ISSN 2590-7387 (En línea)

Memorias

2.º Congreso Internacional

Crimen económico y fraude financiero y contable

FONDO EDITORIAL
CORPORACIÓN UNIVERSITARIA REMINGTON

Memorias: Segundo Congreso Internacional: Crimen económico y fraude financiero y contable
Congreso Internacional: Crimen económico y fraude financiero y contable (1.º: 2016: Medellín).
Medellín: Corporación Universitaria Remington, 2017
80 p.; 16,5x23 cm.

ISSN: 2590-7387 (En línea)
DOI: https://doi.org/10.22209/Cice.n2

1. Corrupción administrativa – Costa Rica. 2. Delitos económicos. 3. Selección de personal. 4. Auditoría. 5. Delitos por computador. 6. Control de medicamentos. I. Título. II. Autores. III. Corporación Universitaria Remington.

CDD: 364.168 C749

Primera edición, septiembre de 2017

Fondo Editorial Remington
Lina María Yassin Noreña, editora jefe
fondo.editorial@uniremington.edu.co
Calle 51 # 51-27, Edificio Uniremington
Telefax: (57) (4) 3221000, extensión 3001 - 3008
Medellín, Colombia

Diseño, diagramación y carátula
Cristina Yepes Pérez, diagramadora editorial
Fondo Editorial Remington

Compiladora
Jormaris Martínez Gómez
Grupo de Investigación Capital Contable

Contenido

Editorial
Segundo Congreso Internacional: Crimen económico y fraude financiero y contable

Tal vez fue Gary Becker quien introdujo la *teoría del crimen* en la microeconomía durante la década de 1950. Desde esta, el concepto se utilizó en los debates sobre las políticas de ajuste estructural promovidas por el Fondo Monetario Internacional y el Banco Mundial durante los años 1980 y 1990 (Benería y Sarasúa, 2011).

Sin embargo, las situaciones que han generado la última gran crisis económica hacen que se vuelva a hablar de crímenes económicos. La diferencia ahora es que la expresión fue definida por la Corte Penal Internacional como "cualquier acto inhumano que cause graves sufrimientos o atente contra la salud mental o física de quien los sufre, cometido como parte de un ataque generalizado o sistemático contra una población civil" (Benería y Sarasúa, 2011).

La idea de crimen económico nos lleva, pues, directamente a pensar en los delincuentes y los corruptos. Según la definición dada por la RAE (Real Academia Española) y la Asale (Asociación de Academias de la Lengua Española) en su *Diccionario*, los primeros serían aquellos que cometieron un acto antijurídico que el derecho o sistema legal de un Estado califica como tal; y los corruptos serían quienes se dejan o han dejado sobornar, quienes son perversos o mal habidos en su actuar (RAE y Asale, 2014). Así pues, tanto estas definiciones como la ya citada de la Corte Penal Internacional nos conducen a pensar que la noción de crimen económico en la actualidad ya ha desbordado los límites de la simple economía: involucra también problemas de las ciencias jurídicas, los derechos humanos y hasta la ética.

Entrando en materia, nos queda reconocer que la corrupción hace muchos años trascendió fronteras; que los elementos más esenciales de la sociedad están involucrados y que seguramente el más sensible de todos

https://doi.org/10.22209/Cice.n2a01

está presente allí: *la conciencia*, y, claro está, las mismas autoridades. Lo más lamentable es la indiferencia y que percibamos estos hechos como *parte del paisaje*.

En la academia, el sector real y en la vida cotidiana utilizamos la estadística como una herramienta para tomar decisiones. Definitivamente, qué espinoso es tener que usar esta misma herramienta para sensibilizar a la sociedad acerca del verdadero tamaño y de las consecuencias de los crímenes económicos. Y es que precisamente las cifras nos sitúan en un contexto real, y por eso, apelando a ellas, hoy es posible manifestar que en los resultados de una reciente encuesta realizada en Medellín, y en la cual participé, se encontró que de una muestra representativa de las 10.850 pymes registradas en la Cámara de Comercio, un porcentaje importante aceptó haber realizado o estar dispuesto a realizar prácticas no transparentes (45,2 %). Lamentablemente, también hay que decir que las variables más destacadas fueron la extorsión y el soborno, con un 73,5 % y un 68 %, respectivamente.

En un marco más amplio, Gil y Jiménez (2015, p. 157), tomando datos de la OCDE (2002), indican que el 99 % de las empresas en América Latina son pymes; para el caso de Colombia, estas suman el 96,4 %, por lo que se han constituido en la organización económica más cercana a la comunidad y en las mayores empleadoras; sin embargo, sus prácticas no siempre obedecen a criterios éticos, transparentes y socialmente responsables (Gil y Jiménez, 2015).

Quiero hacer referencia también a la encuesta sobre delitos económicos realizada anualmente por PricewaterhouseCoopers (PwC) capítulo Colombia a empresarios, presidentes, miembros de juntas directivas y directores, denominada "Hacia una nueva ética en los negocios: preparados para evitar el crimen económico y cibernético"; esta trae a colación cifras reveladoras y preocupantes, como las siguientes (PwC, 2016):

- El 36 % de las organizaciones experimentaron delitos económicos.
- Uno de cada cinco encuestados nunca ha llevado a cabo evaluaciones de riesgo de fraude.
- Los métodos de detección de las compañías no responden a tiempo.
- Casi la mitad de los delitos económicos graves fueron perpetrados por actores internos de la compañía.

- La ciberdelincuencia es el segundo delito económico más reportado y afecta al 32 % de las organizaciones.
- La falta de personal con experiencia en la prevención y detección de LA/FT (lavado de activos y financiación del terrorismo) es un problema serio para las empresas.

También quiero destacar dos puntos trascendentales del informe de PwC (2016):

1. El instrumento encuentra que el delito económico evoluciona y las medidas de prevención retroceden.
2. Uno de cada diez delitos económicos es descubierto por accidente.

Así entonces, estos elementos dejan entrever que realmente se socializan las estadísticas de los eventos y las consecuencias, pero hemos dejado de lado la socialización de los mecanismos de prevención y control, los cuales, en última instancia, son una forma de apropiar a la comunidad del conocimiento y de una cultura de la prevención, el control, la denuncia y el autocuidado.

En este evento nos congregamos en un ejercicio donde se compartirán experiencias, investigaciones y propuestas en torno al crimen económico en el ámbito público y privado y en el medio nacional y extranjero. Miraremos también las grandes y pequeñas empresas como generadoras de actos corruptos y, también, de procesos, mecanismos o actividades preventivas y correctivas. Todo ello en busca de que los asistentes a este congreso seamos partícipes de esos mecanismos y propuestas para combatir de manera eficaz los diversos actos que afectan colectivamente a la humanidad.

Sea el momento para agradecer a todas las personas que han aportado en el diseño, promoción y ejecución de este evento: a Empresas Públicas de Medellín (EPM), por este escenario en el que nos encontramos, a TMF Group, a la Contraloría General de Medellín, a los empleados de Uniremington y a todas las personas que directa o indirectamente nos están acompañando.

Bienvenidos, conferencistas, investigadores, empresarios, docentes, estudiantes y comunidad en general. Este es un espacio propicio para

debatir y exponer cifras y propuestas y para que seamos multiplicadores sociales del conocimiento, la prevención, la detección y el control del crimen económico y el fraude financiero contable.

Referencias

- Benenría, L. y Sarasúa, C. (2011). Delitos y crímenes económicos contra la humanidad. *Revista de Economía Crítica, 12*(12), 156.
- Gil, A. y Jiménez, J. (2015). El contexto económico global de la pyme. *Estudios Regionales*, 179.
- PwC. (2016). Encuesta Delitos Económicos 2016 - Capítulo Colombia. Recuperado de https://www.pwc.com/co/es/publicaciones/crime-survey-2016.pdf
- RAE y Asale. (2014). Recuperado de http://lema.rae.es/drae/?val=corrupto

Muchas gracias por su presencia y participación activa.

Jorge Alcides Quintero Quintero
Decano de la Facultad de Ciencias Contables
Corporación Universitaria Remington - Uniremington

La corrupción en la contratación administrativa: el caso de Costa Rica

Luis Gustavo Socatelli Porras[1]

Resumen

La presente ponencia hace un análisis de diferentes variables que son fuente de corrupción en los procesos contractuales en Costa Rica, así como focos para generar extorciones o pago de dádivas a empleados públicos, producto del alto nivel de monopolio, de la discrecionalidad en la gestión de compras públicas y de la limitada información que se les da a los grupos de interés u oferentes y a la sociedad civil. Para el análisis se utiliza el modelo de Robert Klitgaard (2000), en el cual se considera que una combinación adecuada de las variables monopolio, discrecionalidad y transparencia, pueden incidir en administrar bajos índices de aceptación de los niveles de riesgo de la corrupción.

Palabras clave: contratación administrativa, corrupción, transparencia, Costa Rica.

Introducción

La extorsión y vicios en los procesos de contratación administrativa nacen en Costa Rica como consecuencia de una débil legislación que por muchos años rigió en el país. El tema no fue abordado por la Constitución Política actual (1949), ni por la Ley General de la Administración Pública (1978); solo hasta 1995, en el cual se promulgó la Ley de Contratación, ley que regula dicho proceso, apareció en el orden legislativo.

Pero esta tuvo igualmente sus inconvenientes, pues no estableció un ente rector en materia de contratación administrativa para el sector público, aspecto que tampoco se aborda integralmente en sus reformas

[1] *Tribunal Registral Administrativo. Costa Rica, San José.*
Contacto: lsocatelli@ice.co.cr; lsocatelli@tra.go.cr
https://doi.org/10.22209/Cice.n2a02

siguientes y que ha generado un vacío legal. Es así como esta ponencia propone el análisis de las variables monopolio, discrecionalidad y poca transparencia en los procesos de compras públicas de Costa Rica como elementos principales de los focos de corrupción.

Desarrollo del tema

Para desarrollar un análisis de la gestión de la contratación administrativa en Costa Rica y de los casos de extorsión que se generan en estos procesos contractuales es necesario conceptualizarlos en varios aspectos; primeramente, es menester exponer lo que se entiende por contratación administrativa y corrupción.

La contratación administrativa la define Rodríguez (2015, p. 3), como:

> *El conjunto de principios, normas y procedimientos que regulan la forma en la cual la Administración Pública interactúa en el mercado como cliente, al adquirir sus bienes y servicios, necesarios para el cumplimiento de sus fines y la satisfacción del interés público.*

Es a través de los procesos contractuales que la administración pública busca satisfacer una necesidad para el cumplimiento de sus fines; además, el bien o servicio adquirido debe también tener los componentes de precio-calidad que determinen que se cumpla con el objeto contractual.

Sin embargo, se presentan acciones que no necesariamente se encuentran dentro del bloque de legalidad, bien por corrupción de los funcionarios, o bien de las mismas empresas que participan en estas actividades de contratación; todo lo anterior es consecuencia de aspectos del modelo que son difusos o que no gozan de una adecuada transparencia.

Es clara entonces la importancia del abordaje del tema de la corrupción, del que Caiden (1997, p. 1) afirma lo siguiente:

> *La corrupción en todas sus formas corroe, socava y contradice todos los elementos democráticos. Es la manifestación del ethos antidemocrático, ya que expresa el egoísmo, el egocentrismo, el particularismo, los privilegios injustos, el aprovechamiento de las debilidades y de las fallas, la utilización inescrupulosa de los débiles, los explotables y los indefensos y toda clase de acciones cuestionables. Se trata de beneficios no merecidos, no equitativos,*

> *injustos e inmorales derivados de posiciones de confianza y de responsabilidad pública que son utilizadas para acciones mezquinas e innobles, las cuales resultan ofensivas a cualquier noción de salvaguarda pública sobre la cual se edifica la democracia.*

Hay que añadir el marco conceptual de la transparencia en la gestión de compras públicas, con la que se busca integrar al ciudadano y a las empresas como el pilar de la gestión gubernamental, es decir, el ciudadano resulta ser el elemento primordial en la gestión de Estado y, por ende, el motor de las acciones que se desarrollan en las instituciones para atender las demandas de la sociedad civil, pero a su vez para realizar una rendición y control de cuentas de las actividades que desarrolla. Es por ello que los gobiernos han optado por el gobierno abierto, el mismo que la Organización para la Cooperación y el Desarrollo Económico (OCDE) define con los siguientes aspectos:

> *"Tres son las características más relevantes que tiene que presentar una Administración para poder calificarla de abierta:*
> *• Transparencia: que las acciones, y los individuos responsables de las mismas, estén bajo el escrutinio público y puedan ser impugnadas.*
> *• Accesibilidad: que los servicios públicos y la información sobre los mismos sean fácilmente accesibles por los ciudadanos.*
> *• Receptividad: que sea capaz de responder a nuevas demandas, ideas y necesidades" (OCDE, 2006, p. 44).*

Para abordar el análisis se tomará, como ya se dijo, el modelo de Robert Klitgaard (2000), que indica que la gestión de la transparencia en la administración pública es una de las herramientas para controlar la corrupción, la misma que se ha arraigado en diferentes países.

Se deben establecer varias etapas para desarrollar un ambiente que permita minimizar los riesgos de corrupción y en primera línea se debe destacar la manera de enfrentarla, de generar conciencia sobre su impacto económico y social, de tal suerte que se evite su arraigo dentro del Estado.

Como segunda línea de acción corresponde desarrollar políticas y acciones concretas que la prevengan e impidan que contamine organismos o unidades administrativas sanas, por lo que es necesario

el fortalecimiento del control interno para detectar acciones ilegítimas, malversación de recursos, incumplimiento de metas institucionales y, a la postre, insatisfacción de las necesidades de la sociedad civil.

Es por ello que la transparencia lleva a elementos que permiten generar una nueva cultura no solo en la organización, sino en la sociedad civil, pues al formular políticas que permitan un expurgo mayor en lo tocante a contratos del Estado, empresas contratadas, conflictos de intereses, priorización de proyectos, participación de la empresa privada en conductas corruptas, entre otros, se impulsará el desarrollo de comportamientos éticos que a su vez permearán las raíces de la conducta ética de los ciudadanos.

Según lo expuesto por Klitgaard (2000), quien logra desarrollar una ecuación con elementos para considerar en la gestión de la corrupción en la cual la trasparencia es fundamental, la corrupción obedece a una fórmula: C= M+D-T; cuando hay monopolio, cuando tú puedes decidir lo que recibes, cuando hay discrecionalidad, cuando tú puedes decir cuánto recibes y cuando no hay transparencia, hay tentación a la corrupción.

En este sentido, se pueden destacar varios puntos en la gestión de la transparencia: efectivamente, entre mayor sea la concentración de tareas o procesos en una sola persona, mayor riesgo hay de que germine la corrupción, pues no existe una segregación adecuada de acciones que permitan establecer un ambiente de control para detectar aspectos anómalos. Por otra parte, se suma a esta ecuación la discrecionalidad debido a la ausencia de reglas, procedimientos o acciones estandarizadas que avalen la toma de decisiones relacionadas con condiciones contractuales, tipos de experiencia, certificaciones u otros requisitos cerrados que limitan a los oferentes para participar en contrataciones.

Finalmente, otro elemento es la inexistencia de la transparencia por la ausencia de elementos fundamentales como participación ciudadana, sistemas de información que permitan establecer una trazabilidad de las transacciones que se desarrollan en la organización, una adecuada publicidad de sus actos y, por consiguiente, una política acertada de rendición de cuentas en forma oportuna, veraz y confiable. La inexistencia de estos factores en la ecuación convierte a las organizaciones en entes muy vulnerables para la corrupción, por lo cual es fundamental que la administración pública desarrolle acciones concretas.

De tal forma que el análisis de la extorsión en la contratación administrativa se enfocará bajo el modelo de la ya mencionada ecuación de la corrupción de Klitgaard (2000), en la cual C es corrupción, M es monopolio de las decisiones, D es discrecionalidad en la toma de decisiones y T es transparencia en gestión pública: C↓ = ↓M + ↓D - ↑T

Para administrar el riesgo de la corrupción se debe cumplir con la lógica de disminuir M y D y aumentar T, y para ello es necesario contar con un ambiente de control interno adecuado y fuerte que permita maximizar positivamente estos elementos, los mismos que se explican a continuación.

Del monopolio. Una de las grandes debilidades que arrastra el modelo costarricense de contratación administrativa corresponde al débil bloque de legalidad en cuanto a la rectoría en la gestión de compras, pues no se define una entidad que genere los parámetros, normas y directrices generales, de tal manera que haya criterios unificados, pues la Ley de Contratación Administrativa (1995), básicamente tiene unos principios generales, de publicidad, de libre participación y de satisfacción del fin público, por indicar los más importantes, pero lo cierto es que actualmente cada institución que no pertenezca a la administración central puede desarrollar su propio modelo de contratación y, por tanto, definir aspectos como registro de proveedores, mecanismos de admisibilidad de los potenciales proveedores, metodología de evaluación de oferentes, entre otros; además, puede establecer sus propias herramientas informáticas para gestionar las compras.

Es por ello que cada institución pública se vuelve a su vez un monopolio en la gestión automatizada de contratación pública, lo que genera una incertidumbre y riesgos de extorsión en los procesos contractuales, pues cada organización desarrolla su gestión con los acentos que considere pertinentes. Como ejemplo, en este momento se encuentran en gestión sistemas de compras públicas en CompraRed 2.0, lanzado en el año 2001 por el Ministerio de Hacienda y que cobija a casi un total de 78 instituciones de la administración central; pues este dejará de funcionar totalmente en el año 2016 para dar cabida al Sistema de Compras Públicas (SICOP), que es una versión totalmente digital, prácticamente igual al sistema Mer-link® que impulsó la Secretaría Técnica de Gobierno Digital entre los años 2011 y 2012.

También existe el Sistema de Compras Municipales, que no se aplicó en todos los municipios, y un sinnúmero de plataformas que utilizan los

bancos estatales, empresas de servicios públicos y del sector no financiero del país.

A lo anterior debe sumarme que únicamente se tiene el Sistema Integrado de Actividad Contractual (SIAC) de la Contraloría General de la República (CGR), que más que sistema de gestión es un instrumento que utiliza dicha institución para que las dependencias estatales remitan información sobre la actividad contractual.

Como se ve, este amplio monopolio de las diferentes instituciones del Estado es lo que deriva precisamente en actividades que no benefician a la empresa privada a la hora de concursar libremente en todos los procesos contractuales. Las más afectadas son las pymes, pues tienen menor capacidad instalada para conocer las diferentes plataformas contractuales, por lo que muchas proceden a obtener la información de una empresa grande, lo que las lleva a subcontratar servicios y a ajustarse a los márgenes de rentabilidad que diseñó aquella para concursar.

Al existir diferentes plataformas y por la carencia de un bloque de legalidad suficientemente fuerte, falencia ya mencionada, se permite que las instituciones públicas monopolicen aspectos como requisitos de admisibilidad en los procesos contractuales en cuanto al tipo de bien, experiencia, variables financieras, entre otros, que no necesariamente están al alcance de todas las empresas.

Si bien se entiende que la contratación administrativa no es una acción popular en la que absolutamente todos pueden participar, lo cierto es que existen aspectos no claramente reglados en cuanto a la posibilidad de establecer reuniones previas con proveedores para definir condiciones técnicas que solo pueden ser cumplidas por un oferente y que en muchos casos se negocian dádivas que a la postre derivan en procesos contractuales que no permiten la participación de otros debido a lo cerradas que son las condiciones técnicas.

Discrecionalidad. Al igual que el monopolio, la discrecionalidad de la administración pública nace precisamente en su débil bloque de legalidad, pues la contratación administrativa no se ha visto como un sistema, sino como una actividad aislada de las diferentes instituciones del Estado. Cuando se promulga la Ley de Contratación Administrativa en el año 1995, en el ejercicio no se toman en cuenta observaciones de la Contraloría General de la República,

lo que motivó a que los cambios que se generaron en dicha ley fueran ordenados por sentencias judiciales en el ámbito de la Sala Constitucional y, más recientemente, en el Juzgado Contencioso Administrativo.

Estos cambios por supuesto que generaron parches en la normativa desarrollada inicialmente y produjeron nuevamente discrecionalidades en la gestión de contratación administrativa, lo que impide una libre participación y concurrencia de las diferentes empresas en la dicha contratación.

Sobre este punto también debe destacarse que si bien la Ley de Contratación Administrativa y su reglamento establecen las normas respectivas para la gestión de compras públicas, es muy poco lo que indica en cuanto a la estructura organizacional ideal que debe primar en las instituciones del Estado para garantizar una adecuada segregación de funciones, pues únicamente existe un Reglamento para el Funcionamiento de las Proveedurías Institucionales de los Ministerios de Gobierno, Decreto n.º 30640 del 27 de junio de 2002, que compete solamente a la administración central de Costa Rica y únicamente detalla aspectos principales que deben de cumplirse en las proveedurías institucionales, pero no establece el recurso humano respectivo con que se debe contar.

Es esta discrecionalidad la que deriva en procesos de corrupción en las compras públicas. Los casos más sonados en Costa Rica son el del Instituto Costarricense de Electricidad (Alcatel) y el del préstamo finlandés-Caja Costarricense de Seguro Social, en los cuales se vieron involucrados expresidentes de la república y altos funcionarios de cada una de estas organizaciones; estos procesos recientemente fueron resueltos tras una década, e incluyeron delitos como enriquecimiento ilícito, peculado y conflicto de intereses.

Transparencia. Siendo la transparencia un elemento primordial en la gestión pública, debe de acotarse que el Estado costarricense ha empezado a incursionar en las gestiones del gobierno abierto a fin de poner a disposición de la ciudadanía los diferentes procesos contractuales; sin embargo, existe una gran limitación debido a que esta información contractual no está centralizada para conocer la trazabilidad y el estado de gestión de compras públicas, pues como se señaló anteriormente existen varios sistemas en funcionamiento.

En junio de 2016, por iniciativa de un legislador se plantea un proyecto de ley para la utilización de un único Sistema de Compras Públicas, con el objetivo de que todas las dependencias del Estado, sean centralizadas, descentralizadas, financieras o no financieras, deban realizar todos los procesos de contratación administrativa en una única plataforma. Esto es fundamental para corregir las carencias y para poder garantizar un ambiente de control y rendición de cuentas que minimice el impacto de la corrupción.

Como elementos que muestran la radiografía del Estado costarricense en lo tocante a los indicadores más importantes estudiados por la Contraloría General de la República, por medio del Índice de Gestión Gubernamental (IDG), merecen destacarse los resultados obtenidos entre los años 2013 y 2014, tal como se muestran en la **Tabla 1.**

Tabla 1. Resultados del Índice de Gestión Gubernamental, años 2013-2014.

Factores IDG	2014			2013		
	Eficiencia	Transparencia	Ética y prevención de la corrupción	Eficiencia	Transparencia	Ética y prevención de la corrupción
Global	66,3	62,3	62,9	69,1	57,7	59,4
Planificación	77,2	75,8	60,1	76,1	74,1	53,5
Gestión financiero-contable	52,7	68,4	55,2	57,9	64,7	47,9
Control interno	69,4	46,7	64,5	73,7	43,1	60,0
Contratación administrativa	60,0	57,4	75,6	59,9	51,6	75,2
Presupuesto	79,0	66,8	45,7	76,1	64,2	43,6
Tecnologías de información	65,1	54,6	67,5	65,8	50,3	64,7
Servicio al usuario	61,4	69,9	59,7	57,6	62,4	54,0
Recursos humanos	65,5	55,5	70,8	65,8	47,5	68,5

Fuente: Contraloría General de la República (2014).

De los datos anteriores, señala la Contraloría General de la República (2014), que la calificación más baja corresponde a la transparencia (62,3) y dentro de ella al control interno; luego están las tecnologías de información, la gestión de recursos humanos y la contratación administrativa con puntajes inferiores a 60, en tanto que solo la planificación supera los 70 puntos. Como se indicó, la renuencia de algunas instituciones a publicar información en sus páginas de internet o por otros medios es el principal justificante de esos resultados, salvo en lo relativo a las tecnologías de la información, donde las limitaciones que sufren las entidades de menores recursos tienen un impacto notable.

En cuanto al criterio de ética y prevención de la corrupción, que obtuvo un puntaje de 62,9, el factor más bajo es el presupuesto, fundamentalmente por la falta de revisiones y la limitada participación ciudadana, que también se pone de manifiesto en la planificación. Igualmente, requiere atención la gestión financiero-contable, que se ve afectada por la falta de normalización interna y por la carencia de revisiones externas y de auditorías orientadas a la detección de riesgos de fraude. Además, un grupo importante de entidades no prepara estados financieros de manera directa, lo que les impide tener un conocimiento de primera mano sobre el estado de sus recursos financieros. En este caso, tanto la contratación administrativa como la gestión de recursos humanos superan los 70 puntos, lo que parece obedecer a las regulaciones aplicables, en el caso de la primera, y a la implementación de controles para verificar la presentación de las declaraciones juradas de bienes y el disfrute oportuno de vacaciones. Finalmente, el criterio de eficiencia obtiene un puntaje de 66,3, que resulta menor que el 69,1 obtenido en el Índice de Gestión Institucional (IGI) 2013.

Conclusiones

De lo expuesto se concluye: a. Que en el caso costarricense existe un marco legal débil en materia de contratación administrativa que permite niveles de discrecionalidad y monopolio que generan focos de corrupción. b. Que existe una atomización de sistemas de información en materia de contratación administrativa que no permite tener un adecuado proceso de gestión y transparencia de la actividad contractual del país. c. Que no existe una autoridad rectora en materia de contratación administrativa que permita establecer lineamientos y estandarización de los procesos contractuales

para garantizar la libre participación e igualdad de condiciones para los oferentes. d. Que existe incerteza jurídica para los oferentes en el proceso contractual, lo que limita el acceso de potenciales oferentes e incide en el desarrollo de nuevos negocios y de la empresa privada en cuanto a la venta de bienes y servicios para el Estado. e. Que según el IDG, Costa Rica mantiene indicadores de desempeño en materia de transparencia, ética y prevención de la corrupción inferiores al 70 %, aspecto que denota un gran trecho en estos ítems para lograr mejores resultados en el futuro.

Referencias

- Asamblea Legislativa de la República de Costa Rica. (1949). Constitución Política.
- Asamblea Legislativa de la República de Costa Rica. (1978). Ley n.º 6227 General de la Administración Pública y sus reformas.
- Asamblea Legislativa de la República de Costa Rica. (1995). Ley n.º 7494 de Contratación Administrativa (1995) y sus reformas.
- Caiden, E. (1997). La democracia y corrupción. *Revista del CLAD Reforma y Democracia*, *8, 1*.
- Contraloría General de la República de Costa Rica. (2014). Memoria anual 2014. Recuperado de: www.cgr.go.cr
- OCDE. (2006). *La modernización del Estado: el camino a seguir* (p. 44). Madrid: INAP-MAP. Ministerio de las Administraciones Públicas, España.
- Klitgaard, R. (2000). Contra la corrupción. *Revista Finanzas y Desarrollo*. Recuperado de: https://www.imf.org/external/pubs/ft/fandd/spa/2000/06/pdf/klitgaar.pdf
- Ministerio de Hacienda. (2003). Reglamento de funcionamiento de las proveedurías institucionales de los ministerios del Gobierno. Decreto Ejecutivo n.º 30640-H de 27 de junio de 2002. La Gaceta n.º 19 de agosto de 2003.
- Rodríguez, I. (2015). Generalidades de la contratación administrativa en Costa Rica. Módulo Generalidades de la Contratación Administrativa. Mer Link. Junio, 2015.

Indicios de alarma de fraude en las transacciones con partes relacionadas

Diego Fernando Hernández[1]

Resumen

En este artículo se presenta un compendio de indicios de fraude en las transacciones con partes relacionadas, pues es evidente que no todas las pequeñas y medianas empresas en nuestro país presentan estados financieros consolidados, pero sí una relación de inversión, donde puede llegar a considerarse un control conjunto o influencia significativa, con efectos en la situación financiera y en los resultados de una entidad.

Muchas pequeñas y medianas empresas colombianas no son cotizadas ni son gestionadas por sus propios dueños y de manera frecuente se realizan transacciones con familiares cercanos al propietario-gerente, los cuales se acercan al concepto de *stakeholders*.

Palabras clave: matrices y subordinadas, estados financieros, consolidación, control, influencia significativa.

Introducción

La globalización, según Reyes (2006, p. 3), "es un conjunto de propuestas teóricas que subrayan especialmente dos grandes tendencias: a. los sistemas de comunicación mundial; y b. las condiciones económicas, especialmente aquellas relacionadas con la movilidad de los recursos financieros y comerciales", que trascienden y sobrepasan las soberanías de los diferentes países.

Sin duda alguna, la globalización como fenómeno de movimientos trasnacionales, desde sus enfoques culturales, sociales y económicos, ha llevado a las pequeñas y medianas organizaciones a mirar desde otras

[1] *Facultad de Ciencias Contables, Uniremington.*
Contacto: diego.hernandez@uniremington.edu.co
https://doi.org/10.22209/Cice.n2a03

perspectivas el riesgo, en especial desde el enfoque económico, tal como lo afirman Lascurain y López (2013), con sus principales elementos tales como: la inversión extranjera, la movilidad de capitales y la apertura comercial, con el objeto de identificarlos, mitigarlos y gestionarlos.

Paralelamente, la apertura económica ha hecho que los mercados se movilicen tras la caída de las barreras arancelarias, en especial los de Suramérica, donde las pequeñas y medianas empresas se sienten vulnerables ante la gran cantidad de organizaciones que han llegado a cada uno de sus países, con sus robusteces financieras y sus estrategias. Maihold, & Villamar, (2016), han determinado que los países del sur no son homogéneos en cuanto al mercado y que cada uno tiene sus propias características y, por tanto, su propia relación con el resto del mundo, lo que hace que aparezcan conflictos de intereses.

Pese a ello, en esta última década las grandes compañías multinacionales han dirigido su atención a América Latina (AL), especialmente a aquellos países considerados como emergentes, dado que su potencial desarrollo, su crecimiento económico y el incremento en su población son atractivos y los especialistas recomiendan invertir.

Lo anterior se puede observar gracias a un sistema de información financiera estadounidense, la lista de Dow Jones, que ha considerado a 35 países como mercados emergentes, entre estos, latinoamericanos como Argentina, Brasil, Chile, Colombia, México y Perú. Igualmente, la Compagnie Française d'Assurance pour le Commerce Extérieur- Coface señala un grupo de países especialmente importantes en AL: Colombia y Perú **(Figura 1).**

En la **Figura 1** se observa que Colombia, como país emergente de AL, cumple con el 66,66 % en tres criterios seleccionados por Coface. El primer criterio tiene en cuenta el precio, la competitividad y la ganancia, establecido por la devaluación de la moneda frente al dólar y por la forma como el país ha manejado la situación de deterioro de la moneda para aumentar la competitividad eficazmente. Al mismo tiempo, en esta categoría se evalúan los países que han aumentado sus exportaciones de materia prima. El segundo criterio analiza la capacidad de endeudamiento; se estudian las condiciones en las variables de préstamos más estrictos y se destacan los países que pueden beneficiarse de la competitividad de los precios y las ganancias; asimismo, tiene en cuenta los bajos niveles

de deuda corporativa. El tercer criterio evalúa las políticas de riesgo. Este indicador de Coface tiene en cuenta las presiones para el cambio, entre ellos todo lo relacionado con la corrupción y el desempleo y los instrumentos que hacen referencia a la educación *vs.*, la proporción de jóvenes. Como se puede visualizar en la **Figura 1**, pocos países presentan bajo riesgo político.

Figura 1. Infografía empresas en los países emergentes. 34 países filtrados según 3 criterios.
Tomada y modificada de: Coface, 2016; países emergentes. https://goo.gl/eKyKLN

En contraste con los análisis de mercados internacionales, con el crecimiento poblacional y especialmente con los criterios económicos, se hace necesario que las pequeñas y medianas empresas adopten medidas de asociación con el ánimo de participar en mercados abiertos internacionalmente, lograr las metas y objetivos trazados por la administración, ser más

competitivas y generar estabilidad; se conoce internacionalmente como empresa en marcha, es decir, generar confianza a los inversores para que la empresa trascienda en términos de sostenibilidad económica, generación de rentabilidad y sostenimiento a través del tiempo.

Con todo y lo anterior, como lo expresan Rozas, Corredor y Guerra (2011, p.135), "la dinámica de la economía mundial implica que las empresas deben buscar oportunidades de mercado en todo el mundo. Las grandes compañías buscan negocios globalmente, y las estrategias de mercadeo deben ser acordes con esta realidad". Por ello las pequeñas y medianas empresas no deben tener miedo a los cambios, a la generación de estrategias de mercado y, sobre todo, a enfrentarse con los mercados internacionales.

Igualmente, es necesario que las pequeñas y medianas empresas, especialmente las que son dirigidas por sus propios dueños, conozcan algunos de los riesgos asociados con las partes relacionadas en la presentación de la información financiera. En concordancia con lo mencionado, es fundamental describir en este artículo los indicios de fraude más comunes en las transacciones con partes relacionadas.

Partes relacionadas. La contabilidad como fuente de comunicación genera la información necesaria y suficiente para que los inversores puedan realizar sus aportes o la inyección de capital, con el objeto de aumentar su participación en los mercados emergentes y así lograr mayor competitividad y alcanzar los estándares necesarios para su visibilización frente a los mercados, lo cual aumenta su capacidad a través de sus grupos económicos.

Las partes relacionadas, bajo un contexto internacional, se relacionan con la capacidad de dominio o de influencia significativa de una sobre la otra al momento de tomar decisiones de operaciones de la actividad, o su respectiva acción financiera.

Así mismo, las Normas Internacionales de Información Financiera (NIIF, 2012), también conocidas por sus siglas en inglés como IFRS *(International Financial Reporting Standards),* establecen formas de relaciones particulares, a las cuales las pequeñas y medianas empresas deberían apuntar para el logro de la asociación comercial, captura de mercado, expansión de sus líneas y estabilidad económica; dichas formas de relación para el manejo en sus partes relacionadas se desarrollan de tres maneras:

a) En las personas naturales que poseen una pequeña o mediana empresa, es posible que se presente a través de un familiar cercano el cual puede:
   - Ejercer control o control conjunto sobre la persona que informa.
   - Ejercer influencia significativa sobre la persona que informa.
   - Ser un integrante personal clave de la administración de la persona que informa.

b) Una persona jurídica está relacionada con la empresa que informa si le aplica alguna de las siguientes condiciones:
   - La persona jurídica y la empresa que informa son integrantes del mismo grupo económico.
   - Ambas empresas son negocios conjuntos de una tercera organización.
   - Un integrante del personal clave de la gerencia de la empresa o de una controladora de la organización, o un familiar cercano a ese miembro, ejerce control o control conjunto sobre la empresa que informa o tiene poder de voto significativo en ella.

     Control conjunto, como lo definen las NIIF (2012), "es el acuerdo contractual para compartir el control sobre una actividad económica. Existe únicamente cuando las decisiones financieras y de operación estratégica exigen el consentimiento unánime de los participantes" (p. 90).

     Por su parte, las Normas Internacionales de Información Financiera para *pymes* (NIIF *pymes*, 2010-2) afirman que hay influencia significativa cuando se tiene el "poder de participar en las decisiones políticas, financieras y de operación de una asociada, sin llegar a tener el control o control conjunto sobre tales políticas" (p. 86); y al mismo tiempo dichas normas afirman que "cuando un inversor mantiene, directa o indirectamente (a través de subsidiarias), el 20 % o más del poder de voto en la asociada, se supone que tiene influencia significativa, a menos que pueda demostrarse claramente que tal influencia no existe".

     Las NIIF *pymes* incorporan el siguiente ejemplo en el Módulo 33 Información a revelar sobre partes relacionadas:

La entidad J pertenece en partes iguales a los miembros de la familia X Sr. y Sra. X y sus hijas Srta. Y y Srta. Z. La entidad es dirigida por los miembros de la familia. Sus puestos en la entidad J son los siguientes: Sra. X, directora de operaciones; Sr. X, director de administración; Srta. Y, directora financiera; y Srta. Z, directora de ventas **(Figura 2).**

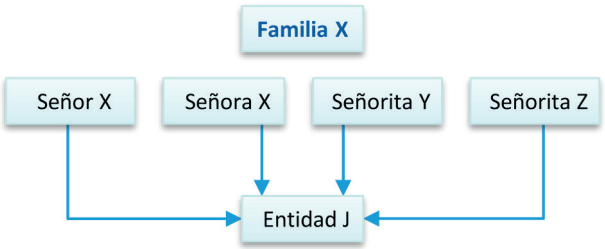

Figura 2. Partes relacionadas de una persona natural.
Tomada y modificada de: NIIF pymes (2010).

En la ***Figura 2,*** *cada miembro de la familia X posee el 25 % del poder de voto en la entidad J. En ausencia de evidencia en contrario, cada uno de ellos tiene influencia significativa sobre la entidad J. Para los estados financieros de la entidad J, todos los miembros de la familia son partes relacionadas Módulo 33, 2009, p.11).*

c) Entre personas jurídicas cuando son aplicables cualquiera de las siguientes condiciones, entre otras:
   - La entidad y la organización que informa son parte del mismo grupo económico.
   - Una organización es una asociada o un negocio conjunto de la otra entidad.
   - Ambas organizaciones son negocios conjuntos de la misma tercera parte.

En la **Figura 3**, también tomada del Módulo 33 de las NIIF *pymes*, se observa:

La entidad controladora tiene una participación controladora en las subsidiarias A, B y C y tiene influencia significativa sobre las asociadas 1 y 2. La subsidiaria C tiene influencia significativa sobre la asociada 3.

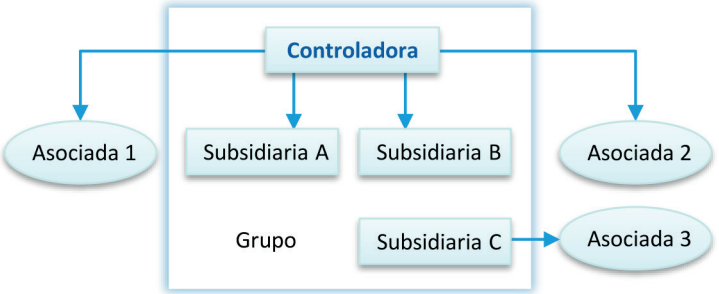

Figura 3. Partes relacionadas con una persona jurídica.
Tomada y modificada de: NIIF pymes (2010).

> *Para los estados financieros separados de la controladora, las subsidiarias A, B y C y las asociadas 1, 2 y 3 son partes relacionadas. Para los estados financieros de la subsidiaria A, la controladora, las subsidiarias B y C y las asociadas 1, 2 y 3 son partes relacionadas. Para los estados financieros separados de la subsidiaria B, la controladora, las subsidiarias A y C y las asociadas 1, 2 y 3 son partes relacionadas.*
> *Para los estados financieros de la subsidiaria C, la controladora, las subsidiarias A y B y las asociadas 1, 2 y 3 son partes relacionadas. Para los estados financieros de las asociadas 1, 2 y 3, la controladora y las subsidiarias A, B y C son partes relacionadas. Las asociadas 1, 2 y 3 no están relacionadas entre sí. Para los estados financieros consolidados del grupo de la controladora, las asociadas 1, 2 y 3 están relacionadas con el grupo (Módulo 33, 2009, p.13).*

Por su parte, la Superintendencia de Sociedades hace referencia a que una forma de organización son los grupos económicos, que en el caso de la legislación colombiana se denominan grupos empresariales o situaciones de control, dependiendo del grado de integración que tenga la matriz con sus subordinadas.

Ceballos (1997) señala que el tema de partes relacionadas o matrices y subordinadas es central en el desarrollo mismo de la empresa contemporánea, ya que la interacción de estas hace que se genere el volumen necesario de negocios para lograr la debida competencia económica.

En este orden de ideas, Fierro (2008) dice que "los grupos empresariales están generalmente conformados por una entidad controlante o matriz y

una o más controladas o filiales, adquiridas o constituidas por la primera con fines especiales" (p. 90).

Alarmas de fraudes. En el enfoque de la auditoría moderna, según Lefort y González (2008), se establece que el principal reto que tiene un auditor externo en una organización es identificar en primera instancia si ésta pertenece o no a un grupo económico, si es subsidiaria, si está controlada de forma conjunta, si es asociada, si se encuentra bajo subordinación o si tiene alguna influencia significativa, pues, como se ha podido observar, es difícil reconocer a través de los estados financieros estas figuras de control o partes relacionadas.

En segunda instancia, si este auditor encuentra alguna forma de vinculación económica, debe realizar una valoración sobre las transacciones comerciales realizadas entre las diferentes empresas vinculadas, ya que estas actividades ponen en riesgo los resultados obtenidos y la posibilidad de trasladar recursos entre compañías a fin de aumentar el rendimiento de la inversión y disminuir la carga impositiva.

A continuación se realiza una descripción de las transacciones más comunes entre partes relacionadas y sus posibles fraudes.

Precios de venta por debajo de los precios de mercado. Se define el valor razonable como:

> *valor razonable al precio que se recibiría por vender un activo o que se pagaría por transferir un pasivo en una transacción ordenada entre participantes en el mercado en la fecha de la medición, es decir, un precio de salida (NIIF 13, 2012, p. 2).*

Téngase en cuenta que un valor de mercado activo es aquel en el cual las transacciones se realizan de forma similar con respecto a precios, artículos y condiciones comerciales.

Cuando existe influencia por vinculación económica, los precios de venta entre este tipo de compañías ya no son los mismos, lo cual afecta los márgenes de utilidad y distorsiona las cargas tributarias, lo que a su vez va en detrimento de los ingresos fiscales en los países donde se localizan las partes que intervienen.

Costos importantes sobre los precios de mercado. Afectan significativamente el margen de rentabilidad bruta, el cual se obtiene restando de los ingresos los costos de venta; el margen bruto. Se define como el cociente que arroja la división de la utilidad bruta entre las ventas netas; este riesgo afecta los ingresos del Estado a través del impuesto a las ganancias, definido este bajo la NIC 12 como el ingreso fiscal de actividades ordinarias imponible, menos los costos y gastos deducibles fiscalmente, multiplicado por la tasa impositiva.

Así mismo, las revelaciones en los estados financieros y especialmente en las cuentas por cobrar como rubro en los estados financieros y asientos contables que no indican la naturaleza de parte relacionada de los préstamos, Mariño (2006), determina que en algunos casos se disfrazan las cuentas por cobrar o por pagar con vinculados económicos con las cuentas de clientes y proveedores, para no reflejar en los resultados el riesgo de cambio asociado con transacciones en moneda extranjera, o bien para no reflejar en el estado de resultados ingresos originados fiscalmente por concepto de rendimientos presuntivos.

Pagar precios superiores por productos genéricos. Apunta a un grupo de bienes o servicios que, bajo su misma naturaleza, ofrecen las mismas ventajas y beneficios en un mismo mercado y bajo un mismo contexto. Al realizar este tipo de prácticas en las compañías vinculadas se transfieren costos, gastos y activos movibles con el objeto de mejorar rentabilidades y disminuciones tributarias en el lugar donde se encuentra la organización.

Ventas ficticias a casa matriz o a compañías vinculadas. Esta práctica se realiza para mostrar ingresos, generar beneficios brutos y mejorar indicadores de liquidez; por lo tanto, se asocia con el maquillaje de estados financieros, que se utiliza para incrementar las cuentas de anticipos y los avances recibidos.

Conclusiones

La globalización brinda, sin lugar a dudas, oportunidades para el desarrollo, el crecimiento y la expansión; sobre todo, genera espacios para la movilidad de capitales, de bienes y servicios, generando así horizontes abiertos para la competitividad que lleven a la creación de estrategias organizacionales

y permitan un correcto intercambio de recursos bajo un adecuado entorno comercial.

Es evidente que en un espectro global donde confluyen innumerables transacciones se generan riesgos, originados en entornos tanto comerciales como financieros; riesgos de exclusión de pequeñas y medianas empresas que no están preparadas para afrontar las fuertes demandas propias del mundo contemporáneo.

Es así como surgen bajo un contexto internacional, y en especial bajo el nuevo marco normativo de las NIIF, conceptos tales como *negocios conjuntos* y *activos controlados conjuntamente*, para que las pequeñas y medianas empresas logren unirse en dichas modalidades y afronten los cambios derivados del fenómeno de la globalización.

Por lo anterior, hay que gestionar todos los riesgos, derivados de los mercados internacionales, disminuir su impacto y, sobre todo, verificar la probabilidad de ocurrencia para así detectar el fraude relacionado entre compañías vinculadas. Es necesario tener un conocimiento amplio y suficiente de los tipos de transacciones que se pueden llevar a cabo entre los grupos económicos, las relaciones de inversión, matrices y subordinadas, y poseer todos los documentos soporte que afirmen las mismas, ya que pueden existir movimientos ficticios en los cuales se realicen bienes o servicios sin haber sido prestados; como también puede existir sobrevaloración de activos e ingresos y subvaloración de pasivos y gastos con el ánimo de mostrar fortaleza financiera o, por el contrario, sobrevaloración de los gastos y pasivos y subvaloración de los activos e ingresos con el objetivo de presentar en sus estados financieros debilidades que permitan la disminución de impuestos.

Referencias

- Ceballos, A. (1997). Sociedades matrices y subordinadas en la Ley 22 de 1995. *Revista Derecho Privado*, *2*, 105-120.
- Compagnie Française d'Assurance pour le Commerce Extérieur. (2016). empresas de países emergentes: ¿podemos esperar que vuelva el milagro del fénix? Recuperado de: http://www.coface.com.ar/Noticias-y-Publicaciones/Publicaciones/Empresas-de-paises-emergentes-Podemos-esperar-que-vuelva-el-milagro-del-Fenix
- Fierro, M. (2008). *Estados financieros consolidados* (2.ª edición). Bogotá: ECOE Ediciones. Recuperado de: http://www.ebrary.com

- Ifrs.org. (2009). Módulo 33 Información a revelar sobre partes relacionadas. Recuperado de: http://www.ifrs.org/Documents/33_Related_Party_Disclosures_ES.pdf
- Ifrs.org. (2012). NIIF 13 Medición del valor razonable. Recuperado de: http://www.ifrs.org/IFRSs/Documents/IFRS13sp.pdf
- Ifrs.org. (2012). NIC 12 Impuesto a las ganancias. Recuperado de: http://www.ifrs.org/IFRSs/Documents/Spanish%20IAS%20and%20IFRSs%20PDFs%202012/IAS%2012.pdf
- Ifrs.org. (2012). NIC 24 Información a revelar sobre partes relacionadas. Recuperado de: http://www.ifrs.org/IFRSs/Documents/Spanish%20IAS%20and%20IFRSs%20PDFs%202012/IAS%2024.pdf
- Lefort, F., y González, R. (2008). Hacia un mejor gobierno corporativo en Chile. *Revista Abante*, *11*(1), 17-37.
- Lascurain, M., y López, J. A. (2013). Retos y oportunidades de la globalización económica. *CONfines de Relaciones Internacionales y Ciencia Política*, *9*(17), 9-34.
- Maihold, G., y Villamar, Z. (2016). El G20 y los países emergentes. *Foro Internacional*, *56*(1), 165-211.
- Mariño, J. D. B. (2006). El régimen de precios de transferencia en Colombia un análisis de su desarrollo, del principio de plena competencia y de la vinculación económica. Vniversitas, 55(111), 33-63.
- NIIF para las *pymes*. (2010). Material de formación. Recuperado de: http://www.ifrs.org/IFRS-for-SMEs/Documents/Spanish%20IFRS%20for%20SMEs%20Modules/14_InversionesenAsociadas.pdf
- Reyes, G. E. (2006). *Teoría de la globalización: bases fundamentales*. Madrid Red Nómadas. Recuperado de http://www.ebrary.com
- Rozas, G. S., Corredor, V. C., y Guerra, H. S. (2011). *Negocios internacionales: fundamentos y estrategias*. Bogotá, Universidad del Norte. Recuperado de: http://www.ebrary.com
- Superintendencia de Sociedades. (2012). Comportamiento de los grupos empresariales del sector real de la economía, *10*.

Conozca a sus empleados: la debida diligencia, una tarea que demanda mucho cuidado

César Augusto Roldán Jaramillo[1]

Resumen

La debida diligencia de los empleados y candidatos a pertenecer a una empresa es una responsabilidad que muchas organizaciones circunscriben al proceso de selección. Sin embargo, debería llevarse a cabo con una periodicidad establecida mientras haya una relación laboral. Existen numerosas fuentes para recopilar información, bien sea de carácter público o privado; estas últimas requerirán de autorización del individuo para respetar su derecho a la intimidad y a la privacidad.

Independientemente del área responsable del proceso, existen diversos aspectos por considerar antes de realizar la debida diligencia, entre ellos la disponibilidad de recursos, el tamaño de la organización, el alcance de las indagaciones o consultas, la criticidad de cargos, los objetivos estratégicos de la organización y las decisiones propias del gobierno corporativo. Existen buenas prácticas que pueden aplicarse, además de diversas encuestas sobre temas de defraudación y corrupción que son públicas, medidas no solo como percepción, sino también sobre hechos ocurridos que sirven como guía para gestionar riesgos asociados al fraude y a la corrupción. Es necesario recolectar información, pero más importante es el uso que se le dé a la misma. Aquí radica el valor agregado de realizar debidas diligencias a candidatos y a empleados. No somos investigadores, somos recaudadores de información; no somos jueces, solo recolectamos, recogemos, analizamos e integramos datos para convertirlos en información y, luego, emitimos conceptos en aras de ser diligentes, de tomar decisiones y evitar la materialización de un riesgo que pueda interferir en el cumplimiento de los objetivos de la organización.

[1] *Empresas Públicas de Medellín.*
Contacto: cesar.roldan@epm.com.co
https://doi.org/10.22209/Cice.n2a04

Palabras clave: debida diligencia, listas públicas, listas privadas, señales de alerta, fraude, corrupción.

Debida diligencia

La debida diligencia (*due diligence* en inglés) se define como el mecanismo mediante el cual se obtiene un adecuado conocimiento de la contraparte, sometida a ella mediante la aplicación de diferentes mecanismos, procedimientos y medidas que permiten alcanzar un grado razonable de conocimiento sobre dicho tercero; se entiende por tal, cualquier contraparte de las relaciones empresa-entorno y del interior de cada organización, por lo que cada una de ellas debería tener definidos mecanismos para llevar a cabo debidas diligencias a todos sus grupos de interés, como empleados, contratistas, proveedores, directivos, clientes/usuarios, comunidad, socios, dueños, entre otros.

Cuando hablamos de debida diligencia, podemos ubicar dos momentos: uno básico y otro ampliado de mayor profundidad. El primero, llamado debida diligencia básica o limitada; el segundo, conocido como debida diligencia ampliada, reforzada o avanzada.

De la expresión inglesa *know your client* (*KYC* por sus siglas en inglés) podríamos derivar el concepto de conocimiento del empleado, *know your employee* (*KYE* por sus siglas en inglés), el cual abordaremos.

Como ya se mencionó, conocer a nuestros empleados es tan importante como conocer a cualquier otra contraparte con la que nos relacionemos en el desarrollo de nuestra gestión. Este es uno de los grupos de interés que en muchas oportunidades es ignorado o cuya relevancia es minimizada por oficiales de cumplimiento dadas las múltiples ocupaciones en que se encuentran o por su excesivo interés en otras contrapartes.

La Circular Externa 100-00006 del 2016 de la Superintendencia de Sociedades de Colombia (para los sujetos obligados por esta) determina, entre múltiples aspectos, que se deben identificar las situaciones que puedan generar riesgo de lavado de activos/financiación del terrorismo (LA/FT) en las operaciones, negocios o contratos que realiza cada empresa, y presenta como ejemplo "aceptar nuevos socios o empleados con antecedentes judiciales" relacionados con dichos delitos.

La circular en mención establece la necesidad de debida diligencia para el conocimiento de los trabajadores y fija la periodicidad para ello: al

momento de vincularlos y por lo menos anualmente actualizar sus datos. Sea o no esta la norma que rija una determinada empresa, los empleados y oficiales de cumplimiento deberían adoptar de cada una de las normas existentes aquellas mejores prácticas para tener un sistema de prevención robusto y fuerte.

Conocer los empleados debe ser un compromiso de las áreas de cumplimiento, de gestión humana, de selección de personal y de seguridad, y debe cumplirse no solo sobre aquellos que ya se encuentran vinculados a la organización, sino sobre los que aspiran a pertenecer a ella.

Realizar las debidas diligencias para *KYE* debería ser un procedimiento rutinario, debería llevarse a cabo al ingreso del empleado a nuestra organización y durante el tiempo de su permanencia.

Se puede decir, entonces, que la debida diligencia de los empleados es estática o puntual (la toma de una fotografía) y también dinámica y permanente (el monitoreo). Esto se traduce en apoyar las áreas de gestión humana en el diagnóstico o análisis de ajuste de aquellos que aspiran a ingresar a la empresa y en realizar monitoreo permanente o mantenimiento de la información para las personas ya vinculadas.

Ahora bien, por motivos de costos cada organización deberá definir claramente cuál es la población objetivo. ¿Todos los candidatos?, ¿solo los más opcionados?, ¿todos los empleados?, ¿solo directivos?, ¿cargos críticos?, ¿importancia de la función?, ¿exposición al riesgo?, ¿ubicación geográfica? o ¿algún otro criterio? Aquí está tal vez una de las primeras decisiones que se deben tomar cuando el empleado u oficial de cumplimiento establece un control para este importantísimo grupo de interés.

Cómo hacer la debida diligencia

Se considera que mínimamente se debería realizar una debida diligencia para los candidatos y, como se mencionó anteriormente, esta actividad deberá apoyarse en el proceso de selección o de medición de competencias que hagan los expertos (en este caso el área de gestión humana o a través de un tercero que preste dicho servicio).

Los aspectos propios del proceso de selección son objeto de análisis en este momento, pero se dejan a consideración algunas propuestas que, según criterio, características y capacidades, cada organización podrá tomar o no, siempre demostrando una actuación responsable, ética y transparente.

Cuando hablamos de debida diligencia para los candidatos se sugiere llevar a cabo las indagaciones que se consideren necesarias para emitir un concepto desde la perspectiva de prevención del LA/FT, respetando en todo momento los derechos fundamentales (básicamente, los derechos a los que se refieren los artículos 15, 18, 20 y 21 de la Constitución), sin dejar el mínimo detalle por resolver. La posición en esta ponencia, basada en la experiencia laboral del autor, es que se está haciendo frente a un proceso de indagación y verificación, no de investigación (aunque muchos así lo ven).

Sobre este punto, la posición del autor es que los empleados y oficiales de cumplimiento no son investigadores, sino, como ya se dijo, recaudadores de información de apoyo; además, no hacen juicios, centran su trabajo en recoger, analizar e integrar datos para convertirlos en información, la misma que se guarda en bases para luego emitir un concepto en aras de ser diligentes en el relacionamiento con terceros, tomar decisiones y evitar así la materialización de un riesgo que pueda interferir en el cumplimiento de los objetivos de la organización.

Una pregunta común entre los empleados y oficiales de cumplimiento es ¿a qué fuentes acudimos? La respuesta depende. Depende del grado de profundidad de información que se necesite, de la disponibilidad de tiempo, personal y recursos económicos, y de una caracterización de los cargos para determinar el grado de profundidad o alcance para cada uno de ellos.

Listas públicas y privadas de consulta. ¿Cómo manejarlas?

Existen listas públicas que a criterio del autor son indispensables: *OFAC (Office of Foreign Assets Control),* ONU (Organización de la Naciones Unidas), Policía Nacional (aunque esta tiene fines netamente personales), *FBI (Federal Bureau of Investigation),* Interpol (Organización Internacional de Policía Criminal) y Banco de Inglaterra. En la primera es indispensable hacer dos consultas mínimas: por nombres y apellidos, y otra por número de identificación.

A continuación, una muy breve descripción de algunas bases de datos que pueden ser consultadas para hacer la gestión del riesgo:

Registraduría Nacional del Estado Civil. Esta consulta es muy importante, ya que permite conocer el estado del documento de identidad. Por esta

vía se puede establecer si el documento está vigente, si el titular no se encuentra registrado, si ha sido dado de baja por muerte, si tiene pérdida de derechos políticos o civiles por la comisión de delitos o si el número suministrado no corresponde al nombre de la persona. El único requisito para acceder a la consulta es tener disponible la fecha de expedición del documento.

En caso de encontrar un documento con alguna anotación diferente a "vigente", se debe ampliar el alcance de su debida diligencia. Para hacer la verificación es necesario dirigirse a la dirección electrónica www.registraduria.gov.co e ingresar al módulo que dice "solicite gratis aquí el certificado de vigencia de la cédula".

Procuraduría General de la Nación. En esta consulta se determina si la persona registra o no antecedentes disciplinarios. Se puede generar o consultar, entre otros, el certificado ordinario, que contiene las anotaciones de las providencias ejecutoriadas en los últimos cinco (5) años, aun cuando su duración sea inferior a ese período. También se pueden obtener las providencias automáticas que señale la ley y aquellas que se encuentren vigentes al momento de generar el certificado, aunque hayan transcurrido más de cinco (5) años desde la ejecutoria del fallo.

En caso de encontrar antecedentes, será una alerta para profundizar los análisis y debería ser comunicada al área de gestión humana para determinar las acciones o fijar qué trámites realizar para tomar decisiones. Para hacer esta búsqueda debe dirigirse a la dirección electrónica www.procuraduria.gov.co y hacer clic en el módulo "ingresar consulta o expedición de antecedentes".

Contraloría General de la República. Permite la consulta o generación del certificado de responsabilidad fiscal de personas naturales. Allí se verifica si la persona se encuentra o no reportada como responsable fiscal. En caso de alertas, como en la fuente anterior, deberá considerar las decisiones en los diferentes escenarios posibles. Para hacer uso de esta herramienta debe dirigirse a la dirección electrónica www.contraloriagen.gov.co e ingresar al módulo "certificado de responsabilidad fiscal".

Para el caso de consultas en listas privadas o bases de datos del sistema financiero, deberá contar con autorización del candidato, tal como lo

establecen las leyes de hábeas data financiero y de protección de datos. Si en la solicitud de inscripción (para los candidatos) o en el contrato de trabajo (para los ya vinculados) se cuenta con dicha autorización, se podrán, entonces, consultar dichas bases de datos solamente con el propósito autorizado por aquellos.

Sin embargo, si las consultas solo se realizan en bases de datos públicas con alcance exclusivo de prevención de riesgos LA/FT, la Ley 1581 establece que no será necesaria la autorización.

Otras posibles fuentes

Otro aspecto que podríamos adaptar en nuestras organizaciones proviene del sector público en Colombia y fue creado mediante la Ley 190 de 1995. Todos los aspirantes a tomar posesión de un cargo público o quienes vayan a contratar con el Estado deben diligenciar una declaración juramentada de bienes y rentas (situación patrimonial, créditos, débitos, participación en sociedades y grupo familiar, entre otros).

Se sugiere conocer esta declaración y determinar si incluirla o no (o al menos parte de ella) dentro de los requisitos de vinculación.

Todos los empleados y oficiales de cumplimiento deberían conocerla para determinar su aplicabilidad en cada una de sus organizaciones, pues contiene la siguiente información:

- Nombre completo, documento de identidad y dirección del domicilio permanente.
- Nombre y documento de identidad del cónyuge o compañero(a) permanente y parientes en primer grado de consanguinidad.
- Relación de ingresos del último año.
- Identificación de las cuentas corrientes y de ahorros en Colombia y en el exterior, si las hubiere.
- Relación detallada de las acreencias y obligaciones vigentes.
- Calidad de miembro de juntas o consejos directivos.
- Mención sobre su carácter de socio en corporaciones o sociedades de hecho entre compañeros(as) permanentes.
- Información sobre existencia de sociedad conyugal vigente o de sociedad de hecho entre compañeros(as) permanentes.
- Relación e identificación de bienes patrimoniales actualizada.

Hoy en día muchas empresas solicitan tanto al momento del ingreso como durante la relación laboral que los candidatos y empleados suscriban una declaración de conflictos de intereses donde manifiesten la existencia de estos o la posibilidad de que los haya en el futuro. Este mecanismo, complementado con mucha más información, configura lo que podríamos llamar una debida diligencia ampliada de nuestros empleados. Tan importante como la información misma es el uso que se le dé, así como el entendimiento y el razonamiento que se le aplique, de forma tal que nuestra gestión agregue valor al quehacer organizacional.

Existen otros mecanismos que, independientemente de quién los lleve a cabo, pueden ser muy útiles para fortalecer nuestra debida diligencia. Cabe mencionar la verificación de referencias, la visita domiciliaria, las pruebas de polígrafo, los análisis de estilos de vida, entre otros. Este autor desconfía de las referencias porque, naturalmente, las personas ponen como tales a quienes darán información conveniente, positiva.

Otras señales de alerta que los empleados y oficiales de cumplimiento deberían considerar son la multiplicidad de viajes por fuera del sitio de trabajo (de la ciudad o del país), antecedentes de no declaración de potenciales conflictos de intereses o renuencia a hablar sobre ellos, numerosos regalos de terceros en temporadas específicas (como en fin de año), estilos de vida claramente superiores a los comunes a su cargo, exceso de invitaciones, viajes, almuerzos o cortesías, así como cierta intensidad en algunas relaciones con terceros.

Una práctica que requiere de una alta confidencialidad y que en estos días ha estado en muchas conversaciones es la entrega de la declaración de renta año tras año por parte de los directivos y cargos críticos. Esto es útil siempre y cuando se use en los análisis periódicos.

Hay un tema altamente sensible y vigente: análisis de las redes sociales. Aquí surge una gran pregunta: ¿deben las empresas revisar los medios sociales de sus empleados o candidatos? Según un artículo publicado por *The Wall Street Journal*...

> *... una encuesta de 2013 de CareerBuilder, que ayuda a las compañías a identificar y atraer empleados, halló que 39 % de los empleadores accede a las páginas sociales de los postulantes, mientras que 43 % indicó que habían encontrado algo que los llevó a descartar a un candidato, como publicar información o fotos indebidas, o criticar a un exjefe (párr. 1).*

¿Qué dicen algunas encuestas?

Es oportuno también considerar las diversas encuestas que realizan año a año diferentes firmas sobre los perfiles de los defraudadores, pero hay que aclarar que no se debe descartar a un candidato por el hecho de que cumpla con ciertas características de dichos perfiles.

Según la encuesta 2014 de la *Association of Certified Fraud Examiners* (*ACFE* por sus siglas en inglés), 42 % de los casos de defraudación fueron cometidos por empleados de la organización, el 36,2 % por gerentes o personas con posición de mando, el 18,6 % por los dueños o altos ejecutivos y el 3,2 por otros (*Report to the Nations on Occupational Fraud and Abuse*, p. 40).

Y los defraudadores por grupo etario tenían una distribución normal: los rangos de 36-40 años con el 17,6 % y de 41-45 años con el 18,1 %; es decir que entre los 36 y los 45 años se concentra el 35,7 % de los defraudadores según la *ACFE* (*Report to the Nations on Occupational Fraud and Abuse*, p. 48).

Según datos de la encuesta de la firma *KPMG (Klynveld Peat Marwick Goerdeler Http)*, Perfiles Globales del Defraudador 2016, se perfiló a 750 defraudadores en 78 países, cuyos testimonios fueron tenidos en cuenta para concluir que "la tecnología resulta ser un facilitador clave a la hora de cometer el crimen" (p. 20) y que "la tecnología en temas de fraude se vuelve un arma de doble filo y las organizaciones deben estar mejor preparadas para anticiparse a este desafío" (p. 20). Este mismo documento resalta que…

> *… en 24 % de los casos, el defraudador usó la tecnología para la creación de información falsa o engañosa, en 20 % de los casos, proporcionó información falsa o mentirosa a través de correo electrónico u otra plataforma de mensajería, y en 13 % de los casos, abusó del acceso que tenía permitido a los sistemas informáticos de la empresa (p. 20).*

La lista de hallazgos es extensa:

> *Quien hace el fraude es, en su mayoría, trabajadores que llevan más de 6 años en la empresa y es un hombre que está entre los 36 y 55 años de edad. Un 65 % de los defraudadores son empleados de la compañía; en el caso colombiano*

> *la cifra se eleva al 71 %. Sus ejecutores están entre cargos ejecutivos y niveles de dirección en un 57 % y 52 % respectivamente en nuestro país (pp. 7-8).*

Se diagnosticó que hay una alta probabilidad de actuar en complicidad con otros empleados o terceros (62 % de los fraudes) y que…

> *… la ganancia personal fue la primera motivación entre los defraudadores con 60 % de las menciones, la codicia fue el segundo factor, con 36 %; y el sentido de "porque puedo hacerlo" fue el tercero, con 27 % (un 62 %, 14 % y 29 % para el caso colombiano, respectivamente) (p. 8).*

¿Qué de la intimidad de las personas?

En el mundo existen antecedentes de multas a empresas por investigar a sus empleados. Es el caso de unos contratistas de un banco que habrían entrado a las casas de los empleados para grabar y tomar fotografías, y hasta registrado su basura en busca de información adicional. En este punto es importante, entonces, tener en cuenta el documento de la OIT (Organización Internacional del Trabajo) "Protección de los datos personales de los trabajadores".

Toda la información anterior o la que a criterio del área de cumplimiento se deba recolectar estará sometida al *apetito al riesgo* que la misma organización haya definido, esto es, lo que para algunos será una bandera roja para tomar drásticas decisiones, para otras organizaciones podrán ser alertas informativas o escenarios de riesgos con los cuales pueden convivir.

El proceso de monitoreo puede establecerse mediante la consulta en las fuentes anteriores (algunas de manera automática, otras de manera manual) y la recolección periódica de información directamente con los empleados, pero siempre mediante una conversación permanente, toda vez que esto permite crear un buen ambiente y envía un mensaje de transparencia a todos y cada uno de ellos.

Conclusión

Se reitera que los empleados y oficiales de cumplimiento no fungen como investigadores ni mucho menos como jueces, sino que su rol es el de indagadores y analistas de información que fundamentan la toma de decisiones en las organizaciones a las que pertenecen.

La recomendación permanente es que las áreas de cumplimiento deben realizar la debida diligencia tanto de los candidatos como de los empleados y mantener actualizada su información como parte de la gestión de prevención de riesgos LA/FT.

Referencias

- Circular Externa 100-00006 del 2016 de la Superintendencia de Sociedades de Colombia sobre el Sistema de Autocontrol y Gestión del Riesgo LA/FT. Puede consultarse en: http://www.supersociedades.gov.co/superintendencia/normatividad/circulares-externas/Paginas/circulares-externas.aspx
- Constitución Política de Colombia. Puede consultarse en: http://www.constitucioncolombia.com/
- Ley Estatutaria 1581 de 2012. Ley Estatutaria de Protección de Datos Personales por medio de la cual se dictan disposiciones generales para la protección de datos personales. Puede consultarse en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf
- Ley Estatutaria 1266 de 2008. Ley Estatutaria de Hábeas Data Financiero 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. Puede consultarse en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
- *Report to the nations on occupational fraud and abuse* - Encuesta 2014 de la Association of Certified Fraud Examiners, Inc puede consultarse en: https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf
- Perfiles Globales del Defraudador 2016 por KPMG. Puede consultarse en https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/profiles-of-the-fraudster-au.pdf
- Protección de los datos personales de los trabajadores. Repertorio de recomendaciones prácticas. Puede consultarse en: http://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_PUBL_9223103290_ES/lang--es/index.htm

Crimen económico en el sector salud: medidas para prevenirlo

Luis Alfonso Pérez Romero[1]

Resumen

La Organización Mundial de la Salud (OMS), preocupada por las prácticas corruptas en el sector a nivel global, ha definido un modelo para compartir en todas las naciones que deseen combatir la corrupción en la industria farmacéutica, el cual llamó *Programa de buena gobernanza para las medicinas* (*GGM*, por su sigla en inglés *Good Governance for Medicines*), publicado en el 2013. La estrategia con la que se inició este programa en varios países está relacionada con la promoción de la práctica ética y desarrollo para el uso de medidas de anticorrupción en el sector farmacéutico, con el objetivo fundamental de transparentar la producción, comercialización y administración de los productos farmacéuticos en el mundo. Esta propuesta de GGM se ha implementado para otras ramas del sector salud, como son las entidades administradoras y prestadoras de los servicios en salud. Se expone de manera detallada la posición global de la corrupción de algunos países de América y el caso de Marruecos como marco de referencia para mostrar cómo se ha abordado este flagelo; específicamente, se expondrán datos de la situación de la corrupción del sector en México, Chile, Perú y Colombia, países que integran la Alianza del Pacífico, para luego terminar con una propuesta para prevenir este crimen económico en los países de América.

Palabras clave: crimen económico en salud, corrupción en salud, modelo para prevenir la corrupción en el sector salud**.**

[1] *Universidad Autónoma de Guadalajara. México.*
Contacto: luisalfonsoperezromero@gmail.com
https://doi.org/10.22209/Cice.n2a05

Introducción

El crimen económico ha ido en franco crecimiento desde la década de los 90, fecha en la que se comienza a medir la corrupción a nivel global para mostrar los países más corruptos y registrar las mejores prácticas para enfrentar este mal. El sector salud ha sido afectado en todas las naciones por las prácticas corruptas. En América se han visto grandes cambios en los sistemas de salud en busca de mejorar la calidad de vida de sus habitantes, pero también se han visto en los primeros 15 años del milenio muchos casos de fraude, corrupción, nepotismo y demás actividades tipificadas dentro del crimen económico en México, Chile, Colombia, Perú, Venezuela, Brasil, etc. Este texto muestra datos como evidencias de este flagelo en América y Marruecos, y, asimismo, explica cómo estas naciones lo están enfrentando; y al final hace una propuesta para integrar la ética sostenible en el sector salud.

Antecedentes

La empresa Pricewaterhouse Coopers (PwC), publicó en el 2016, la evolución de delitos económicos, mostrando las cifras que se han mantenido en el 40 % desde el 2007 al 2016. Latinoamérica ha estado en un 34 % y México en un 43 %; cifras alarmantes de una cultura de la corrupción que ha afectado más a México. Esta situación es paradójica, ya que el 83 % de los CEO (por su sigla en inglés *Chief Executive Officer*) de México consideran que la corrupción y el soborno son la principal amenaza para sus negocios y, además, son conscientes de que el 25 % de las empresas han perdido oportunidad de negocios por estos delitos. En esta misma encuesta se han logrado registrar los siguientes delitos de crimen económico de mayor frecuencia: malversación o robo de activos, efectivos y otros recursos; corrupción, fraude en adquisiciones, fraude contable y delito cibernético. Para el futuro, en México se tendrán que enfrentar los siguientes delitos: malversación de fondos, información privilegiada, delito cibernético, sobornos y corrupción, espionaje y fraude en adquisiciones (PwC, 2016).

Debido a los constantes delitos de crimen económico en México y América Latina se ha podido conocer el perfil del defraudador y corrupto: sexo masculino, graduado de las universidades públicas o privadas, de 31 a 40 años de edad, casado y de tres a cinco años de

antigüedad en la empresa donde ha cometido el crimen (el 70 % de los corruptos están dentro de la empresa). Ante esto, es paradójico que en el 90 % de las empresas exista un código de conducta, con principios y valores de la organización bien establecidos; el 88 % de los líderes de las empresas comunican la importancia de la conducta empresarial ética dando buen ejemplo y tratando la corrupción como prioridad; el 87 % de las empresas consideran que la conducta empresarial ética es un componente clave dentro del procedimiento de recursos humanos; y el 79 % ofrece canales confidenciales para presentar quejas, inquietudes o denuncias de actos corruptos o fraudulentos cometidos por personas de la misma empresa.

El 90 % de los directivos apoya firmemente las directrices corporativas, el 89 % espera que sus socios comerciales adopten una postura firme contra la corrupción, el 89 % prefiere no llevar a cabo un negocio con riesgo de incurrir en sobornos, y finalmente el 86 % considera que el soborno no es una práctica legítima. Lo interesante es preguntarse qué está pasando, por qué tanta corrupción en 2016 en México a pesar de estos hallazgos, qué sucede realmente en América Latina.

Las formas de corrupción más comunes en México están jerarquizadas de la siguiente manera: pagos indirectos a través de socios comerciales (67 %), pagos indebidos a través de nómina (25 %), proveedores ficticios-facturas falsas (25 %), regalos, viajes y entretenimiento indebidos (25 %), sobreprecio (17 %) y deficiencia en los controles de tesorería (17 %).

En el Índice de Percepción de Corrupción del 2015, publicado por la Organización Transparencia Internacional, presenta la ubicación de los países de América ante el entorno global, siendo Canadá el mejor evaluado, ubicado en el lugar nueve en la posición global, por lo que se considera como el país menos corrupto de América, seguido por Estados Unidos en la posición global 16, Uruguay en la posición 21, Chile en la 23, Costa Rica en la 40, Cuba en la 56, Jamaica en la 69, El Salvador, Panamá, Trinidad y Tobago en la 72, Brasil en la 76, Colombia en la 83, Perú en la 88, México en la 95, Paraguay en la 130 y Venezuela en la 158. Se puede observar que el país de Latinoamérica mejor ubicado es Chile y el peor es Venezuela.

A pesar de los grandes esfuerzos para eliminar estas prácticas en cada nación se sigue observando un crecimiento de este flagelo, que afecta de manera negativa a las instituciones públicas y privadas **(Figura 1).**

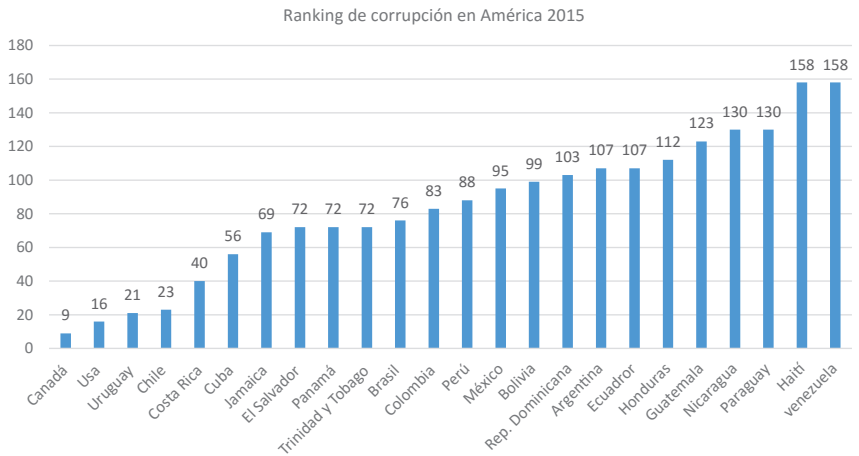

Figura 1. Índice de Percepción de la Corrupción en América, de 168 países en el mundo.
Tomada y modificada de: http://transparencia.org.es/wp-content/uploads/2016/01/tabla_sintetica_ipc-2015.pdf

USAID (2015), Agencia de los Estados Unidos para el Desarrollo Internacional, publica la percepción de la corrupción en los países de América y ubica a Venezuela en el primer lugar seguida de Colombia y Argentina en tercer lugar, Perú en el quinto lugar y México en el noveno lugar; evidentemente, estos datos coinciden con los publicados por Transparencia Internacional en 2015 **(Figura 2).**

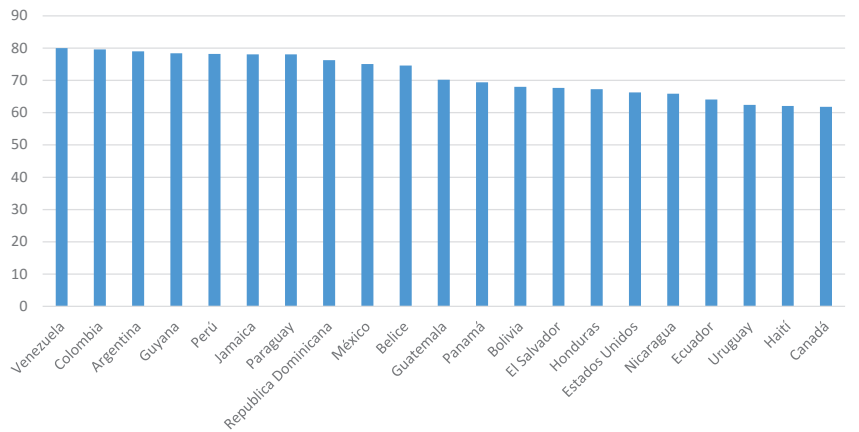

Figura 2. Percepción de corrupción 2014.
Fuente: García, Montalvo y Seligson (2015).

Desde una perspectiva global y latinoamericana se puede observar que México ha ido mejorando de manera progresiva en el enfrentamiento de la corrupción gracias a grandes esfuerzos; sin embargo, sigue mostrando cifras muy altas de corrupción en comparación con otros países de Latinoamérica **(Figura 3).**

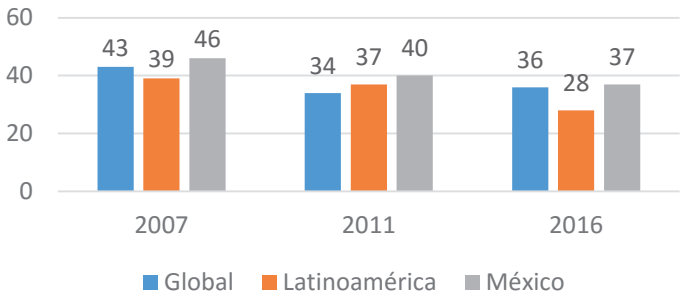

Figura 3. Porcentaje de corrupción por años.
Fuente: Adaptación de datos proporcionados por transparency.org

Chile, pese a estar en mejor posición que los demás países de Latinoamérica, reporta desde el 2003 hasta el 2015, altas cifras de percepción de corrupción por parte de sus ciudadanos: 70 % de manera general y un 57 % para los organismos públicos.

Como ya se dijo, la OMS ha definido un modelo para combatir la corrupción en la industria farmacéutica. La estrategia con la que se inició este modelo en varios países fue orientada a la promoción de la práctica ética y aplicación de medidas de anticorrupción en el sector farmacéutico, con los siguientes objetivos:

1. Incrementar la transparencia y la regulación en todo el sistema de proveedores de productos farmacéuticos.
2. Promover la integridad institucional en el sector farmacéutico.
3. Medir el impacto de la corrupción en el sector farmacéutico e integrarlos en la agenda de la política pública en salud.
4. Institucionalizar el GGM en todo el sistema de proveedores del sector farmacéutico.

El modelo propuesto por la OMS, tiene tres fases:

1. **Fase I:** realizar un diagnóstico de la transparencia en el ámbito nacional para conocer el tamaño de la corrupción a la que se enfrentará y sus implicados; además, tipificar el delito de crimen económico en el sector salud y elaborar los reportes correspondientes.
2. **Fase II:** desarrollar el programa nacional GGM y diseñar la plataforma oficial para la ejecución, evaluación y control del mismo.
3. **Fase III:** implementar el GGM e integrarlo en el Plan Nacional de Salud para un período de cuatro años o más **(Figura 4).**

Figura 4. Integración de las tres fases para combatir la corrupción en la industria de la salud.
Tomada y modificada de: OMS, WHO/EMP/MIPC/2013.

Este estudio del GGM ha marcado la pauta para que en el futuro inmediato la OMS desarrolle trabajos relacionados con la transparencia y gobernanza para el sector salud.

Caso Marruecos

El caso de Marruecos para combatir la corrupción, ha propuesto un modelo para fortalecer el sector salud que va más allá de la lucha contra la corrupción en los hospitales o clínicas; trata este delito dentro de un sistema integral que involucra a todos los grupos de interés para diseñar un modelo orientado hacia la prevención; dicho modelo fue desarrollado en los primeros años del nuevo milenio y marcó la pauta para el Plan Nacional de Salud del período 2008-2012.

El modelo anticorrupción elaborado en Marruecos contempló cinco fases: en la primera fase se realizó un análisis de riesgo, prácticas corruptas, actores e impulsores de la corrupción; en la segunda fase se marcó las prioridades para encontrar las razones de la corrupción, definir los objetivos y establecer los criterios; en la tercera fase se definió unas medidas

anticorrupción, unas metas claras y alcanzables en el corto y mediano plazo, unos indicadores medibles y unos niveles de responsabilidades; en la cuarta fase se presupuestó la ejecución del plan con los recursos necesarios para esta labor; y en la quinta fase se diseñaron los esquemas de monitoreo de las prácticas administrativas y los formatos de resultados esperados en el sector salud.

Es interesante en el caso de Marruecos como lograron simplificar la complejidad del sistema de salud, definiendo todas las actividades de apoyo: administración e insumos médicos (adquisiciones y mantenimiento), administración de recursos humanos (asignación de recursos humanos, eliminando el nepotismo y amiguismos como práctica muy común para los altos cargos administrativos) y administración del circuito médico (etiquetado/registro, adquisición/oferta y distribución). También se diseñaron actividades del proceso horizontal con su debida inspección y controles de conformidad. Para complementar el modelo se integró el servicio de salud con orientación e información, acceso y admisiones, administración de urgencias, planificación de acciones médicas, facturación y pagos.

Los actores clave definidos por el sistema de salud para prevenir la corrupción fueron señalados como: a) responsables del pago (seguros médicos, seguridad social, pago privado y público), b) agencia reguladora gubernamental, c) proveedores de medicinas y equipos médicos, d) proveedor público y privado, e) pacientes y f) otros insumos. En este modelo el paciente es considerado como un elemento más del sistema, por lo que se sugiere diseñar un nuevo modelo en donde todos los grupos de interés (*stakeholders*) graviten alrededor del bienestar del paciente.

El modelo de Marruecos, falló por varias razones:

1. No hubo voluntad política para mantener el programa.
2. Falta de liderazgo para un programa nacional.
3. Se trabajó por varios años en el diagnóstico, diseño del sistema y elaboración del plan de acción, pero se falló en la implementación y operación del mismo.
4. No hay reglas claras de monitoreo, auditorías ni evaluación.
5. No se contó con los recursos necesarios para la operación del modelo en el ámbito nacional.

6. Se pueden observar en el modelo fallas en la inclusión de actores clave.
7. El nivel de percepción de corrupción en Marruecos para el sector salud ha estado en cifras superiores al 80 %, lo que lleva a sospechar que es un problema enraizado y de años.
8. El sistema debe integrar otros sectores claves como económico, industrial, etc.

Caso Colombia

En el caso de Colombia se puede observar que la corrupción está coludida entre el sector público y privado, ya que el desfalco en los últimos 10 años (robos billonarios) ha llevado a la clausura de entidades prestadoras de servicios de salud (EPS). Las EPS han realizado multimillonarios cobros dobles al sistema: COP 2.2276.168, 1,6 billones en costos para el Fosyga (Fondo de Solidaridad y Garantía), 1.426 millones por medicamentos o servicios a personas muertas, 22.153 millones se reembolsaron a nombre de pacientes que no aparecen en la base de datos única de afiliados y 48.352 millones por pago de insumos y medicamentos que estaban incluidos en el Plan Obligatorio de Salud (POS) (El Espectador).

El Fosyga y la Superintendencia de Salud, que dependen cien por ciento del Ministerio de Salud, son los dos entes involucrados en los grandes robos de dinero y en especie.

Ya se conocen las EPS corruptas que han dejado sin empleo a más de 20.000 familias en todo el país. En la **Figura 5** se pueden visualizar los entes reguladores, pagadores y las entidades prestadoras y administradoras del sistema de salud colombiano; se muestra con línea gris el flujo del dinero sin corresponsabilidades entre el Fosyga y las EPS-IPS y con color amarillo y rojo, el flujo de buenas prácticas, transparencia, rendición de cuentas y sanciones por parte de la Superintendencia de Salud; la **Figura 5** permite ver que la falla fundamental está en la cabeza, esto es, en el Fosyga, y en las falencias del sistema por la falta de modelos y procesos claros de la Superintendencia.

Conclusión

Se propone el modelo de ética sostenible para que se implemente en el sector salud, tal y como se ha estado implementando de manera parcial en el sector turismo de México. Integrar los componentes éticos y de responsabilidad social empresarial en el sector salud ayudará a prevenir los actos de corrupción **(Figura 6).**

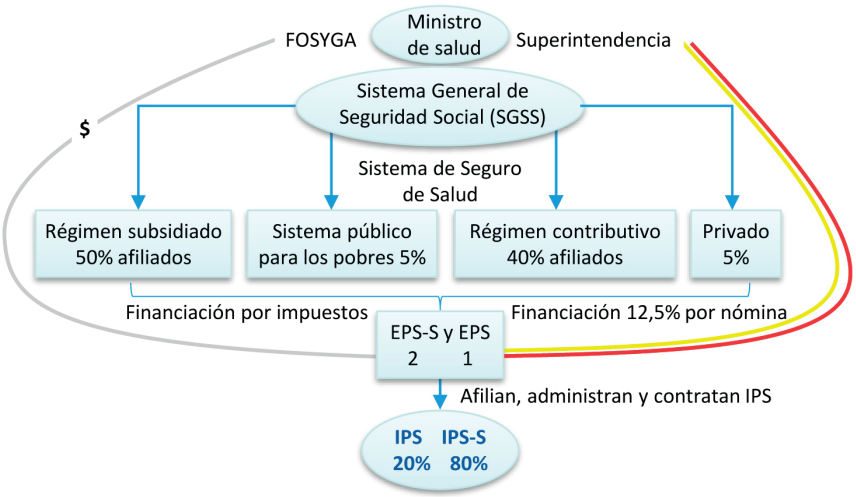

Figura 5. Enfoque integral de los grupos de interés del sector salud de Colombia.

Figura 6. Integración de la ética y la responsabilidad social empresarial.
Tomada y modificada de: Pérez, Garzón e Ibarra (2016).

Se sugiere en la **Figura 7** poner en el centro de las decisiones el bienestar del paciente y que el Gobierno asuma su papel como ente regulador, supervisor y ordenador del sistema de salud con todos los grupos de interés: las EPS o conocidas como empresas administradoras del sistema, las IPS o instituciones y/o organizaciones prestadoras de los servicios

médicos-hospitalarios y la ubicación dentro del sistema de salud de dichos grupos (ampliamente conocidos por el extranjerismo *stakeholders*).

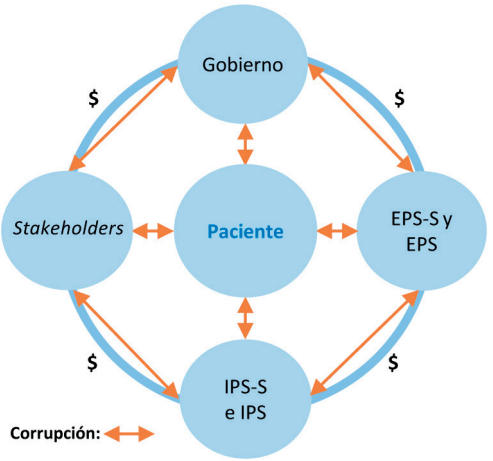

Figura 7. Modelo para prevenir la corrupción en el sector salud de Colombia.

En este modelo, cada grupo de interés *(stakeholders)* tiene su respectivo modelo de negocios y venas conectoras de los riesgos de corrupción entre todos los actores. ¿Quién es el corrupto en este modelo? Todos los actores son considerados con alto riesgo de caer en las redes de la corrupción. Actualmente no existen los vasos comunicantes para que la corrupción fluya dentro de un marco tolerable. En China ya se definieron agravantes de este delito y hasta se aplica la pena de muerte en algunos casos.

Los casos de estudio de Marruecos, Chile, Perú y Colombia son claros ejemplos de la urgencia de diseñar e implementar la gobernanza, de modificar las leyes con penas superiores a los 20 años de cárcel y de definir la responsabilidad civil y el pago a las víctimas del delito económico. También quedó en evidencia que toda acción para atender la corrupción en un sector necesita de un sistema, inclusive, de todos los sectores de la economía. Ya quedó claro que son insuficientes las buenas intenciones y la buena voluntad de los grupos de interés, así que se tiene que evolucionar hacia la gobernabilidad y sanciones penales ejemplares con reparación de las víctimas.

Referencias

- García, S., Montalvo, D. y Seligson, M. (2015). Cultura política de la democracia en Colombia. USAID. Recuperado de: http://www.vanderbilt.edu/lapop/colombia/Colombia-Informe-Especial-2015-070915-W.pdf
- Fink, H. y Hussmann, K. (2013). Combatir la corrupción con estrategias sectoriales: sector salud Marruecos. *Chr. Michelsen Institute, CMI, U4 Anticorruption Resource Center*. Recuperado de: www.U4.no. https://issuu.com/cmi-norway/docs/u4issue-2014-01
- Pérez, L., Garzón, M. e Ibarra, A. (2016). Código de ética empresarial para las pymes: marco de referencia para la sostenibilidad y responsabilidad social empresarial (RSE). Recuperado de: http://www.revistaespacios.com/a15v36n02/15360211.html
- PwC, Encuesta sobre Delito Económico. (2016). Recuperado de: www.pwc.com/crimesurvey
- WHO Medicines Strategy (2004-2007). *Countries at the core. Geneva, World Health Organization*.
- WHO/EMP/MIPC/2013.1. (2004-2012). *Evaluation of the good governance for medicines programme*. Recuperado de: www.who.int/medicines/areas/governance
- http://www.elespectador.com/noticias/investigacion/eps-realizaron-multimillonarios-cobros-dobles-al-sistem-articulo-655986
- https://www.transparency.org/whatwedo/publication/people_and_corruption_africa_survey_2015
- http://transparencia.org.es/wp-content/uploads/2016/01/tabla_sintetica_ipc-2015.pdf

El capital humano en el desarrollo del encargo de auditoría: acercamiento desde las Normas Internacionales de Control de Calidad

Mario Heimer Flórez Guzmán[1*]; Ludivia Hernández Aros[1];
Laura Constanza Gallego Cossio[1]; Luis Eduardo Parra Hernández[1];
Martha Lucía Mayolo Bonilla[1]

Resumen

El presente artículo da cuenta de la importancia que tiene el capital humano en el encargo de una auditoría, analizado aquel desde las Normas Internacionales de Control de Calidad (NICC); la investigación es de corte documental y de carácter descriptivo explicativo, y se soporta en la teoría de la efectividad, la teoría del control y en las teorías adyacentes de capital humano; además, se fundamenta en las mencionadas NICC.

Como conclusión se obtuvo que la valoración del capital humano en el desarrollo de una auditoría depende de una serie de indicadores, los cuales relacionan cualidades de los empleados con la situación de un ente (valoración de carácter subjetivo), que es reflejada en el nivel de rotación del personal, el perfil del empleado, el conocimiento, la motivación y la formación del mismo para llevar a cabo un encargo de auditoría.

Palabras clave: valoración del capital humano, encargo de auditoría, NICC, teoría del control y aseguramiento.

Introducción

El capital intelectual, o más conocido como activo intangible, se presenta hoy en día como un factor clave para generar competitividad y eficacia; es por ello que se hace necesario conocer y valorar sus componentes, aunque pasa inadvertido debido a que su valoración se considera un poco compleja.

[1] *Facultad de Contaduría Pública, Universidad Cooperativa de Colombia, sede Ibagué.*
[*] *Contacto: mario.florez@campusucc.edu.co*
https://doi.org/10.22209/Cice.n2a06

A partir de lo anterior se caracterizan los elementos y variables del capital humano que se deben tener en cuenta en la aplicación de las NICC para un encargo por medio de indicadores y de un esquema que permita tener claridad sobre los elementos y variables que generan mayor eficacia.

Finalmente, el propósito del estudio es valorar el capital humano desde las NICC para la ejecución de una auditoría.

Análisis de capital intelectual para el desarrollo de un encargo de auditoría

El capital intelectual es definido como un valor intangible y de primera necesidad; es el factor con más relevancia dentro de las organizaciones por su extensión. Abarca capitales como el humano, el relacional y el estructural, y es definido por Alama (2008) como el "conjunto de activos intangibles que poseen las empresas, y que conjuntamente con los activos tangibles forman parte de su patrimonio" (p. 56). En la **Figura 1** se evidencia la configuración del capital intelectual.

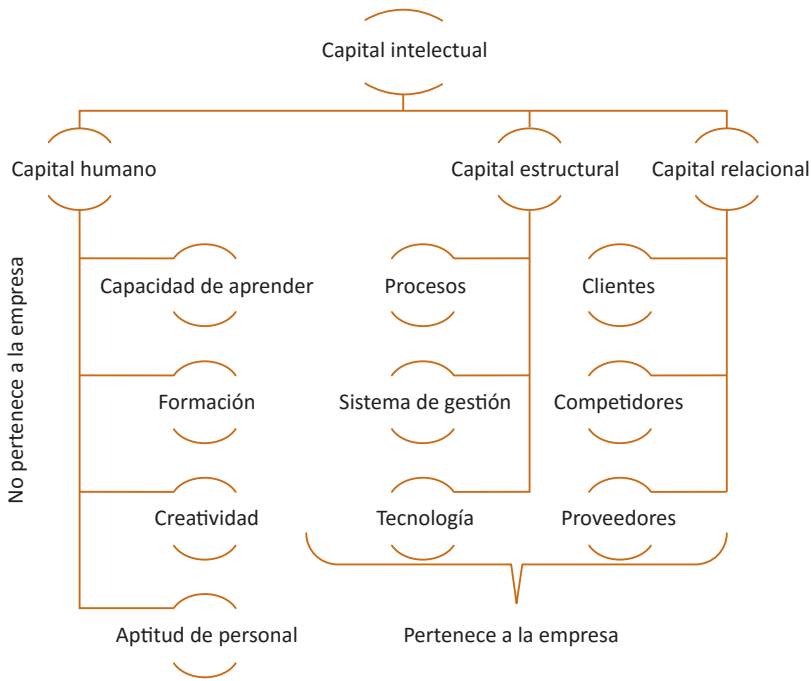

Figura 1. Configuración del capital intelectual.
Tomada y modificada de: Gutiérrez, Parra y Mayolo (2016).

Ahora bien, el capital humano lo compone el personal que labora en la organización y está determinado por la capacidad de aprender, por la formación del empleado, por la creatividad y por la aptitud en la ejecución de las actividades. López y Grandino (2005) definen el capital humano como el conocimiento tácito o explícito de las personas que ayuda a reestablecer el conocimiento, caracterizándose por ser propio del empleado (no es propiedad de la empresa), es decir, es un factor que agrega valor a las organizaciones y de él se desprenden capitales como el estructural y el relacional.

Altuve (2005) define el capital humano como aquel que incluye todas las capacidades individuales, destrezas, conocimientos, experiencia profesional, capacitación, incorporación de nuevas tecnologías y su aporte a la empresa; lo anterior, en función del crecimiento organizacional de forma armónica y coherente. De igual manera, esta definición se ajusta a lo propuesto por Destinobles (2006): el conjunto de conocimientos y de competencias que poseen los individuos. En la **Figura 2** se clasifica el capital humano en los niveles emocional y operativo.

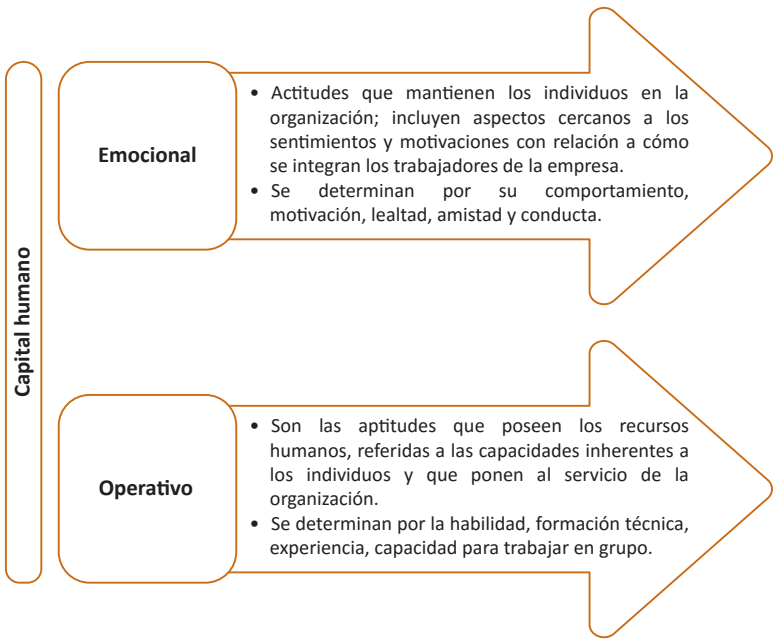

Figura 2. Clasificación del capital humano.
Tomada y modificada de: Elaboración propia (2016) a partir de Navas y Ortiz (2002).

Su importancia tiene que ver con la productividad de las organizaciones; hay que tener en cuenta que las bases de mejora continua en las empresas son "las personas" porque estas poseen potencial suficiente para alcanzar resultados; lo anterior es aplicable en un encargo de auditoría, ya que el capital humano debe cumplir con los estándares profesionales que incluyen "conocimientos y competencias" propios de su campo de experticia.

López y Grandino (2005) proponen seis categorías del capital humano: perfil del empleado, rotación del personal, educación, compromiso y motivación, formación y resultados obtenidos, según las metas organizacionales. Estas categorías contienen aspectos cualitativos de los empleados con base en el conocimiento individual y colectivo que genera aprendizaje y, para la empresa, eficiencia y eficacia en el desarrollo de sus actividades.

El capital humano en el encargo de una auditoría es valorado a través de indicadores que reflejan el seguimiento de las categorías (muy válidas) para que al planear, ejecutar e informar los hallazgos tengan en cuenta dicho capital. En la **Tabla 1** se describen categorías y su medición por parte del líder auditor.

Tabla 1. Indicadores del capital humano.

Categoría	Indicadores	Análisis del indicador
Perfil del empleado	A. Número de empleados según el sexo.	Distribuye los empleados según el sexo.
	B. Distribución de empleados según la edad.	Determina la edad promedio de la empresa.
	C. Distribución de empleados por áreas.	Distribuye los empleados según las áreas de la empresa.
Rotación del personal	A. Número de empleados nuevos.	Nuevas contrataciones en el periodo.
	B. Número de empleados retirados.	Empleados que se retiran por decisión propia.
	C. Número de empleados despedidos.	Empleados que son retirados por decisión de la empresa.
	D. Número de ingresos/ número de salidas*100.	Porcentaje de reemplazo del personal.
Educación	A. Distribución de empleados según nivel educativo.	Determina qué nivel educativo tienen los empleados.
	B. Años de experiencia por empleado.	Determina cuánta experiencia tiene la empresa en sus empleados.

Continúa en la próxima página.

Continuación de la Tabla 1. Indicadores del capital humano.

Categoría	Indicadores	Análisis del indicador
Compromiso y motivación	A. Número de empleados ascendidos/empleados totales.	Determina el porcentaje de ascensos de los empleados.
	B. Antigüedad de los empleados.	Determina la experiencia de los empleados en la empresa; es de gran utilidad para evitar reiteración de errores.
	C. Porcentaje de empleados que se sienten con reconocimiento.	Define el porcentaje de empleados que se sienten reconocidos por su labor.
	D. Porcentaje de empleados que sienten que sus opiniones son tenidas en cuenta.	Señala el porcentaje de empleados que se sienten parte de la empresa.
	E. Porcentaje de empleados que se sienten satisfechos con su labor.	Define los empleados que son felices realizando su labor.
Formación	A. Inversión en formación/ empleados totales.	Mide la inversión que se realiza por empleado para generar bienestar en cada uno.
	B. Número de días en formación por empleado.	Define el número de días que los empleados invierten en formación.
	C. Aplicación de pruebas para comprobar los procesos internos y su eficiencia.	Mide el grado de cumplimiento y conocimiento de los procesos internos de la compañía.
	D. Número de formaciones realizadas en el año.	Establece el número de formaciones que se realizan en un periodo.
Resultados	A. Porcentaje de empleados que se sienten satisfechos en la empresa.	Define el porcentaje de los empleados que se encuentran satisfechos en la compañía.

Fuente: Gutiérrez, Parra y Mayolo (2016).

Ahora bien, las NICC, expedidas en el Decreto 2420 de diciembre de 2015, establecen que la firma de auditoría deberá implementar un sistema de control de calidad que le proporcione una seguridad razonable, de acuerdo con las características del personal: capital humano con conocimiento en normas profesionales, conocimiento técnico (incluido el de la tecnología de la información relevante), con capacidad para aplicar el juicio profesional, y el conocimiento que tenga el equipo del encargo en cuanto a las políticas y procedimientos de control de calidad de la firma (Decreto 2420 Apartado

31). Por otro lado, los informes presentados en desarrollo del encargo de auditoría contendrán los aspectos asociados a la calidad en su preparación.

A continuación, en la **Tabla 2** se presentan las variables y sus elementos del capital humano que se deben tener en cuenta en la aplicación de las NICC.

Tabla 2. Elementos y variables del capital humano en el encargo.

Variables	Elementos	Riesgos	Nivel de riesgo
Capacidad	Conocimiento	Falta de conocimiento sobre el desarrollo de un encargo.	Alto
		Educación limitada para el desarrollo de encargos.	
		Caracterización inadecuada de perfiles para el desarrollo de un encargo.	
		Conocimientos limitados sobre el desarrollo de un encargo de auditoría.	
	Habilidad	Constantes cambios en el personal, lo que genera reprocesos de capacitación.	Bajo
		Falta de habilidades y técnicas en la aplicación de auditorías.	Alto
	Talento	Falta de actualizaciones para aprender nuevas técnicas en el desarrollo de un encargo.	Medio
Comportamiento	Aplicación de valores	Carencia de valores y ética en el desarrollo de encargos de auditoría.	Alto
	Motivación	Déficit de motivación y compromiso para desarrollar el trabajo.	Medio
Esfuerzo	Recursos físicos	Escasez de recursos físicos en el personal que desarrolla el encargo.	Bajo
	Recursos mentales	Déficit de capacidad mental en el desarrollo del encargo de una auditoría.	Alto
	Resultado	Insatisfacción con el resultado del trabajo desempeñado.	Medio

Fuente: Gutiérrez, Parra y Mayolo (2016).

Teijeiro, García y Mariz (2010) determinan que el capital humano está dividido en elementos de dimensión del presente y dimensión del futuro; además, exponen el modelo *Intellectus*, que contiene valores y actitudes, aptitudes y capacidades del individuo **(Figura 3).**

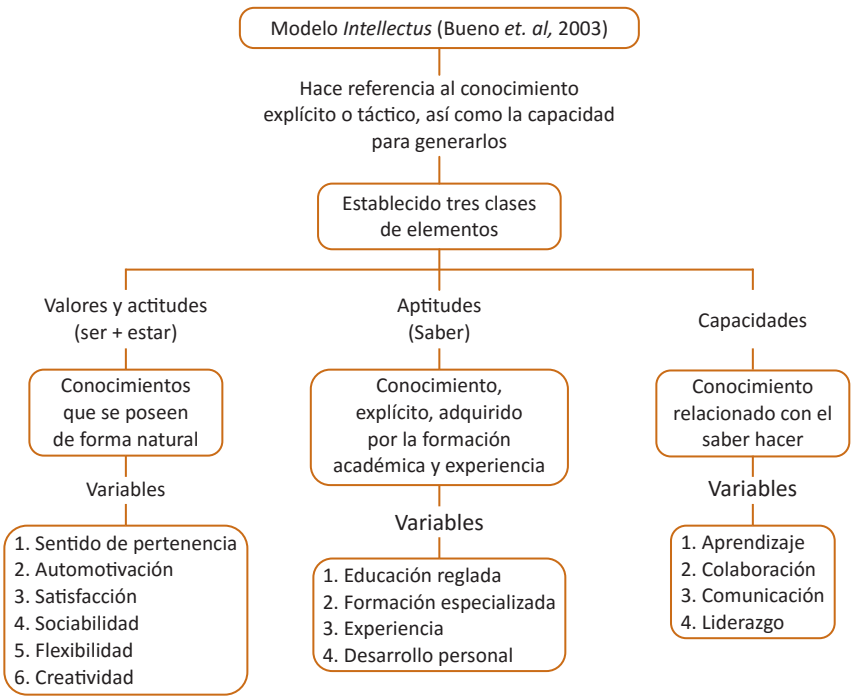

Figura 3. Modelo *Intellectus.*
Tomada y modificada de: Elaborado por Aldana y Arias (2016) a partir de Teijeiro, García y Mariz (2010).

Las NICC exponen las responsabilidades que tiene el auditor independiente o la firma de auditores en relación con su sistema de control de calidad, las revisiones de estados financieros y otros encargos; parte del objetivo mismo de mantener la calidad del trabajo realizado para que genere unos resultados que proporcionen seguridad razonable; es allí donde la firma de auditoría y su personal deberán cumplir las normas profesionales y los requerimientos legales y reglamentarios aplicables (Decreto 2420 de 2015).

Lo anterior refleja la importancia del capital humano en la ejecución del encargo, donde el auditor evaluará todas las categorías, variables y elementos

en función de que exista suficiente personal con la competencia, la capacidad y el compromiso con los principios éticos necesarios para: a) realizar encargos de conformidad con las normas y con los requerimientos legales y reglamentarios aplicables, y b) permitir a la firma auditora o a socios la emisión de informes adecuados en función de las circunstancias (Decreto 2420).

Conclusiones

El capital humano es considerado como el activo que no le pertenece a la empresa y está conformado por conocimientos y capacidades individuales del empleado. En el desarrollo de un encargo la ejecución depende de este capital y su éxito es valorado de gran manera a través de las NICC.

Es de gran importancia que las firmas de auditoría evalúen su capital humano y desarrollen actividades que fortalezcan las habilidades y competencias específicas del auditor, quien estará a cargo de los procesos (planeación, ejecución e informe), fortaleciendo así el enfoque ético de la responsabilidad social de las organizaciones para generar transparencia y confianza en el personal que ejecuta la auditoría, lo que permite un mayor nivel de seguridad de la firma.

Se hacen necesarias la capacitación y formación del auditor desde los aspectos políticos en términos de normatividad vigente (decretos 2420 y 2496 de 2015), en lo social, con respecto al ajuste a los estándares internacionales y a soluciones a dilemas éticos que son inherentes al proceso de auditoría; y en lo técnico, en habilidades y destrezas propias de la auditoría administrativa (control interno) y contable, así como en el uso de herramientas especializadas para el análisis de datos. Lo anterior es viable en cualquier tipología de auditoría: forense, de gestión, ambiental, social, de sistemas, financiera, de cumplimiento y otras emergentes.

Referencias

- Alama Salazar, E. M. (2008). *Capital intelectual y resultados empresariales en las empresas de servicios profesionales de España* (tesis doctoral). Universidad Complutense de Madrid, España.
- Aldana Aragón, E. V. y Arias Canizales, L. T. (2016). *Valoración del capital humano en el proceso de auditoría de control interno* (tesis de pregrado). Universidad Cooperativa de Colombia, Ibagué, Colombia.
- Altuve, J. E. (2005). Capital intelectual y generación de valor. *Revista Actualidad Contable Faces*, *5*(5), 7-22. Recuperado de: http://www.redalyc.org/pdf/257/25700502.pdf

- Colombia. (2015). Decreto 2420 de 2015, por medio del cual se expide el Decreto Único Reglamentario de las Normas de Contabilidad, de Información Financiera y de Aseguramiento de la Información y se dictan otras disposiciones. Diario Oficial, 49.726, Bogotá, 14 de diciembre de 2015. Recuperado de: http://wp.presidencia. gov.co/sitios/normativa/decretos/2015/decretos2015/DECRETO%202420%20DEL%2014%20DE%20DICIEMBRE%20 DE%202015%20-%20copia.pdf
- Colombia. (2015). Decreto 2496 de 2015, por medio del cual se modifica el Decreto 2420 de 2015 Único Reglamentario de las Normas de Contabilidad, de Información Financiera y de Aseguramiento de la Información y se dictan otras disposiciones. Diario Oficial, 49735, Bogotá, 23 de diciembre de 2015. Recuperado de: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%202496%20DEL%2023%20DE%20DICIEMBRE%20DE%202015.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=excepcion_al_tratamiento_bajo_niif_de_la_cartera_de_creditos_y_de_los_aportes_sociales_en_cooperativas
- Destinobles, A. G. (2006). *El capital humano en las teorías del crecimiento económico*. Madrid: B - EUMED. Recuperado de: http://www.ebrary.com
- Gutiérrez Portela, F., Parra Hernández, L. E. y Mayolo Bonilla, M. L. (2016). *Valoración del capital humano en el desarrollo del encargo de auditoría: un análisis desde las Normas Internacionales de Control de Calidad* (tesis de pregrado). Universidad Cooperativa de Colombia, Ibagué, Colombia.
- López Cabarcos, M. A. y Grandío Dopico, A. (2005). *Capital humano como fuente de ventajas competitivas. Algunas reflexiones y experiencias*. Barcelona: Netbiblo. Recuperado de: http://ruc.udc.es/dspace/bitstream/handle/2183/11793/8497451198.pdf?sequence=2
- Navas López, J. E. y Ortiz de Urbina, M. (2002). El capital intelectual en la empresa: análisis de criterios y clasificación multidimensional. *Revista Economía Industrial*, *346*(1), 163-172. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=716729
- Teijeiro Álvarez, M., García Álvarez, M. T. y Mariz Pérez, R. M. (2010). La gestión del capital humano en el marco de la teoría del capital intelectual. *Revista Economía Industrial*, *378*(1) 45-57. Recuperado de: https://www.researchgate.net/publication/277263709_La_gestion_del_capital_humano_en_el_marco_de_la_teoria_del_capital_intelectual_una_guia_de_indicadores

Afectación del cibercrimen en las pymes

Rodrigo Alcides Patiño Arango[1]

Resumen

Así como la tecnología y el *software* avanzan a gran velocidad, los delincuentes cibernéticos, como se les suele llamar, también se están capacitando con el fin de contrarrestar los obstáculos que se presenten y así alcanzar sus objetivos.

Por lo tanto, la regulación que se viene implementado para intervenir estos fraudes es contundente; sin embargo, los delincuentes cibernéticos ignoran las consecuencias de sus actos, pues su propósito está dado en alcanzar las metas trazadas para tener una "mejor calidad de vida", según sus perspectivas.

Por lo anterior, la sensibilización que a las entidades se les ofrece por parte de personas expertas en la materia, deben ser tenidas en cuenta, pues el delincuente no cesa de mejorar sus estrategias e idear nuevos métodos para incurrir en los delitos, por lo tanto, como estos están en constante ejecución de estrategias para cometer sus fraudes, entonces todas las charlas orientadas a evitar caer en este delito, ayudarán a salvaguardar lo que se está administrando.

Palabras claves: pymes, fraude electrónico, delitos económicos.

Introducción

Las pymes que se encuentran en un nivel de crecimiento constante están llamadas a utilizar la tecnología; por lo tanto, es recomendable que tengan la suficiente capacitación en cuanto a la adquisición y uso de la misma, de tal suerte que se conviertan en aliados estratégicos de las entidades financieras como pioneras en el manejo de la seguridad para

[1]*Facultad de Ciencias Básicas e Ingeniería, Uniremington.*
Contacto: coordinador.basicas@uniremington.edu.co
https://doi.org/10.22209/Cice.n2a07

sus transacciones, y de esta manera evitar su exposición a los actos de los delincuentes cibernéticos.

Es importante que las pymes de hoy sean proactivas frente a las dificultades que puedan afrontar ante los grandes avances tecnológicos que cada día están inundando el medio y, especialmente, ante las grandes exploraciones que hacen los criminales cibernéticos, quienes han extraído miles de millones de dólares de manera ilícita, con el evidente detrimento económico que ello implica.

El fraude electrónico, uno de los pilares de los delincuentes cibernéticos

Con la definición de fraude electrónico nos daremos cuenta de la manera como los delincuentes cibernéticos se apropian de la información de las personas, mediante un estudio exhaustivo y muy certero cuyo fin es trasladar o extraer lo que tienen en las cuentas de las entidades financieras sin dejar rastro alguno del proceso realizado.

Rodríguez (2014, p. 290) define el fraude electrónico como…

> *… la conducta desplegada por un tercero ajeno al titular del medio electrónico de pago, no autorizada ni consentida por este, por conductos electrónicos y que le causa un perjuicio. Como el escenario en el que un tercero se apropia de los datos de identificación de la tarjeta de crédito o de cualquier medio electrónico de pago individual y de su titular y, empleando los mismos, celebra contratos a distancia por medios electrónicos, telefónicos o telemáticos, debiendo aclarar que más bien utiliza dichos datos para efectuar el pago de las obligaciones derivadas de dichos contratos a distancia, realiza transferencias electrónicas de dinero a cuentas previamente determinadas, o bien efectúa retiros de dinero en efectivo a través de cajeros electrónicos.*

Según la Confederación de Cámaras de Comercio (Confecámaras, 2016) en su informe de primer trimestre de 2016, en Antioquia se ubican 294.359 mipymes, las cuales se ven abocadas a incursionar en los nuevos mercados para competir con precio, calidad y servicio, y esto las lleva a tomar decisiones que deben ser analizadas por sus implicaciones en el corto, mediano o largo plazo.

Así mismo, la Ley 590 (Congreso de Colombia, 2000) establece claramente la cantidad de personas que la conforma (el personal debe

ser mayor que 10 y menor que 200 personas); por lo tanto, estar hoy dentro de este *ranking* es una ventaja competitiva y comparativa, pues muchas de ellas no han resistido a los cambios que se han presentado, ya sea desde la exigencia de los clientes, desde la competencia o desde los nuevos requerimientos que exige el Estado. Así que este tipo de empresa debe trabajar de la mano con las entidades financieras, de tal manera que puedan, en un alto porcentaje, implementar niveles de seguridad que coadyuven a salvaguardar la información de sus empleados, clientes y proveedores para evitar fraudes.

Por lo anterior, en la actualidad una gran cantidad de mipymes conservan lo tradicional de la administración, supervisión y control, pues consideran que lo que se hizo varios años atrás se puede replicar hoy y que hasta el momento se ha sobrevivido pese a la gran competencia que existe, pues creen que los clientes que consumen sus productos y servicios seguirán siendo fieles mientras subsistan.

Además, algunas de las mipymes realizan sus procesos de forma manual, es decir, se comercializa el producto o el servicio y el cliente paga de contado, hace la consignación en la cuenta de la empresa o por medio de cheque, o tiene un crédito; pero, en todo caso, no hace uso de medios electrónicos para el pago de sus obligaciones dado que esto puede generar un sobrecosto.

Un ejemplo de lo que puede suceder cuando una pyme desea implementar nuevas tecnologías para que su negocio siga mejorando es el siguiente: si tiene un producto que vale COP 15.000, con una utilidad del 10 % (COP 1500), y el cliente lo va a cancelar haciendo uso de su dinero plástico, entonces, la entidad financiera le puede cobrar a la empresa alrededor de COP 600, lo que reduce, evidentemente, la utilidad a COP 900. Para que el deterioro de la utilidad no sea tan alto, la idea es que las transacciones tengan incluidos varios productos, aunque esto no depende de la empresa, sino del cliente que está comprando.

Dado que la empresa continúa su crecimiento de forma positiva, se ve en la obligación de implementar nuevas alternativas que coadyuven al mejoramiento; es ahí cuando debe usar las herramientas tecnológicas e incursionar en el mundo de la cibernética, el cual cambia sustancialmente la manera de realizar los procesos y les brinda a los clientes nuevas formas de pago y la posibilidad de identificar desde su sitio web toda la diversidad de productos y servicios.

Sin embargo, como la empresa está iniciando su proceso de incursión en el mundo de las tecnologías de la información y la comunicación, está expuesta a lo que hoy se denomina cibercrimen; su vulnerabilidad es total, pues los delincuentes cibernéticos ponen todo su empeño para atacar estas empresas u organizaciones recién llegadas al espacio cibernético.

Así como las empresas de hoy realizan todo un proceso de investigación de mercados para ingresar o diversificar un nuevo producto o servicio, también los delincuentes cibernéticos investigan para encontrar los puntos débiles y defraudar.

De esta manera, el uso e implementación de la cibernética y de las tecnologías de la información y las comunicaciones implican para la empresa una inversión significativa si quieren disminuir substancialmente el riesgo de crimen cibernético; garantizar la seguridad exige capacitación permanente de las entidades competentes y, especialmente, que las empresas se conviertan en aliadas estratégicas de las entidades financieras, las cuales están en permanente actualización de sus procesos para evitar el fraude electrónico. Deben adquirir *softwares* licenciados tanto de sistemas operativos como de aplicativos, *software* de seguridad y antivirus; además, requerirán de personal calificado cuya mano de obra será más costosa.

De acuerdo con la encuesta realizada por PricewaterhouseCoopers (PwC) (2016, p. 7)...

> *... las empresas hoy más que antes buscan su expansión, aumentar su oferta de productos y servicios, y llegar a más personas en distintas regiones y comunidades, un objetivo estratégico que necesita fundamentalmente de la tecnología y que trae consigo riesgos para la organización al ampliar su marco de actuación en entornos diferentes y con nuevas formas de hacer negocios.*

Habría que decir también que debido a la gran competencia y a las nuevas exigencias de los clientes, la empresa debe expandir su portafolio de productos y servicios, de tal manera que su actividad económica no se vea afectada.

De igual modo, la PwC (2016, p. 8) dice que la delincuencia económica no conoce fronteras y que es un riesgo siempre latente, dispuesto a vulnerar la puerta de seguridad de las organizaciones y a violar las barreras de control implementadas.

Según nos dice la PwC (2016, p. 8), hace unos años la distancia nos protegía de los delincuentes cibernéticos, hoy todo es diferente. El delincuente puede estar sentado junto a nosotros o ser nuestra antípoda y el riesgo no cambia: con la misma velocidad y oportunidad tendrá la posibilidad de convertirnos en su víctima. La diferencia estará en los controles de seguridad cibernética instalados para salvaguardar la información de la organización, los cuales evitarán las transacciones ilegales y el acceso indebido.

Según datos de la misma PwC (2016, p. 1), "el 32 % a nivel global, el crimen cibernético asciende este año al segundo puesto de delitos económicos reportados", "más de un tercio de las organizaciones en Colombia reportan haber sido víctimas del delito económico, el cual corresponde al 32 %" y "más de la mitad de los encuestados, el 61 % en Colombia, declaran que los defraudadores son actores al interior de la organización".

Desde luego, para Colombia estas cifras son preocupantes porque indican que somos los primeros en seguir estas prácticas ilícitas.

Cabe señalar que de acuerdo con la encuesta realizada por la compañía de auditoría Ernst & Young (EY) (2016, p. 1)...

> *... el soborno y la corrupción continúan representando una amenaza para el crecimiento global y contribuyen a la volatilidad de los mercados financieros. Por ello, organismos nacionales e internacionales coordinan sus enfoques y estrategias para investigar prácticas no éticas y, por su parte, los cuerpos de seguridad están centrando en detectar malas conductas individuales.*

De igual manera, la EY (2016) da a conocer medidas que permiten mitigar el riesgo de fraude electrónico en las empresas, entre las cuales están:

- Establecer políticas que fomenten la denuncia de conductas fraudulentas.
- Realizar evaluaciones periódicas del riesgo de fraude.
- Desarrollar un plan de respuesta a ataques cibernéticos para contar con una estructura de respuesta centralizada.
- Ejecutar un programa de cumplimiento integral contra la corrupción que incorpore técnicas de análisis de datos y mejorar la formación específica (p. 3).

Por otra parte, la firma de auditoría Deloitte (2016, p. 1) hace hincapié, en una de sus publicaciones sobre servicios de ciberseguridad, en que:

> *Las inversiones en seguridad cibernética se encuentran en un máximo histórico. Sin embargo, los ataques cibernéticos exitosos siguen en aumento, tanto en su número como en su sofisticación. Sin duda, la seguridad basada en el cumplimiento es una parte indispensable para abordar estas amenazas, pero hoy en día la mejor práctica es tener un enfoque proactivo basado en el riesgo. Sin embargo, teniendo en cuenta la frecuencia, la variedad e imprevisibilidad de los ataques, el objetivo de estar 100 % protegido no es realista ni viable económicamente.*

Por su parte, la Ley 1273 de 2009, en sus artículos 1 y 2, habla de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y otras infracciones, las cuales vienen aplicando los entes de seguridad y control. También está explícita cada una de las penalidades y las multas a las que se someten las personas que incurren en estos delitos.

Reseña de casos de fraude electrónico

1. Según la *Revista Semana* (2016, p. 1): "Colombia perdió $1 billón por ataques cibernéticos (...) la empresa de seguridad informática Cisco publicó un informe en el que señala las vulnerabilidades que tienen las empresas nacionales frente al cibercrimen".
2. Según el periódico *El Tiempo* (2015, p. 1): "Cibercrimen generó pérdidas por US$ 600 millones en Colombia (...) que el cibercrimen representa el 15 % de los ilícitos cometidos a empresas en Colombia".
3. Según el periódico *El Heraldo* (2015, p. 1): "Caen 18 de 'los Piratas del Caribe' por fraudes de más de $330 mil millones (...) que el Cuerpo Técnico de Investigación (CTI), bajo la coordinación de la Fiscalía 52 Seccional de la Estructura de Apoyo de Ibagué, detuvo de manera simultánea en Barranquilla, Soledad, Cartagena, Santa Marta, Ibagué y Bogotá a 18 integrantes de la banda de "Los Piratas del Caribe".
4. Según el periódico *El País* (2016, p. 1) un juez de garantía dictaminó cárcel para "el actual vicepresidente del sindicato de Bancolombia en Cali, por su presunta responsabilidad en el hurto de $484 millones a

través de la clonación de tarjetas de créditos y del fraude de datos de cuentas bancarias".

Conclusiones

Las pymes que desean incursionar en las tecnologías de la información y las comunicaciones deben analizar claramente la decisión que han de tomar, pues esto requiere de una buena inversión de capital y tiempo, acompañados de una excelente relación y comunicación con los entes encargados de estas tecnologías, y, por ende, con las entidades financieras, que son la clave para que las empresas sigan creciendo, de tal manera que la ejecución de la actividad económica siga su rumbo y pueda permanecer en el medio compitiendo con precio, calidad y buen servicio.

Los altos costos necesarios para la implementación de las nuevas tecnologías de la información y las comunicaciones serían equivalentes al nivel de seguridad al que están apuntando, pues garantiza que la trazabilidad de los procesos y manejo de información cumplan con los estándares de seguridad.

Referencias

- PricewaterhouseCoopers. (2016). Encuesta Global de Delitos Económicos Colombia. Recuperado de: https://www.pwc.com/co/es/publicaciones/crime-survey-2016.pdf
- Confecámaras. (2016). Nacimiento y supervivencia de las empresas en Colombia. Recuperado de: http://www.confecamaras.org.co/noticias/467-las-camaras-de-comercio-y-empresarios-de-todo-el-pais-dieron-inicio-a-su-reunion-cumbre-en-la-ciudad-de-cartagena
- Deloitte. (2016). Servicios de ciberseguridad, consultoría en riesgos empresariales. Recuperado de: http://www2.deloitte.com/co/es/pages/risk/solutions/servicios-de-ciberseguridad---deloitte-colombia---ers.html?icid=top_servicios-de-ciberseguridad---deloitte-colombia---ers
- Ernst & Young. (2016). La lucha contra el soborno y la corrupción, prioridad mundial para empresas y gobiernos. 14.ª Encuesta Global sobre Fraude. Recuperado de: http://www.ey.com/Publication/vwLUAssets/EY-encuesta-global-sobre-fraude-2016-resumen-ejecutivo/$FILE/EY-encuesta-global-sobre-fraude-2016-resumen-ejecutivo.pdf

- Ley 590. (2000). Disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=12672
- Periódico el Heraldo (2015). Caen 18 de los Piratas del Caribe por fraudes de más de $330 mil millones. *El Heraldo*. Recuperado de: http://www.elheraldo.co/nacional/caen-18-de-los-piratas-del-caribe-por-fraudes-de-mas-de-330-mil-millones-214764
- Periódico el País (2016). Así fue la investigación sobre fraude en Bancolombia. *El País*. Recuperado de: http://www.elpais.com.co/elpais/judicial/noticias/asi-fue-investigacion-sobre-fraude-bancolombia
- Periódico el Tiempo (2015). Cibercrimen generó pérdidas por US$ 600 millones en Colombia. *El Tiempo*. Recuperado de: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604
- Revista Semana (2016). Ataques cibernéticos le costaron al país 1 billón de pesos. *Revista Semana*. Recuperado de: http://www.semana.com/tecnologia/articulo/ataques-ciberneticos-le-costaron-al-pais-1-billon-de-pesos/464341
- Rodríguez, A. (2014). Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos. *Universitas, 63*(128), *285-314*. DOI: http://dx.doi.org/10.11144/Javeriana.VJ128.aerb

Impacto del cibercrimen: bajo la realidad aumentada

Feibert Alirio Guzmán Pérez[1]

Resumen

Este trabajo muestra algunos aspectos fundamentales sobre el impacto que presenta la incursión de nuevas tecnologías asociadas a la realidad aumentada y cómo estas repercuten de forma directa en el aspecto económico y financiero, tanto para maximizar utilidades en un mercado eficiente como para posibles desvíos hacia fraudes, especulación cibernética y cibercrímenes que llevan a mercados ineficientes. Se analiza el caso Pókemon GO y los muy recientes algoritmos matemáticos para automatizar la toma de decisiones en los mercados de capitales y divisas.

Palabras clave: cibercrimen, realidad aumentada, algoritmos matemáticos.

Introducción

Dentro de las tendencias tecnológicas, el cibercrimen persigue las redes sociales, el internet de las cosas, la realidad aumentada, el comercio electrónico, las transacciones financieras, etc., con el objetivo de vulnerar la seguridad informática. Sin embargo, plataformas como Facebook, MySpace, Twitter, WhatsApp, YouTube, Instagram, LinkedIn, ResearchGate, entre otras, permiten que los usuarios pongan a disposición y alcance de todos su información personal, lo cual repercute significativamente al no activar los controles de privacidad que estas ofrecen; tanto es así que el Buró Federal de Investigación (FBI) lleva años monitoreando dichos sitios, lo que deja en el ambiente una gran pregunta: si ellos lo hacen con el objetivo de prevenir diversos delitos cibernéticos, ¿qué pasaría si dicha información cae en manos de un *hacker*?

[1]*Facultad de Ciencias Empresariales, Uniremington.*
Contacto: feibert.guzman@uniremington.edu.co
https://doi.org/10.22209/Cice.n2a08

Según las estadísticas, cada día roban miles de datos de información personal y atacan miles de dispositivos móviles y computadores; según Kaspersky Lab (2015), en su 5.ª Cumbre Latinoamericana de Análisis de Seguridad, cada segundo se crean tres virus informáticos en el mundo y en el mismo tiempo se reciben 20 ataques cibernéticos. Vásquez y Cárdenas (2015) en su propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas, evidencian que la aparición de nuevas herramientas de tecnología incrementa el uso de las transacciones financieras por internet, lo que a su vez aumenta el delito informático, concordando con Kasperky Lab (2015) de que en Colombia el 20.9 % de usuarios han sufrido amenazas, lo que implica una respuesta a la pregunta planteada, cada usuario de internet puede ser víctima de un *hacker* por el hecho de no proteger su información.

Un ejemplo claro de estas prácticas ilegales se evidenció gracias a una demanda que un grupo interpuso contra Facebook ante el Tribunal Civil en Viena por el uso indebido de la información: 25.000 usuarios acusaron a la red social de suministrarla de forma ilegal al programa de vigilancia Prism de la Agencia de Seguridad Nacional Estadounidense (NSA), según diversos comunicados de prensa de abril de 2015. Igualmente, en El Internacional (2010) Facebook y MySpace admitieron que habían vendido datos de usuarios sin permiso.

Por tanto, las modalidades de los cibercriminales son diversas: se envían mensajes falsos de entidades financieras, agencias de viajes, etc., para perpetrar fraudes de tarjetas de crédito que se llevan a cabo, por lo general, empleando *botnets* o redes de ordenadores personales que han sido infectados con virus; por todo lo anterior es necesario aplicar controles que salvaguarden la información, porque de lo contrario se les facilita el trabajo a los cibercriminales, quienes obtienen millones de dólares anuales gracias a sus fraudes; según informes de la PricewaterhouseCoopers (PwC), cada día hay millones de víctimas en todo el mundo.

Por otra parte, el internet de las cosas, con el despertar de los avances móviles 3G a 4G y la computación en la nube, va a la vanguardia tecnológica, lo que incide en la comunicación global e implica que cada vez más usuarios se animen a adquirir electrodomésticos inteligentes para

controlar con su móvil la intensidad de luz, el sonido del estéreo, los víveres de la nevera, la chimenea, la televisión e, incluso, el ingreso a su vivienda bajo protección de alarma, monitoreo policial o automatizado. Por ende, cada vez más "las ciudades del futuro cercano tendrán miles de sensores conectados por redes 4G con sistemas de información que ofrecerán a sus gestores multitud de oportunidades de análisis en tiempo real del máximo interés" (Martínez, 2016, p. 42), permitiendo así que la seguridad informática se transforme a pasos agigantados y, de igual manera, el deseo de los cibercriminales de quebrantar dichos sistemas.

Sin embargo, se puede controlar en tiempo real la información de entidades públicas y privadas desarrollando diversos patrones o algoritmos matemáticos que ayuden en la toma de decisiones con base en la tecnología *big data* y en la minería de datos. De igual forma se buscan actuaciones inseguras en milisegundos con la finalidad de brindar seguridad, pero al mismo tiempo el cibercriminal no desaprovecha la oportunidad de atacar; por esto, algunos ladrones emplean *AirDroid*, una poderosa herramienta que controla los *smartphones* vía remota (Kochetkova, 2016); a todo esto se suma el hecho de que los usuarios se conectan a redes Wifi poco seguras, denominadas *señuelo*.

Por lo tanto, la tecnología que se dio en los años 60, conocida como realidad aumentada, comenzó a ser eficiente cuando las tecnologías móviles evolucionaron y permitieron el acceso a internet, a una cámara y a la interacción multimedia (sonido, video, imagen, animación, texto e interactividad); también fue vital la detección de patrones o puntos estratégicos georreferenciados por medio del Sistema de Posicionamiento Global (GPS), que amplifican la interacción hombre-máquina, permitiendo a la cámara del dispositivo mostrar una realidad paralela a lo observado, como es el caso de Pókemon GO, Google Glass, documentos para la educación, juegos, entre otros.

Sin embargo, la incursión de tecnologías móviles de alto impacto, económico, social y tecnológico, no implican descuido de los cibercriminales, por el contrario los pone alerta, es por tal motivo, que la realidad aumentada con la abundancia de *smartphones* en venta deja una puerta abierta para capturar datos por los *hackers* evidenciando lo que pasaría cuando la información cae en sus manos (extorsión, soborno, secuestro de información,

entre otras actividades ilícitas que repercuten en el uso correcto de las Tecnologías de la Información y la Comunicación, TIC).

Marco teórico

El impacto del cibercrimen: bajo la realidad aumentada permite al usuario navegar por medio de su dispositivo móvil en un ambiente habitual atribuyendo diversos tipos de imágenes, rutas, videos, *links* entre otros. Por lo anterior cada vez más personas serán víctimas de la instalación de *software* malicioso sin darse cuenta y de tal forma dar un acceso libre a su información personal.

Igualmente el *malware* se instala con el consentimiento del usuario y al no ser una aplicación propia del *Play Store* de Google, se cataloga como *AndroRAT*, no siendo más que una aplicación maliciosa con la que pueden acceder a su ubicación satelital, al listado de contactos, imágenes, videos, documentos y cifrado de claves que empleen para pagos en línea o simplemente al conectar su dispositivo al ordenador, lo que implica que puede ser víctima de los más de 170 mil virus informáticos que circulan cada día.

Sin lugar a duda las leyes y la cooperación internacional juegan un papel crucial para mitigar la cibercriminalidad; la cual crece en igual medida que las TIC, impactando con aplicaciones como la realidad aumentada y de esta forma valerse de herramientas conocidas pero que muestran su verdadero potencial con los avances tecnológicos.

La realidad aumentada abre diversas brechas para los cibercriminales y los criminalistas tecnológicos, dado que estos deben abordar nuevas técnicas desde la óptica de la seguridad informática, unos para combatirla y otros para quebrantarla. Es por este motivo que se da una mirada a los algoritmos matemáticos desde la óptica de cómo ayudan en la toma de decisiones en los sistemas financieros, pero, a su vez, se genera una gran incertidumbre.

En un ambiente pesimista, ¿qué pasaría si los ciberataques se enfocan en los algoritmos matemáticos?, no solo impactaría en la economía o aspectos propios de la entidad financiera, por el contrario, se generarían especulaciones cibernéticas en función de los datos obtenidos e incluso si el algoritmo no es eficiente se afectaría la toma de decisiones.

Esto implica que actualmente la carencia de conocimiento, la ineficiencia en la seguridad tanto civil como en el ciberespacio y el poco respaldo de leyes que regulen la protección de datos de los dispositivos móviles, Tablet y Computadores de Escritorio (PC), reflejan un ambiente desalentador el cual se ve respaldado por los asaltos. Alrededor de 2.000 celulares son hurtados diariamente en Colombia según noticias RCN del 6 de septiembre del 2016, se evidencia que el *hackeo* de datos a los que se exponen los usuarios es una alerta inquietante, según *Linus Torvalds*, el trabajo del *hacker* es "Interesante, emocionante y alegre", "intrínsecamente interesante y desafiante" (Himanen, 2001), y "va más allá del ámbito de sobreviviente o de la vida económica" (Capurro, 2003), lo que implica que siempre se puede ser víctima no solo de expertos sino también del prójimo, en donde esta figura corresponde al próximo, ósea el más cercano, acompañado de una motivación personal por conocer la privacidad o información financiera con la intención de actuar con dolo.

La encuesta global de delitos económicos de PwC (2016) la cual planteó dos categorías para los mismos:

1. **El que roba dinero y empaña la reputación.** Esta se atribuye al fraude cibernético, "incluye delitos informáticos monetarios, robo de identidad y de tarjetas de crédito". Dichos delitos provocan pérdidas millonarias y un alto número de víctimas. A pesar de su fuerte exposición, rara vez representan una amenaza existencial para las compañías (Global & Econ, 2016).

2. **El que roba propiedad intelectual (PI) y termina destruyendo un negocio.** El delito económico más crítico al que se enfrentan las organizaciones es el espionaje internacional, por ejemplo, el robo de PI clave (secretos comerciales, información de productos o estrategias de negociación). Según Global & Econ, (2016). Los profesionales en informática llaman a ese tipo de ataque *"eventos de extinción"*, debido a que un robo de este tipo puede causar no solo una pérdida millonaria sino también puede estar acompañado por la destrucción de un negocio, de una empresa o de un sistema económico completo. Este tipo de ataques no solo son difíciles de detectar, sino que quizás no forman parte del radar de amenazas evaluado por la compañía.

Por lo expuesto anteriormente, se alerta a los usuarios que el uso del dispositivo móvil corre riesgos de seguridad, lo que hace vital, validar y proteger la información al momento de emplear aplicaciones empresariales, por medio de antivirus legalizados y no en las versiones *open free*. En lo que respecta a las garantías de seguridad de la información y almacenamiento transmitida a estos dispositivos, se debe identificar el riesgo en relación a como se consulta, envía, almacena, procesa o comparte a través de los mismos. El informe de PwC (2015) presenta que "el riesgo se mide como la multiplicación entre el impacto y la probabilidad de ocurrencia (Riesgo = Impacto *Probabilidad), el impacto se refiere a la(s) consecuencia(s) luego de materializado el riesgo, y la probabilidad se refiere a si podría o no suceder el riesgo y con qué frecuencia" (Silgado, 2014).

Los riesgos técnicos presentados de OWASP *Mobile Security Project* adaptables a las aplicaciones móviles en general y sus impactos en la información, se evidencia en la **Tabla 1.**

Tabla 1. Riesgos técnicos OWASP y su descripción.

1. *Weak Server Side Controls.* Debilidad en los controles del lado del servidor de la aplicación.
2. *Insecure Data Storage.* Almacenamiento de datos inseguro.
3. *Insufficient Transport Layer Protection.* Protección insuficiente en la capa de transporte.
4. *Unintended Data Leakage.* Fuga de datos involuntaria.
5. *Poor Authorization and Authentication.* Autenticación y autorización pobres.
6. *Broken Cryptography.* Criptografía rota.
7. *Client Side Injection.* Inyección del lado del cliente.
8. *Security Decisions Via Untrusted Inputs.* Decisiones de seguridad vía entradas no confiables.
9. *Improper Session Handling.* Manejo de sesiones inapropiado.
10. *Lack of Binary Protections.* Falta de protección de los binarios.

Fuente: Adaptado por el autor de Silgado (2014).

Analizar este tipo de riesgos permite identificar las debilidades en función del almacenamiento que soporta el servidor de la aplicación, midiendo su

nivel de seguridad en la capa de transporte y la fuga involuntaria de datos al momento de su autentificación con la finalidad de evitar ser víctima de un *hacker* que implemente algoritmos matemáticos y altera la toma de decisiones de las entidades financieras.

En palabras de un empleado de Microsoft® que manifiesta que la empresa compite con el trabajo de los *hackers*, a menudo hay que atacarlos, y así exigir a un empleado la tarea de investigar, pero el *hacker* considera que "la sensación es estimulante y adictivo" (OSI, 1998), entonces, cualquier tipo de empresa puede ser víctima, pero en especial las entidades financieras, ya que estas son las preferidas por los *hackers*. Según Enrique Beltrán (2004) los ataques a la seguridad informática aumentaron de 10.000 a 80.000 en tres años, siendo los bancos catalogados como los que más daño han sufrido, mientras que los ataques o amenazas para el 2016 a diferencia de los años anteriores se centran en la banca móvil, como los más extendidos o atacados, esto implica, que los cibercriminales empleen *malware* que se enfoca al robo de dinero por medio de los dispositivos móviles, preferiblemente *smartphone*, en donde los "Faketoken y Marcher" troyanos destinados a la banca móvil, situados en el top 10 de los virus según informe de tendencias de Kaspersky Lab de (Sunrise, 2015), impacten negativamente en las estadísticas mundiales en relación a la cibercriminalidad, apuntando a que la intangibilidad de sus servicios propicia el flujo de datos en internet y por ende las operaciones que implican compra y venta de productos se vean afectadas.

El Banco de Pagos Internacionales (BIS) a través del subdirector de análisis económico Hyun Song Shi, alertó sobre la depreciación que están sufriendo ciertas monedas en el mundo por la utilización de algoritmos matemáticos y operaciones electrónicas *off shore,* que sustituyen al elemento humano y operan de forma automatizada. En una investigación resiente del BIS (2016), conocida como Colgando el teléfono. Operaciones electrónicas en mercados y sus implicaciones, se efectúa un análisis que puntualiza las operaciones *off shore* a través de transacciones automatizadas regidas por algoritmos matemáticos, ajustándose a supuestos de liquidez del precio y el mercado.

Sin embargo, el tipo de cambio creció de tal forma que no logró ajustar el desequilibrio propuesto, las divisas de países como Colombia, Chile,

México y Perú son de libre convertibilidad a otra moneda, mas no son aceptadas como medio de pago en cobro internacional, según Raymundo Tenorio en entrevista con Aristegui realizada el 20 de septiembre de 2016 por CNN, manifestó que México pasó por una depreciación acumulada o devaluación del periodo del 2013 al 2016 en un 55 %; por lo general, la divisa en México suele mantener un rango entre los 12 y 14 pesos, pero en su momento el incremento llegó a los 20 pesos mexicanos, pero este incremento no se vio afectado por lo que las personas suelen cambiar en las casas de cambio, por el contrario este incremento se dio por las compras al mayoreo las cuales satisfacen a los clientes de los bancos como exportaciones e importaciones.

Por esto, el 17 de febrero de 2016, el Banco de México, Banxico (2016), diseñó algunas intervenciones con el objetivo de contrarrestar la especulación internacional, saliéndose del mercado de subastas diarias de dólares y realizó una intervención discrecional atribuida a operaciones derivadas de algoritmos matemáticos operados fuera y dentro del país denominada especulación cibernética.

Sin embargo, la liquidez del peso para México según especialistas del BIS, manifiestan que dichos algoritmos matemáticos solo facilitan las operaciones de compra y venta de activos, pero sumado con la caída del petróleo, el caso de China en la incursión de su moneda a la canasta de divisas del Fondo Monetario Internacional (FMI), las discrepancias en las políticas monetarias permitiría que estas operaciones afecten significativamente la moneda, dado que donde han intervenido estas operaciones electrónicas de capitales *off shore,* puedan generar especulaciones cibernéticas.

Por tanto, Agustín Carstens, gobernador del Banco de México, reconoció la presencia especulativa en los dos primeros meses del año (2016), asegurando la volatilidad del peso frente al dólar, motivo por el que la incursión de nuevas tecnologías que apunten a la realidad virtual permiten que las organizaciones puedan ser propensas a ataques de los cibercriminales si no se protegen, y ser víctima de un ciberataque en América Latina que aumentó del 21 % para el 2011 al 33 % para el 2014 y 39 % para el 2016, lo que implica una tendencia a ser víctima de un ciberataque en un futuro no muy lejano **(Figura 1).**

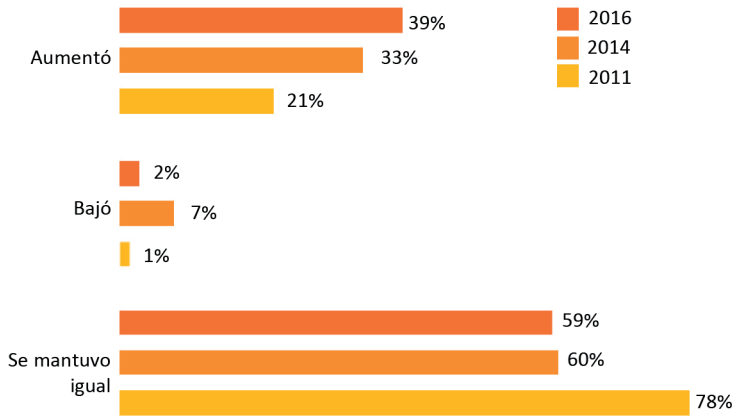

Figura 1. Precepción de ser víctima de un ciberataque.
Tomada y modificada de: Encuesta global sobre delitos económicos 2016 (Global & Econ, 2016).

En el 2012 el 38 % de los incidentes del cibercrimen fueron de tipo económico proveniente del sector financiero (SF) y se incrementaron en un 50 % los fraudes de altos directivos en el mismo, según el comunicado de prensa de la PwC Arrocha, (2012), a diferencia del 2016 donde casi el 40 % de las entidades temen convertirse en víctimas del delito informático. Las secuelas o impacto del cibercrimen fueron la pérdida financiera y el daño en la reputación **(Figura 2).**

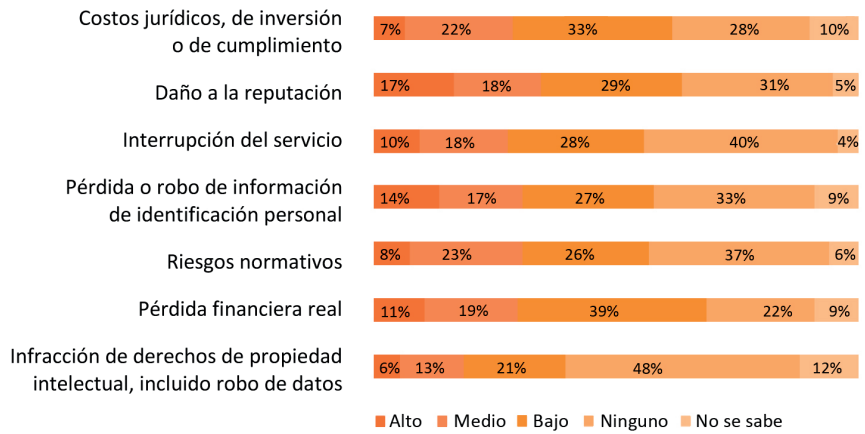

Figura 2. Impacto del cibercrimen en América Latina.
Tomada y modificada de: Encuesta global sobre delitos económicos 2016 (Global & Econ, 2016).

Conclusiones

La relación de la cibercriminalidad para el 2016, según la percepción de la encuesta global de PwC, muestra un aumento gradual del 6 % entre el 2014 y el 2016, lo que implica que la tendencia de los ciberataques aumentó, por lo que las entidades financieras de América Latina reflejaron pérdidas en el rango de 50.000 a 100.000 USD en un 20 % y en el rango de 1 a 50.000 USD en un 32 %, cifras que ratifican cómo el impacto que presenta la incursión de nuevas tecnologías asociadas repercuten de forma directa en el aspecto económico y financiero de las entidades financieras, tanto para maximizar utilidades en un mercado eficiente como para posibles desvíos hacia fraudes.

Sin embargo la especulación cibernética y cibercrímenes que llevan a mercados ineficientes, analizando el caso Pókemon GO y los muy recientes algoritmos matemáticos para automatizar la toma de decisiones en los mercados de capitales y divisas bajo la realidad aumentada, permite acercarse a lo que demanda el futuro en relación a avances tecnológicos, dado que la percepción de América Latina respecto a si las agencias de orden público cuentan con habilidades y recursos para investigar delitos informáticos en Colombia, Ecuador y Perú, el 45 % consideran que no las poseen, el 27 % considera que si, el 23 % no sabe.

Por ende, si analizamos la aplicación Pokémon GO, muchos de los usuarios por la impaciencia de no lograr obtener la App oficial, optaron por instalar otras versiones, lo que implico, un gran aumento en el ataque a dispositivos móviles dado que "el programa incluye una herramienta de "control remoto malicioso" llamada *DroidJack*, que provee de un acceso "por la puerta trasera" al teléfono y a toda la información contenida en él, esto debido a que la aplicación puede ver y modificar toda la información de la cuenta de Google de quienes la descargan".

Con la creación de un Avatar, la aplicación Pokémon GO permite al usuario interactuar con el mundo real y el mundo virtual, este juego de realidad aumentada creado por Niantic®, empresa que aumentó de forma exponencial sus acciones al lanzamiento de dicho juego para dispositivos móviles, iPhone y dispositivos Android. "Brinda una plataforma que utiliza ubicaciones reales para animar a los jugadores a que salgan a explorar a lo largo y ancho del mundo" (Niantic, 2016), **(Figura 3).** Ya que "la realidad aumentada funciona con base a la superposición de información sobre la

realidad, a partir de tres recursos tecnológicos básicos que en ocasiones se complementan entre sí: los patrones de disparo del *software*, la geolocalización y la interacción con Internet". (Fombona & Ferreira, 2012).

Figura 3. Realidad aumentada, parte de tu nuevo mundo.
Tomada y modificada de: https://goo.gl/ppudqB

Por este motivo, el *smartphone* es la herramienta principal del juego, y esté debe cumplir con unas características técnicas mínimas requeridas, lo que implica, que cada vez los usuarios necesiten adquirir teléfonos de gama alta o mayor capacidad, acceso a internet y ubicación satelital, debido a estas especificaciones cada vez los dispositivos móviles se vuelven más atractivos para los delincuentes en general, ladrones callejeros y los cibercriminales que están a la espera de que se conecten con la finalidad de *hackear* su dispositivo y de esta forma convertirse en una estadística más del robo de celulares y fraude cibernético. Por tanto, hablando de virus se ha detectado una amenaza, reportó Avast, lo que implica que se debe estar protegido, ser cuidadoso de claves, uso de redes públicas, manejo de contactos, ingreso seguro a entidades financieras y no está de más cuidar los objetos personales. Por esto es que "la Ciberseguridad debe plantearse no sólo desde el punto de vista de las amenazas sino también desde los retos que plantean", (Joyanes, 2010), esto con el fin de brindar soluciones que perduren en el tiempo a so pesa de la volatilidad en el cambio tecnológico.

Referencias

- Arrocha, Miriam. (2012). El cibercrimen es una amenaza creciente para el sector de servicios financieros, según reporte de PwC. Comunicado en línea PwC. Recuperado el 29 de septiembre de 2016 de: https://www.pwc.com/ia/es/prensa/assets/pwc-el-cibercrimen-amenaza-sector-financiero.pdf
- Banxico. (2016). Banco de México. Recuperado el 17 de febrero de 2016 de: http://www.banxico.org.mx/viewers/JSP/docsInvestigacionAnio_es.jsp?static=y
- BIS. (2016). *Colgando el teléfono. Operaciones electrónicas en mercados y sus implicaciones*. Recuperado el 29 de septiembre de 2016 de: http://www.bis.org/press/wnew.htm
- Capurro, R. (2003). *Passions of the Internet and the Art of Living*. Recuperado de: http://www.capurro.de/illinois.htm
- Fombona, J., Pascual, M. Á., & Ferreira, M. F. M. (2012). Realidad aumentada, una evolución de las aplicaciones de los dispositivos móviles. *Pixel-Bit. Revista de medios y educación*, (41).
- Himanen, P. (2001). *The Hacker Ethic and the Spirit of the Information Age*. London: Secker and Warburg.
- Joyanes Aguilar, L. (2010). Introducción: estado del arte de la ciberseguridad. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia*, (149), 29-34 p.
- Kochetkova, K. (2016). *Cómo defraudan los ciberdelincuentes a los autónomos. Nosotros utilizamos las palabras para salvar el mundo*. Recuperado el 29 de septiembre de 2016 de: https://blog.kaspersky.com.mx/airdroid-scam/7338/
- Martínez de Castro, M. (2016). *Cinco grandes tendencias de las que estar pendiente en Criminología (II)*. Recuperado el 28 de septiembre de 2016 de: http://www.academia.edu/9705209/Cinco_grandes_tendencias_de_las_que_estar_pendiente_en_Criminolog%C3%ADa_II_
- Niantic, P. (2016). *Pokémon GO*. Videojuegos. Recuperado el 26 de septiembre de 2016 de: http://www.pokemon.com/es/videojuegos-pokemon/pokemon-go/
- OSI (1998). Halloween document II, version 1.4. Recuperado de: http://www.opensource.org/halloween/halloween2.php

- Price Waterhouse & Co. (2016). *Encuesta Global sobre Delitos Económicos 2016*. Recuperado de: http://www.pwc.com.ar/es/publicaciones/assets/encuesta-global-sobre-delitos-economicos-2016-latinoamerica.pdf
- Price Waterhouse & Co. (2015). Encuesta sobre fraude y delito económico 2014. Resultados en España.
- Raymundo, T. (2016). *Se deprecia el peso frente al dólar*. Recuperado el 29 de septiembre de 2016 de: https://www.youtube.com/watch?v=qjhr8--bBQE
- Silgado, F. (2014). Riesgos de seguridad de la información en el uso de dispositivos móviles para aplicaciones empresariales. Recuperado el 29 de septiembre de 2016 de: https://www.pwc.com/co/es/assets/document/mision.pdf
- Sunrise, F. (2015). *Kaspersky Lab., echa un vistazo hacia atrás: repaso los principales incidentes de seguridad de 2015*. Recuperado el 29 de septiembre de 2016 de: https://goo.gl/ncFBX9
- Vásquez Zarate, K. A., & Cárdenas Rodríguez, M. P. (2015). *Propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas*. Trabajo de grado, Programa de Contaduría Pública, Facultad de Ciencias económicas y administrativas. Pontificia Universidad Javeriana. Recuperado de: https://repository.javeriana.edu.co/handle/10554/18900

UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

Facultad
de Ciencias
Contables

MAESTRO
EXTENSIÓN Y POSGRADOS

Capital Contable
Grupo de investigación Uniremington