Febrero 24 de 2016

Contabilidad y seguridad de la información

Introducción

Por efecto de las nuevas normas colombianas, hablar de **aseguramiento de la información** de alguna manera se ha puesto 'de moda' si bien la calidad técnica de la implementación de tales normas es bastante discutible dado que se basa en estándares internacionalmente derogados y se está limitando al cumplimiento legal a la usanza tradicional, lo cual está conduciendo a que los cambios efectivos sean mínimos.

Adicional a ello, a nivel mundial se está discutiendo un tema diferente que toca de manera directa a la contabilidad y al trabajo de los contadores: la **seguridad de la información**. El debate está al 'rojo vivo.'

Como estas líneas están dirigidas, principalmente, a contadores, debe quedar bien claro que **aseguramiento de la información no es lo mismo que seguridad de la información**. La temática que se intenta abordar en estos comentarios es la de la seguridad de la información.[1]

En este trabajo se presentan distintas problemáticas asociadas a ello, vistas según puntos de vista a veces en conflicto, recomendándosele al lector que acuda a los documentos de referencia que se acompañan (para lo cual solo necesita hacer un clic en el vínculo respectivo). Está dividido en los siguientes apartes: (1) Privacidad de los datos; (2) La exactitud de los datos; (3) Los contadores necesitan hacer más para disuadir el crimen cibernético; (4) ¿Encriptar es la solución?; y (5) Palabras finales.

[1] Para lo relacionado con 'aseguramiento de la información', vea: http://www.samantilla1.com/#!aseguramiento/cyv0

Privacidad de los datos

Uno de quienes de mejor manera ha puesto 'el dedo en la llaga' es John Leonard[2] quien en el análisis que ofrece en la revista *Computing* ha planteado la pregunta de si la privacidad de los datos será sacrificada en el altar del libre comercio.

Haciendo referencia a la EU General Data Protection Regulation (GDPR) [Regulación general de la Unión Europea sobre protección de los datos], un documento de 209 páginas publicado en diciembre de 2015, señala que:

> *Las únicas sorpresas que figuran en él fueron la fuerza de las sanciones a disposición de las autoridades y el hecho de que las cuestiones clave tales como el "derecho al olvido" no se había diluido de cara de la feroz presión ejercida por los gigantes de la tecnología y sus aliados políticos.*

Anota que ello se está dando a la par de las negociaciones (hasta ahora casi 'secretas') del EU-USA Transatlantic Trade and Investment Partnership (TTIP) [Tratado trasatlántico Unión Europea-Estados Unidos y asociación para la inversión], que es un acuerdo comercial amplio que busca reducir los aranceles comerciales y las "barreras no arancelarias" para abrir los mercados en la agricultura, productos químicos, productos farmacéuticos, la energía y otros sectores. Está siendo impulsado en gran medida por las corporaciones multinacionales en los sectores y sus aliados políticos en la UE y los EE.UU, y se espera que esté listo para su ratificación en 2018 - al mismo tiempo que el GDPR se convertirá en ley.

Si bien de por sí esos procesos son interesantes, debe destacarse también que hacen parte de la lucha contra el terrorismo y la seguridad de la información, planteándose por lo tanto lo relacionado con cómo en la práctica van a operar 'dos ideologías' en competencia:

> *En Europa, la protección de datos y privacidad son derechos humanos fundamentales, mientras que en Estados Unidos los datos son una mercancía monetizada, y la protección de datos y privacidad son vistos como impedimentos para la libre expresión", explica Heather Burns, especialista en leyes digitales, de WebDevLAw*. (pg. 8).

Como los instrumentos centrales para poner en funcionamiento estas medidas son: (1) el intercambio de información, y (2) la co-operación regulatoria, el asunto toca de manera directa la información contenida en la contabilidad, principal, pero no únicamente la relacionada con información tributaria.

[2] Leonard, John. "Will data privacy be sacrificed on the altar of free trade?" *Computing*, February 2016, pg. 8-10 - http://www.computing.co.uk/.

Así las cosas, la contabilidad, que tradicionalmente ha sido vista como de carácter 'privado' se convierte en libro abierto. Recuérdese que lo que tradicionalmente se ha considerado de carácter público son los estados financieros auditados. Incluso las declaraciones tributarias han sido percibidas como de carácter 'privado.'

Por consiguiente, dependiendo de cómo culminen estos pulsos 'políticos' al más alto nivel, estamos frente a cambios realmente de fondo en la manera como es percibida la contabilidad. Definitivamente se impone la **contabilidad según estándares internacionales** (léase: un sistema único de la más alta calidad) y dejan de ser funcionales los **sistemas normativos jurisdiccionales** (léase: normas a la medida de las conveniencias, esto es, salvedades y excepciones para favorecer sectores, o sistemas 'a la medida' como permitir que los aportes sociales en las cooperativas sean patrimonio y no activos, etc.).

Como la contabilidad queda más abierta al escrutinio ya no solo del funcionario regulatorio de turno sino al escaneo de las analíticas de datos y las tecnologías cognitivas, la seguridad de la información contenida en la contabilidad se convierte en un asunto de máxima prioridad: ya no hay cabida para las trampas.

Este es un asunto que debieran examinar con cuidado quienes hoy, en el siglo 21, se atreven a decir en Colombia que las NIIF se pueden aplicar sin necesidad de registros por partida doble o mediante softwares paralelos.

La exactitud de los datos

En las grandes corporaciones, la figura de auditoría con mayor empoderamiento es la de los directores ejecutivos de auditoría, también conocidos como directores de auditoría jefe (CAO = chief audit officer), que, por ser una función interna de la empresa, normalmente está a cargo del auditor interno jefe. Recuérdese que no puede serlo el auditor externo dado que perdería la independencia.[3]

Por estas mismas fechas, los directores ejecutivos de auditoría mostraron su preocupación por la exactitud de los datos que utilizan para su toma de decisiones. Ello ha sido resumido de manera clara por Michael Cohn.[4]

[3] Este es un tema 'difícil' de entender en Colombia porque la figura de la revisoría fiscal no permite esta separación de funciones y a la larga el revisor fiscal ni puede ser director de auditoría jefe ('porque firma los balances') ni puede ser auditor externo ('porque realiza funciones no-independientes). Parece que ni los reguladores, ni los normalizadores ni la profesión contable colombiana están interesados en que se realicen las transformaciones necesarias.

[4] Cohn, Michael. "Audit Execs Worried about Data Accuracy,"*accountingtoday*, February 22, 2016: http://www.accountingtoday.com/news/audit-accounting/audit-execs-worried-about-data-accuracy-77278-1.html?utm_medium=email&ET=webcpa:e6159229:2526733a:&utm_source=newsletter&utm_campaign=daily-feb%2023%202016&st=email.

Michael Cohn hace referencia a una encuesta realizada por el Institute of Internal Auditors cuyos resultados son desalentadores:

- Menos de uno de cada tres directores de auditoría jefe tienen confianza en las decisiones estratégicas que toman con base en las analíticas de los datos
- Solamente el 29% tienen extremada confianza en esos datos
- El 23% tiene ligera o ninguna confianza en esos datos

La 'causa' de esta desconfianza es que los auditores internos no están revisando tales datos. Al igual que como ocurre con los auditores externos (que revisan la razonabilidad de los estados financieros pero no la seguridad de los datos contenidos y procesados en la contabilidad), los auditores internos no están involucrados en evaluar la calidad de los datos usados por sus organizaciones. La encuesta mencionada señala que solo el 47% tiene poca o ninguna participación en ello.

Cohen finaliza su comentario señalando que:

> *Algunos peligros potenciales citados en el informe son las preocupaciones legales y éticas en la recopilación de datos, tales como la privacidad. La auditoría interna necesita confirmar la idoneidad, exactitud e integridad de los datos. Debe haber adecuada evaluación, no sesgada de los datos una vez que se ha recogido el fin de comprender, por ejemplo, la diferencia entre correlación y causalidad. De lo contrario, las conclusiones a partir de los datos anteriores podrán basarse no en lo que los datos en sí prueban, pero en cambio en lo que alguien quiere probar*.

Algo no está funcionando bien y las soluciones no podrán estar por la vía tradicional de la emisión de normas regulatorias.

Ciertamente la clave pasa por una mejor evaluación de los riesgos asociados a la obtención y uso de los datos ('seguridad de la información') y a la co-operación con los comités de auditoría y con los auditores externos.

Los contadores necesitan hacer más para disuadir el crimen cibernético

Otro artículo elaborado también por Michael Cohn[5] insiste en que los contadores necesitan hacer más para disuadir el crimen cibernético.

Haciendo referencia a un reporte reciente emitido por el Institute of Management Accountants y la Association of Chartered Certified Accountants, señala que 'el crimen cibernético se está volviendo tan generalizado como para que los contadores lo ignoren.'

El reporte, titulado "Cybersecurity – Fighting Crime's Enfant Terrible" [Luchando contra el *Enfant Terrible* del crimen][6] dice en su resumen:

> *El propósito de este reporte es revisar el panorama de la amenaza cibernética, discutir la seguridad cibernética y sus futuras tendencias y áreas de preocupación, así como también resaltar las áreas particulares que sea probable tengan un impacto directo en el futuro de la profesión contable.*
> *En la medida en que los computadores están jugando un rol cada vez más creciente en lo que los profesionales de las finanzas hacen sobre una base diaria, la seguridad cibernética se está volviendo inextricablemente vinculada a tareas tan fundamentalmente importantes como proteger la seguridad y continuidad del negocio, asegurar la confiabilidad de los datos sensibles y ayudar a que los clientes entiendan y administren el rango amplio de los riesgos cibernéticos. Otras consideraciones clave son que la seguridad cibernética ya no es solamente un problema puramente técnico sino que se ha convertido en tan complejo y que no hay un solo tercero en el cual un negocio pueda confiar plenamente para estar seguro.*
> *Los contadores profesionales y los profesionales de las finanzas tienen que intensificar el desafío y aprender cómo sobrevivir a la marea generada por la ola del crimen cibernético.*

Quizás lo más preocupante de este reporte, surgido al interior de la profesión contable, es que al abordar el futuro de la profesión de cara a la seguridad cibernética se limita a las 'soluciones' tradicionales que han ofrecido los contadores (pg. 23ss):

- Mitigar los riesgos del crimen cibernético
- Seguros cibernéticos
- Reconocer al hackeo como una realidad
- Ninguna compañía es demasiado pequeña para ser víctima

[5] Cohn, Michael. "Accountants Need to Do More to Deter Cybercrime,"*accountingtoday*, February 23, 2016: http://www.accountingtoday.com/news/accounting-technology/accountants-need-to-do-more-to-deter-cybercrime-77282-1.html?utm_medium=email&ET=webcpa:e6167126:2526733a:&utm_source=newsletter&utm_campaign=daily-feb%2024%202016&st=email)

[6] Puede descargarse en: http://www.futuretoday.com/content/dam/IMA/pdf/Technology/Digital/ACCA-IMA-Cybersecurity%20Report%20v8.pdf

- Reducir la brecha del conocimiento
- Observar las reglas de la higiene cibernética

Volviendo a Cohen, anota que los profesionales de la contabilidad y de las finanzas también deben seguir de manera estrecha el trabajo del gobierno y de los diversos reguladores, con el fin de tener la última información sobre la legislación y los requerimientos para la adecuada revelación y la investigación pronta de las violaciones cibernéticas.

Yo agregaría que, además de ello, analizar los contextos políticos e ideológicos más amplios que están enmarcando las soluciones que se avecinan, las cuales están creando nuevos escenarios con condiciones diferentes a las tradicionales.

¿Encriptar es la solución?

En la lucha por la seguridad cibernética quizás el principal aliado técnico ha sido el encriptamiento. Sin embargo, el conflicto entre Apple y el FBI ha abierto un nuevo campo de discusión: ¿cuáles son los límites del encriptamiento?

El caso aparentemente es individual pero a la larga mucho más complicado: el FBI le ha pedido a Apple que des-encripte el iPhone de un francotirador y Apple se ha negado. Tal y como lo señala Silvia Ayuso,

> *La compañía aceptaría colaborar con una comisión de expertos en tecnología y seguridad, pero también en libertades fundamentales, que analice el alcance y límites de la encriptación y las posibilidades de un acceso regulado a dispositivos electrónicos como los que fabrica. Eso sí, siempre y cuando el Gobierno deje de intentar obligarle a que le abra una puerta trasera a su sistema de encriptación*.[7]

El lector podrá haberse dado cuenta que arriba, en la sección titulada 'privacidad de los datos' la GPDR da 'fuerza de las sanciones a disposición de las autoridades' lo que llevó a que John planteara la pregunta de si la privacidad de los datos será sacrificada en el altar del libre comercio.

Tal y como lo señala Silvia Ayudo, el problema "es que en la actualidad Silicon Valley y los agentes del FBI, la NSA o del Departamento de Seguridad Nacional "no están hablando entre sí" para buscar una solución consensuada." Por lo pronto, la solución propuesta por Apple es un panel de expertos que analice los límites de la encriptación, mientras que las autoridades están buscando una solución legal que obligue a Apple al des-encriptamiento.

[7] Ayudo, Silvia. "Apple pide que expertos medien en el conflicto abierto con el FBI." *El País.* 22 febrero 2016 http://internacional.elpais.com/internacional/2016/02/22/estados_unidos/1456162303_858501.html

Lo que es un hecho es que, hasta la fecha, las distintas posiciones han sentado precedentes muy peligrosos. Bill Gates, incluso, llegó a ponerse a favor del FBI en la disputa con Apple.[8]

Palabras finales

Si bien es cierto que los contadores necesitamos profundizar en el **aseguramiento de la información financiera**, también lo es que no podemos desconocer el nuevo frente de trabajo generado por la **seguridad de la información**.

Tienen en común en que ambos tocan el núcleo de la contabilidad (el procesamiento de los datos de las transacciones, condiciones y eventos).

Ello quiere decir que el **aseguramiento de la información**, que debe basarse en estándares actuales (y no es estándares derogados o ya superados), debe continuar privilegiando la ética y la calidad de los profesionales y la aplicación de los requerimientos técnicos, así como los requerimientos legales y reglamentarios asociados.

Pero la **seguridad de la información** va mucho más allá, dado que no se refiere únicamente a la contenida en la contabilidad sino que abarca todo tipo de información. Por eso los grandes debates del presente van en otra dirección: decisiones políticas e ideológicas en búsqueda de consensos, acuerdos al más alto nivel. Ello tiene consecuencias críticas en el uso de la tecnología (cfr. Encriptamiento) y en los poderes de las autoridades (limitados) y conlleva un trabajo profesional que ahora tiene nuevos escenarios y nuevas condiciones.

Será necesario estar atentos a estas cosas y participar de manera activa en la búsqueda de soluciones que vayan más allá de las tradicionalmente implementadas por los contadores.

Sígame en Twitter: @SAMantilla1

Sitio web: www.samantilla1.com

Blog: http://samantilla.tumblr.com

---

[8] Cfr: http://www.portafolio.co/internacional/bill-gates-favor-fbi-disputa-apple-491248