interés y fondo filosófico perseguido por la guía; con frecuencia, las guías suenan pomposas y graves, a tal grado que son ininteligibles. Y esa es una de las razones por las cuales algunos empleados no conocen (o dicen no conocer) las políticas de la Compañía.

La industria y el comercio en Colombia también están siendo exigidos en materia de cumplimiento de las normas de privacidad de datos. A junio de 2017, la SIC ya había impuesto cerca de 620 multas por Col$21000 Millones, el 80% de ellas respecto de violaciones del habeas data financiero y las restantes imputables al Uso no autorizado de Datos Personales (DP) con fines de mercadeo, divulgación de datos sensibles en la web, debido a eventuales fallas en la seguridad de sistemas, y a hurto y/o pérdida de la información contenida en Bases de Datos (BDs). Las multas individuales podrían alcanzar (han alcanzado) la trágica cuantía cercana a Col$1500 Millones (~USD$500 Mil).

Debemos ser más responsables y capaces de demostrar cumplimiento – entendido este como adhesión a las normas, leyes, regulaciones, políticas, prácticas y procedimientos -. Uno de los elementos más críticos (que bien concebido, gerenciado, divulgado e interiorizado es generador de cultura de cumplimiento) es la definición de las políticas, en esta oportunidad en materia de privacidad de datos, pero elemento extrapolable a SAGRLAFT, SARO y/o cualquier otra dimensión de gobernanza corporativa.

¿Y cuáles son <u>algunos</u> de los elementos esenciales de un Programa de Cumplimiento en materia de Privacidad de Datos Personales?

Iniciemos con recordar que los datos personales son cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (léase Identificada o Identificable, al combinar con información adicional), en formato digital o físico. Veamos algunos de los elementos:

1. Una **Política de Protección de Datos**, orientada a que los empleados (sin limitarse a los responsables o encargados del tratamiento de datos, para quienes hay obligaciones especiales) sepan cómo, cuando, donde, para qué y por qué se pueden usar los datos, cuáles son los requerimientos de seguridad y protección de los datos, el ciclo de vida y, sin lugar a dudas, las consecuencias del uso indebido. Esta es una forma eficiente de crear cultura con fundamento en las convicciones y no en aproximaciones punitivas. Así se podrán evitar los dolores de cabeza y traumas

financieros para las partes interesadas, a consecuencia de la materialización de riesgos financieros, legales y reputacionales y, mejor aún, se afianzará el respeto por los derechos constitucionales y la dignidad del ser humano.

2. **Política de Ciclo de Vida de los Datos Personales**; esta debe proveer claramente los detalles de gestión desde el momento de la recolección, el mantenimiento y uso, la supresión o disposición, las consultas de los datos personales, la protección requerida durante el ciclo de vida, garantizando una seguridad de extremo a extremo; siempre me ha asaltado la duda sobre la existencia en todas las empresas de una apropiada *Guía de Retención de Datos y Documentos* (GRDD), orientada a definir por cuanto tiempo deben preservarse y cuándo deben eliminarse los datos en los documentos y/o sistemas, a fin de permanecer (dentro de la normatividad) con razonables procesos de recolección, almacenamiento y destrucción de datos (físicos o electrónicos). Sobra anotar que la política debe hacer extrema claridad en materia de los derechos a consultar, reclamar, actualizar, suprimir y revocar las autorizaciones en la gestión de datos, nuevamente, en armonía con el respeto a la dignidad y derecho a la privacidad del ser humano y no por el temor a una intervención del riguroso inspector, vigilante y controlador.

3. **Procedimiento para Gestión de Crisis por Incidentes de Violación Normativa**: Todos los procesos tienen un riesgo inherente y uno residual, lo que conlleva a la potencialidad de la materialización del riesgo. El establecimiento de una guía o procedimiento para gestión de la crisis, delegación de autoridad y escalamiento a la Junta Directiva, acompañada de un plan de respuesta a la crisis, y un equipo de Gestión de Crisis y Continuidad del Negocio; este último juega un en la definición de qué hacer si ocurre una violación de datos, en cómo gestionar la eventual violación, en la prevención de cualquier pérdida adicional de datos, en la forma como la empresa debe informar a los clientes y reguladores sobre la violación, entre otros roles; todo ello, es un deber ser de cada organización respetuosa de la ley y orientada a la gestión responsable del riesgo; aquí, me siento obligado a sugerir un programa de simulacros, alrededor de los eventos calificados por los expertos como de más alto impacto y mayor probabilidad de ocurrencia. El entrenamiento disciplinado y permanente hace al deportista de alto desempeño, en su incesante búsqueda de resultados de clase mundial.

Durante mi ejercicio profesional al interior de importantes compañías, tanto a nivel nacional como internacional, aprendí que existen otras provisiones que se DEBEN tomar en cuenta:

1. La función de Capital Humano o Gestión Humana en su rol de agente catalizador de cultura, a través de procesos planificados de cambio, sin perjuicio de su rol como responsable del tratamiento de datos de los empleados,
2. La función de Gestión Jurídica, como agente de educación y entrenamiento, sin dejar de lado su rol de prevención del litigio a través de una efectiva y proactiva asesoría jurídica integral,
3. La función de Relaciones Públicas, también en un rol de educación y entrenamiento en materia de protocolos de manejo de crisis de cumplimiento, monitoreo de medios, posteo de información en redes sociales, adalides de la imagen corporativa de cara a los medios y otros muchos roles relevantes y críticos,
4. Las aguerridas funciones de Mercadeo y Ventas, movidas por el propósito de la rentabilidad organizacional como esencia de la supervivencia y sostenibilidad del negocio, y el requerido manejo apropiado de la información comercial

5. Los equipos de Tecnología de la Información, en términos de la estructuración de altos estándares de seguridad y prevención de ciber ataques y corrupción de bases de datos y, por último, mas no en última instancia,
6. Una Organización de Cumplimiento estructurada, respetada, balanceada en la ejecución de su rol de consultor interno y aliado para la rentabilidad, sostenibilidad y responsabilidad social del negocio, exhibiendo un Tablero de Mando que ilustre la generosidad e importancia de su rol.

Todo lo anterior y con otras muchas valiosas adiciones que conseguiremos a través de una red de expertos locales, amantes de esparcir conocimiento, será inútil sin un proceso impregnado por las convicciones creadas a través de la cultura organizacional, y el liderazgo transformacional de los niveles que hacen las decisiones de fondo.

(1) **Lecciones aprendidas de "Cómo arreglar las políticas de su compañía para GDPR - Tres cosas que necesita saber": Kristy Grant-Hart, 19/12/2017**
(2) ***Gustavo Vicioso:*** gusavo.vicioso@cable.net.co
(3) ***Consulta Importante:*** http://www.sic.gov.co/centro-de-publicaciones?field_tema_general_tid=5&field_anos_p_value=All