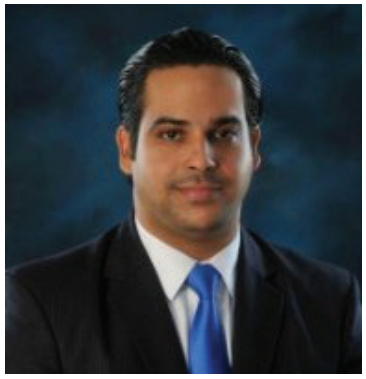
LA SEGURIDAD COMO LÍNEA DE DEFENSA

THE SECURITY AS A DEFENSE LINE

Recibido: 30 / 09 / 2017 ***Aprobado: 17 / 11 / 2017***



Lic. Francisco Frías Pujols,
República Dominicana

Administración de Empresas con Especialidad en Finanzas Corporativas de la Pontificia Universidad Católica Madre y Maestra (PUCMM). Se certificó como Especialista en Prevención de Lavado de Activos por la Asociación de Especialistas Certificados en Prevención de Lavado de Dinero (ACAMS por sus siglas en inglés) y se certificó como Investigador de Fraudes por la Asociación de Investigadores Certificados en Fraude (ACFE por sus siglas en inglés). Actualmente se desempeña como Vicepresidente de Cumplimiento de un Banco Múltiple local. Es facilitador de charlas, talleres y diplomados en prevención de lavado de dinero e investigación de fraudes.

friascarbuccia@hotmail.com

RESUMEN

La aparición de nuevos modelos sociales tiene su causa raíz en el nacimiento y desarrollo sostenido del Internet y los sistemas informáticos. El acceso a la información sin límites nos ha llevado hasta la situación actual, donde prácticamente todo lo que hacemos en nuestras vidas, se encuentra reflejado en la Internet.

En paralelo, a medida que las personas navegaban por el ciberespacio, también comenzaban a hacerlo aquellos que buscaban obtener un beneficio originado en actividades criminales. Estos fueron avanzando de manera exponencial desarrollo de técnicas y métodos para vulnerar sistemas de seguridad. Los llamados ciberdelincuentes tomaban ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema hace unos años.

Con el paso de los años, esta distancia ha ido reduciéndose, y pese a que aún los índices de ciberdelincuencia son altos, junto con la evolución y aparición de nuevas técnicas, los gobiernos y las empresas han tomado consciencia de la gravedad de este problema y han comenzado a buscar soluciones.

Por otro lado, el modelo de las 3 líneas de defensa realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de todas una organización. Este modelo, entiendo, puede traducirse también a las 4 áreas que podrían sufrir un mayor impacto fruto de la inseguridad, de manera tal, que puedan quedar todas integradas para reforzar la Seguridad de una nación. Estas áreas son: El Sistema Financiero Nacional, el Sistema Judicial, las Fuerzas Armadas y los Cuerpos de Seguridad del Estado.

Este escrito persigue mostrar las causas principales del problema de la inseguridad que estamos viviendo los últimos años. Está evidenciada la aparición de nuevos personajes en la sociedad que han fomentado ideas desvirtuadas sobre la forma de vivir del ser humano y sobre en qué deben asentarse sus principales intereses. Estos intereses, lamentablemente, no están muchas veces arraigados a la realidad

de cada quien. De esta situación vienen a desprenderse principalmente personas con pretendencia a vivir a un nivel que está por encima de sus posibilidades, la cual estadísticamente es la principal causa de fraude. También, la pérdida de valores y la ética suponen un problema que sumados al odio y a la persecución del dinero desmedido, ocasionan la presencia de delincuentes que vulneran la seguridad de nuestros espacios cibernéticos y de la sociedad en sentido general.

Palabras clave:

Estado, ciudadanía, defensa, ética, moral, cívica, valores, principios, corrupción, narcotráfico, familia, crimen, lavado de dinero y financiamiento del terrorismo.

ABSTRACT

The emergence of new social models has its root cause in the birth and sustained development of the Internet and computer systems. Access to information without limits has led us to the current situation, where virtually everything we do in our lives, is reflected in the Internet.

In parallel, as people navigated through cyberspace, so did those seeking profits from criminal activity. These were advancing exponentially in the development of techniques and methods to violate security systems. The so-called cybercriminals took advantage of the authorities and their poor readiness to address this new problem a few years ago.

Over the years, this distance has been shortening, and although cybercrime rates are still high, together with the evolution and emergence of new techniques, governments and companies have become aware of the seriousness of this problem and have begun to seek solutions.

On the other hand, the 3 lines of defense model enhances the understanding of risk management and controls by assigning or clarifying roles and responsibilities throughout an organization. This model, I understand, can also be translated into the four areas that could suffer the greatest impact as a result of insecurity, so they can all be integrated to

reinforce the security of a nation. These areas are: The National Financial System, the Judicial System, the Armed Forces and the State Security Corps.

This paper seeks to show the main causes of the insecurity problem we are experiencing in recent years. It's evidenced the appearance of new characters in the society that have fomented distorted ideas on the way of living of the human being and what should settle their main interests. These interests, unfortunately, are often not indexed to the reality of each person. From this situation comes the origin of people with an intention to live beyond their means, which is statistically the main cause of fraud. Also, the loss of values and ethics are a problem that together with hate and persecution of money, cause the presence of criminals that violate the security of our cyberspaces and society in a general sense.

Keywords:

State, citizenship, defense, ethics, moral, civics, values, principles, corruption, drug trafficking, family, crime, money laundering and terrorism financing.

Introducción

La protección del Estado, de la cual se habla en reiteradas ocasiones en la prensa y en nuestras calles diciéndose que debe ser provista de manera organizada y estratégica por las fuerzas castrenses, la policía nacional, instituciones privadas, entre otras, es una realidad que no se puede ocultar. Sin embargo, si nos vamos a la causa raíz de los problemas de inseguridad de nuestro país, agravados de manera progresiva en los últimos años, pensamos que existen varios factores que son los que tienen mayor incidencia, los cuales son el deterioro de la base de la sociedad que es la familia y con ella desencadenándose una pérdida de valores, principios, ética y moral. Asimismo, esto acarrea una falla en el comportamiento cívico que debe mostrar un ciudadano, el cual percibo ya ni siquiera es inculcado con la misma fuerza y convicción en nuestras escuelas, colegios, universidades y nuestros hogares.

Partiendo de los valores arriba mencionados, se desprende la ciudadanía con educación cívica y de ahí el valorar esencialmente a la patria. Es sencillo, sin una formación fuerte arraigada a la ética y moral, no podemos pretender tener ciudadanos íntegros y respetuosos. Nuestras instituciones de seguridad precisamente se derivan del trabajo de esos ciudadanos que son formados en nuestros hogares todos los días. No podemos pretender tener un sistema honrado y responsable sin una base sólida.

He decidido abordar este tema de "LA SEGURIDAD COMO LINEA DE DEFENSA" agradeciéndole a mi padre, el General de Brigada (pensionado de la Fuera Aérea Dominicana) Francisco Frias Carbuccia por su apoyo y asesoría para su elaboración; el cual describo desde cuatro vertientes que a mi entender son las que tienen mayor incidencia en la seguridad nacional, para un sencillo entendimiento que a la vez se pueda ver en su inicio y final como algo integral. Estas vertientes son impactadas por transacciones ilícitas derivadas de lavado de dinero, ataques físicos y cibernéticos a instituciones privadas y públicas, narcotráfico, corrupción administrativa, entre otros crímenes y ofensas que son penalizados por la Ley de lavado de dinero de nuestro país y también por las leyes anticorrupción y de crímenes y delitos de alta tecnología del Estado. Las cuatro áreas que a mi entender son las más impactadas por el narcotráfico, el

lavado de dinero, la ciberdelincuencia y la corrupción administrativa son las siguientes:

a) El Sistema Financiero Nacional. A ser abordado desde la óptica de las obligaciones presentadas en la Ley 155-17 de Prevención de Lavado de Activos;

b) El Sistema Judicial. A ser abordado por la labor realizada en el Poder Judicial a través de la Procuraduría General de la República;

c) Las Fuerzas Armadas. A ser abordada por la labor realizada por el Ministerio de Defensa con el Ejército de la República Dominicana, La Fuerza Aérea y la Armada de la República Dominicana; y

d) Los Cuerpos de Seguridad del Estado. A ser abordados por la labor realizada en la Policía Nacional, el Departamento Nacional de Investigaciones y la Superintendencia de Vigilancia y Seguridad Privada.

Las cuatro líneas de defensa expuestas precedentemente deben estar asentadas sobre una base ética, moral y de valores. En caso de no ser así, solo nos queda esperar el fracaso inminente. Creo que todos los ciudadanos dominicanos tenemos parte de la responsabilidad que únicamente se le ha atribuido a las áreas mencionadas previamente; esto ha sido un tremendo error cometido por décadas en nuestra sociedad, el cual debe ser desafiado con actitud y responsabilidad por cada uno de nosotros.

En adición, tomando en consideración la creciente importancia que están usando los sistemas informáticos en todos los ámbitos de la sociedad actual y que este auge no ha pasado desapercibido por los grupos que operan bajo el margen de la Ley y por supuesto entre ellos, los estados y organizaciones terroristas, se entiende que hacen más vulnerables la defensa del Estado y la mundial.

Desarrollo del tema

Al ser la Seguridad y Defensa Nacional un tema recurrente en la agenda presidencial y un tema de tanta importancia y relevancia, principalmente en estos tiempos donde no solo recibimos un impacto nacional en la seguridad física de los individuos, sino que también a nivel internacional puede afectar nuestra imagen frente a la inversión extranjera y al turismo, que es nuestra principal fuente de ingresos, es necesario tener cada vez más órganos de seguridad más robustos en su estructura y con un personal que se rija por valores éticos y respeto a los símbolos patrios y lo que los mismos representan. Increíblemente, en los tiempos que estamos viviendo actualmente, los principios mencionados hacen más falta en muchas instituciones que una buena preparación académica en países en vías de desarrollo como es República Dominicana.

La base de una sociedad es la familia. Ahí se asienta todo y después de esto viene lo demás. No podemos tener Instituciones serias, responsables y éticas si sus recursos humanos no lo son.

Las cuatro áreas que a mi entender son las más vulnerables por el crimen organizado que realiza ataques ilícitos de lavado de dinero, de narcotráfico, corrupción y cibernéticos son: El Sistema Financiero Nacional, el Sistema Judicial, las Fuerzas Armadas y los Cuerpos de Seguridad del Estado. De manera segmentada, explicaré con mis palabras la incidencia que tienen estas áreas en la protección del Estado; sin embargo, la idea principal de este artículo es mostrar como todas pueden funcionar perfectamente de manera integral para combatir el crimen organizado, ya que las mismas están entrelazadas de manera directa o indirecta.

a) El Sistema Financiero Nacional

El sistema financiero de la República Dominicana está regulado principalmente por la Constitución, la Ley Monetaria y Financiera No. 183-02 y sus normativas complementarias. Los entes reguladores del sistema más importantes son: La Junta Monetaria, el Banco Central de la República Dominicana, la Superintendencia de Bancos de la República Dominicana, la Superintendencia de Valores, entre otras. Estas instituciones conforman la Administración Monetaria y Financiera y tienen la autoridad para fijar políticas, formular e implementar regulaciones y aplicar sanciones. Asimismo, establecen un marco de control interno que las ayudan a cubrir riesgos como posibles conflictos de interés, establecer un código de ética y conducta (incluyendo una línea ética independiente), respeto al Gobierno Corporativo, monitoreo de actividades y transacciones de empleados, establecimiento de canales claros de comunicación, entre otros temas de importancia para una buena gestión empresarial.

El referente más importante de control interno es el marco establecido por el Comité de Organizaciones Patrocinadoras de la Comisión de Normas (COSO por sus siglas en inglés). De acuerdo al marco COSO, el control interno consta de cinco componentes relacionados entre sí; éstos derivarán de la manera en que la Dirección dirija la Unidad y estarán integrados en el proceso de dirección. Los

componentes serán los mismos para todas las organizaciones (públicas o privadas) y dependerá del tamaño de la misma, la implantación de cada uno de ellos. Los componentes de COSO son:

1. Ambiente de Control.
2. Evaluación de Riesgos.
3. Actividades de Control.
4. Información y Comunicación.
5. Supervisión y Monitoreo.

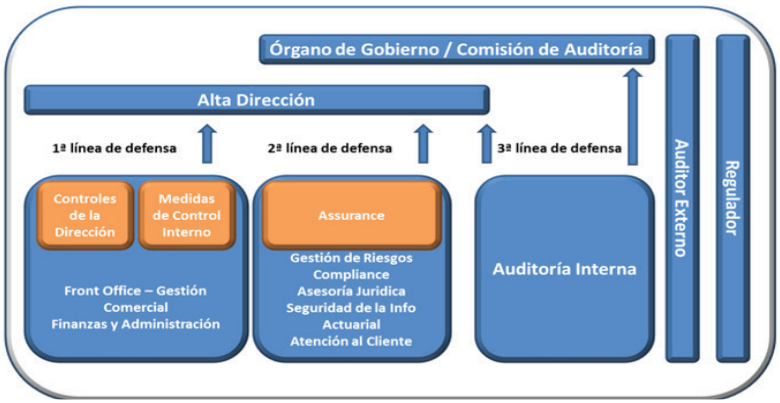
No vamos a entrar en detalle en cada uno de estos componentes, los cuales a su vez constan de varios principios y distintos puntos de enfoque. Lo que sí deseo destacar es que en la imagen del cubo de COSO, el ambiente o entorno de control es la base del Control Interno, aportando disciplina a la estructura. En él se apoyarán los restantes componentes, por lo que será fundamental para concretar los cimientos de un eficaz y eficiente sistema de Control Interno. El ambiente de control marca la pauta del funcionamiento de la Unidad e influye en la concientización de sus funcionarios.

Los factores a considerar dentro del Entorno de Control serán: La Integridad y los Valores Éticos, la Capacidad de los funcionarios de la Unidad, el Estilo de Dirección y Gestión, la Asignación de Autoridad y Responsabilidad, la Estructura Organizacional y, las Políticas y Prácticas de personal utilizadas. Simplemente, los altos funcionarios, los accionistas y miembros del Consejo o la Junta de Directores deben ser el ejemplo y modelo a seguir por los demás empleados de la Institución. Parecería que el marco de control interno COSO es bien parecido, en su esencia, a lo que mencionamos en la introducción del escrito cuando hablábamos de la importancia de la ética, valores, principios y moral de los individuos, los cuales son los que finalmente van a ser los empleados de las Instituciones Financieras Nacionales y serán el soporte de varias familias Dominicanas.

En el modelo de las tres líneas de defensa de Basilea para una efectiva administración de riesgos y control se establece que:

- La primera está en la Administración y sus Gerencias, la que incluye el sistema de Control Interno y la existencia y funcionamiento de los controles mismos;
- La segunda está en las funciones de Riesgo y de cumplimiento, incluyendo: Controles financieros, administración de riesgos, seguridad, calidad, inspecciones, cumplimiento, legal y cadena de abastecimiento entre otros; y
- La tercera es de Auditoría Interna en cuanto a su existencia, independencia, calidad de sus recursos humanos y técnicos y su programa de trabajo.

Asimismo, todas estas deben reportar a órganos independientes que puedan supervisar sus funciones sin conflictos de interés. A continuación se presenta una ilustración sencilla del modelo de las tres líneas de defensa:



Es de conocimiento público que las entidades financieras son consideradas "Sujetos Obligados" bajo el marco de la nueva Ley 155-17 de prevención de lavado de activos y financiamiento del terrorismo de fecha 31 de mayo de 2017. La misma deroga la anterior Ley 72-02 contra el lavado de activos del año 2002. Esta nueva Ley es más robusta en su alcance y obligaciones, y cumple con los estándares del Grupo de Acción Financiera Internacional (GAFI) en materia de prevención de lavado de activos y financiamiento del terrorismo.

Precisamente esta Ley 155-17, en su artículo No. 88 define al Comité Nacional contra el Lavado de Activos como un órgano de coordinación, de naturaleza colegiada, responsable del funcionamiento eficiente del sistema de prevención, detección, control y combate del lavado de activos, financiamiento del terrorismo y del financiamiento a la proliferación de armas de destrucción masiva. En este mismo artículo se presentan quienes conforman el referido Comité que son:

- El Ministro de Hacienda;
- El Procurador General de la República;
- El Ministro de Defensa;
- El Presidente del Consejo Nacional de Drogas;
- El Presidente de la Dirección Nacional de Control de Drogas;
- El Superintendente de Bancos;
- El Superintendente de Valores.

La secretaría técnica del Comité será ejercida por el Director de la Unidad de Análisis Financiero (UAF).

De esta manera, se corrobora como va amarrando el tema de la seguridad nacional en materia de prevención de lavado de activos y financiamiento del terrorismo identificándose también los delitos subyacentes más importantes que afectan a nuestro país provenientes de transacciones del lavado de dinero como son: Evasión de impuestos, narcotráfico, tráfico ilícito de seres humanos, extorsión, soborno y demás formas de corrupción, falsificación de dinero, tráfico de armas, entre otros.

El sistema financiero nacional, en cumplimiento a la nueva Ley 155-17, va a ayudar significativamente en la protección y la seguridad nacional. Las transacciones identificadas como sospechosas de las entidades financieras, por obligación según indica el artículo No. 55, deberán ser comunicadas a la Unidad de Análisis Financiero y si se identifica algún delito subyacente con implicados que atentan

con la seguridad del Estado, serán sujetos de investigación por dicha Unidad y puestas en conocimiento en el referido comité. En este sentido, el riesgo del incremento de transacciones ilegales que afecten a la economía nacional estaría más controlado, así como también aquellos individuos que se dedican a actividades ilícitas, que podrían atentar también de forma física, contra la seguridad ciudadana.

Tengo que adicionar que considerando la influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, etc. Son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Junto al avance de la tecnología informática y su influencia en la vida social, han surgido una serie de comportamientos ilícitos denominados "delitos informáticos bancarios", en especial las falsificaciones informáticos. Dentro de las tipificaciones de delitos informáticos, según lo que establece la Ley 53-07 contra Crímenes y Delitos de Alta Tecnología, podemos citar algunos importantes como:

- Atentado contra la vida de una persona;
- Obtención ilícita de fondos;
- El chantaje;
- La estafa;
- Entre otros.

En los últimos 15 años se ha puesto de moda el "Phishing" en nuestro país. Esta modalidad de fraude es utilizada para engañar y conseguir que se revelen informaciones personales como: Identidades, contraseñas, números de claves bancarias, con la finalidad de realizar transacciones fraudulentas a través del servicio de Internet Banking que proveen la mayoría de los bancos múltiples y también el robo de numeraciones de tarjetas de crédito para realizar consumos en negocios que por lo general van asociados a bebidas alcohólicas, restaurantes, hoteles, entre otros.

Los "Hackers" del sistema financiero generan graves consecuencias a las actividades económicas del Estado, lo que lo coloca en una situación negativa, ya que los ataques cibernéticos normalmente giran en torno al robo de información sensible alterando los informes financieros emitidos por el sistema financiero nacional, y esta información puede, literalmente, conducir a la ruina del Estado.

b) El Sistema Judicial

En esta sección, nos vamos a circunscribir únicamente a la labor de la Procuraduría General de la República Dominicana por ser miembro activo del Comité Nacional contra el Lavado de Activos. El Procurador se nombra por Decreto Presidencial; en este sentido, está insertado dentro del Poder Ejecutivo.

Para apoyar al Procurador en las labores relacionadas a la investigación y persecución del crimen de Lavado de Activos en el país que trabaje en coordinación con las autoridades nacionales e internacionales, se crea una dependencia especializada que es la Unidad del Ministerio Público Antilavado de Activos. El Procurador General es informado de las investigaciones criminales por el Procurador Especializado en materia de prevención de lavado de dinero, quien trabaja también de forma muy cercana con las autoridades financieras del país.

El Procurador Especializado en prevención de lavado de activos se encarga de perseguir el delito subyacente que posiblemente originó el lavado de dinero. Se encarga de compilar las evidencias necesarias para someter legalmente a los implicados en transacciones de narcotráfico, que es el principal flagelo que afecta a nuestro país actualmente y también otros delitos que preceden al lavado de dinero. Esta figura es una arista de mucha relevancia en el combate del lavado de dinero y en la seguridad del Estado. El mismo se nutre de los informes de transacciones y actividades sospechosas de la Unidad de Análisis Financiero y la Superintendencia de Bancos de la República Dominicana, una vez que los mismos han sido previamente analizados cuando se reciben del sistema financiero nacional.

Como pueden observar, las transacciones sospechosas van escalando desde el sistema financiero nacional a la Unidad de Análisis Financiero y llegando finalmente el reporte correspondiente a la Unidad Antilavado de Activos de la Procuraduría a través de las reuniones periódicas o especiales que se organizan, para ser presentadas en el Comité Nacional contra el Lavado de Activos. Es aquí donde convergen los actores más importantes de la seguridad nacional descritos en la Ley 155-17.

La cooperación entre la UAF y la Procuraduría General de la República es algo real y palpable. Recientemente, ambos órganos firmaron un acuerdo de cooperación con el cual formalizan las relaciones y los vínculos de colaboración existentes entre ambas instituciones.

El convenio rubricado por la Directora General de la UAF y el Procurador General de la República, persigue fortalecer los mecanismos y la logística de ambas instituciones en el intercambio de información relacionada con operaciones provenientes del lavado de activos, narcotráfico y otros delitos.

En el acto de firma ambos funcionarios coincidieron en que este acuerdo será de gran ayuda para detectar de manera oportuna, las actividades y operaciones de lavado de activos y otros delitos vinculados al crimen organizado.

Por otro lado, también hay que destacar que desde la óptica del riesgo de crímenes de alta tecnología, la violación de este sistema genera que pueda ser empleado para otorgarle libertad a una serie de delincuentes del Crimen Organizado Transnacional, o por el contrario, eliminar o retardar del sistema libertades o registros de informaciones que puedan ser empleadas para alterar la paz del Estado.

c) Las Fuerzas Armadas

Las Fuerzas Armadas (FF.AA.) tienen como misión fundamental la defensa de la soberanía, la integridad social y el orden constitucional. Suelen dividirse en ramas, servicios armados separados que agrupan los recursos militares empleados por dicho estado en tierra (Ejército), mar (Armada) y aire (Fuerza Aérea). No obstante, en las últimas décadas, las FF.AA se han visto obligadas a aparecer en escenas de amenazas que pueden constituir un peligro real para la autonomía de los Estados, supervivencia de las democracias y el bienestar de los ciudadanos. Estas amenazas no son las típicas que se daban hace unos años atrás, en la cual las FF.AA. podían entrar en acción de combate armado o realizaban actividades de inteligencia o contrainteligencia estratégica con un enfoque en riesgos que podrían afectar físicamente o estructuralmente al Estado; nos referimos más bien al fenómeno de la criminalidad

impulsada principalmente por el auge del narcotráfico y la corrupción pública, la cual se combate desde otra óptica.

Los efectos del narcotráfico y la corrupción pública van más allá de lo que muchas personas podrían pensar, considerando que vivimos en país subdesarrollado. El daño que hace el narcotráfico a una nación incrementando la inseguridad ciudadana, tergiversando los datos reales del crecimiento del Producto Interno Bruto y aumentando las transacciones de lavado de dinero y de lo perjudicial de la corrupción pública, al deteriorar la imagen de honestidad que debe tener el Estado y de incrementar el sentido de hacer dinero fácil en los Dominicanos ante acceder a un soborno o una extorsión de un funcionario nacional o extranjero, son solamente la punta del iceberg.

El daño más lesivo va dirigido como una punta de lanza directamente a la base de la sociedad que es la familia, donde la psicología de la mayoría de sus miembros que no tienen una formación cívica, moral y ética sólida, perciben a los jefes de carteles, puntos de droga y a funcionarios corruptos, como personas de éxito y líderes de la sociedad, por la adquisición de bienes materiales y/o superficiales.

Con el nacimiento de la nueva Ley 155-17 de Prevención de Lavado de Activos y Financiamiento del Terrorismo, y la asignación como uno de los pilares del Comité Nacional contra el Lavado de Activos del Ministerio de Defensa, pensamos que el crimen organizado será combatido de forma más inteligente, ya que este ministerio contará con exposición a informaciones, que probablemente antes no le llegaban de una forma depurada, o quizás ni le llegaban por no existir una estructura como la que tenemos actualmente, con la promulgación de la mencionada Ley. Asimismo, se adelanta el génesis de lo que más se parecería a un Consejo Nacional de Seguridad y Defensa Nacional, el cual aún está pendiente de su creación por el proyecto de Ley del Sistema Nacional de Inteligencia de la República Dominicana.

Con la UAF, como órgano receptor de los Reportes de Operaciones Sospechosas (ROS) que son remitidos por el sector financiero y no financiero, dicha Unidad va a compartir aquellos casos que ellos previamente han determinado son más importantes en el Comité Nacional contra el Lavado de Activos. Esto se va a hacer en presencia del Ministro de Defensa, el representante del Procurador General, del Ministerio de Hacienda, el Director de la Dirección Nacional de Control de Drogas, el representante de la Superintendencia de Bancos, entre otros.

Como es de su conocimiento, los ROS, cuando son validados en las investigaciones de la UAF como positivos, se tipifican cuales son los delitos precedentes del lavado de activos, tal como mencionamos en la sección de a). En nuestro país, dentro de los principales delitos subyacentes del lavado de dinero que involucran directamente al Ministerio de Defensa, quien es el principal representante en el Estado de las Fuerzas Armadas, son actualmente: Narcotráfico y corrupción. En este sentido, vemos como las líneas de defensa van encadenándose en un Comité, donde el Ministro de Defensa va a estar expuesto a informaciones y escuchando los comentarios y análisis realizados por los demás miembros ya mencionados.

Las FF.AA. se encuentran en este momento ante un escenario abierto a varias modalidades de crímenes. Es evidente que estamos en una zona geográfica de alto riesgo, donde nuestro país ha sido catalogado como puente de narcotráfico y donde algunos de los que tienen el control

del país se han visto mencionados e involucrados en actividades de corrupción.

El empleo de las Fuerzas Armadas no responde necesariamente a un proceso homogéneo y uniforme, sino más bien a respuestas individuales que no obedecen a estrategias políticas determinadas, sino a una reacción frente a las crecientes demandas de mayores cuotas de seguridad. En este sentido, es cada vez más importante y saludable que no existan conflictos de interés en los nombramientos de la persona que va a ocupar la posición de Ministro de Defensa, de manera tal que sean personas adornadas de los valores previamente enunciados y que, por tanto, garanticen los mismos principios en el personal de sus instituciones, con bases sólidas de lealtad a toda prueba, en defensa de los mejores y sagrados intereses de la nación dominicana.

También hay que destacar que ante el nuevo peligro que supone la ciberdelincuencia y la propia sistemática de hacer la guerra, los diferentes gobiernos e instituciones internacionales han comenzado a tomar medidas para que esta grave amenaza pueda ser detectada y evitada antes que se produzca.

Los ciberataques están aumentando de forma exponencial en su faceta de sustracción de información confidencial y de secretos industriales, que están produciendo graves pérdidas en las industrias punteras de los estados y transfiriendo conocimiento tecnológico avanzado a estados que practican este tipo de ataques.

Lo ciberataques con fines terroristas o ciberguerra, pueden alcanzar sitios insospechados, y aún no cumpliendo total o parcialmente con su objetivo, la sola difusión mediática del hecho que una población sea vulnerable a este tipo de ataques, provoca irremisiblemente el pánico en una nación.

En este aspecto, la violación de los sistemas de defensa del Estado, pueden generar conflictos a nivel internacional, debido a la utilización de elementos que puedan ser analizados y observados como intentos de agresión contra otro Estado tanto fronterizo como del área de influencia.

Tampoco podemos olvidar que los ejércitos de la mayoría de países desarrollados, están creando o poseen ya secciones especializadas en la detección y el uso de ciberataques como una importante arma de guerra. Entiendo que esto es una sana y proactiva acción a imitar para la defensa de nuestro Estado.

d) Los Cuerpos de Seguridad del Estado

Estos Cuerpos de Seguridad son conformados, a nuestro entender, principalmente por la Policía Nacional, el Departamento Nacional de Investigaciones y la Superintendencia de Vigilancia y Seguridad Privada. Es quizás en estos cuerpos, donde la base del cubo de COSO debe tener una presencia más fuerte, por la diversa cantidad de recursos humanos que la conforman y por la labor directa que realizan de protección ciudadana, tanto pública como privada.

Como es de conocimiento, la Policía Nacional Dominicana es la institución pública encargada de imponer control, orden y seguridad a los residentes y ciudadanos de República Dominicana. La Fuerza Nacional de Policía (tal

y como es hasta el día de hoy) no fue formada oficialmente si no hasta el 2 de marzo de 1936 con la aprobación congresional del decreto No. 1523. Anteriormente, durante la ocupación norteamericana en Santo Domingo de 1916 a 1924, existió la denominada como ‘’Guardia Nacional”, cuerpo castrense que funcionaba como agencia de defensa y policía.

Para establecer el orden público, la policía cuenta con divisiones especializadas de homicidios, de investigaciones criminales, antinarcóticos, de asuntos internos, de crímenes tecnológicos, científica, preventiva, entre otras. En adición, cuenta con una Unidad de Policía Turística y otras Unidades Especiales.

Por la gran diversidad de Unidades y Divisiones con la que cuenta la Policía Nacional, se exige tener un Departamento de Gestión Humana bien robusto que analice los perfiles correctos para cada área y realice pruebas para evaluar la integridad, ética y moral de los candidatos. Sin embargo, es en la escuela de entrenamientos donde deben reforzarse los valores mencionados por los Oficiales de alto rango para que los aspirantes perciban inmediatamente el “Tone from the Top” e imiten las acciones de sus superiores y al mismo tiempo, teman de hacer cualquier acción equívoca.

La mejor reflexión sobre el cambio de imagen que pueda recordar sobre la Policía, es el de la ciudad de New York. Hace unos años que, caminar de noche por las calles de Manhattan era más que peligroso. La combinación de vandalismo juvenil, epidemia de crack, cocaína y corrupción policial, arrojaba cifras alarmantes.

Hoy New York está mucho mejor y basta un paseo nocturno por alguno de sus barrios, para entender por qué ahora es considerada una de las ciudades más seguras de los Estados Unidos. La razón principal de la transformación radical de esta metrópolis fue la aplicación de la política de seguridad conocida como “Tolerancia Cero”. Con ese concepto como vector ideológico se bajó el índice criminal en más de un 60% entre 1990 y 2007, por lo que esa ciudad ya es considerada en el mundo un paradigma en la lucha contra el delito urbano.

El modelo impulsado en 1994 por el entonces alcalde de la ciudad, el republicano Rudolph Giuliani, se basó en una serie de medidas simples: Se puso énfasis en la prevención de crímenes, se multiplicó la presencia de policías en las calles, se restableció el vínculo entre la fuerza y la comunidad y se puso especial énfasis en prevenir y perseguir determinadas contravenciones graves o delitos menores, como pintar graffiti o beber alcohol en la vía pública. Obviamente, el éxito de Giulliani contó con el apoyo del Jefe de la Policía de aquel momento, señor William Bratton, quien estaba entregado a la causa. Este ejemplo confirma que la voluntad ciudadana, sindical y senatorial es importante, para que la Policía no trabaje sola.

El Departamento Nacional de Investigaciones (DNI) está facultado para cumplir su misión, amparado en la Ley 857 del 22 de julio de 1978 y constituye un organismo de apoyo a la estrategia de seguridad nacional, en procura de mantener la estabilidad, orden, prosperidad y continuidad del Estado dominicano.

Como Agencia de Inteligencia, recolecta, procesa y disemina información referente a la seguridad del Estado y sus instituciones, cuyo producto está destinado a servir de base, a la toma de decisiones de los más altos niveles de mando de la nación.

También tiene como misión la colecta, procesamiento y diseminación relativos al crimen organizado, nacional o extranjero, a fin de poder detectar los indicadores que revelen el desarrollo de las actividades delictivas que atentan contra la seguridad del Estado, el orden público, la Constitución y las leyes.

La gran importancia del DNI radica en que son un grupo de personas especializadas en realizar las investigaciones relacionadas a los flagelos que afectan a nuestra sociedad y también en que son un órgano que cuenta con las habilidades, inteligencia y pericia para anticiparse a acontecimientos negativos que pudieran afectar a la seguridad ciudadana y estatal. El perfil de sus Recursos Humanos prima en lo analítico y en la capacidad que puede tener un miembro de analizar desde diferentes vertientes, sin estar sesgado, cualquier situación que afecte la seguridad.

A lo largo de los años, el DNI ha sido partícipe de muchas investigaciones importantes y ha trabajado en conjunto con la Dirección Nacional de Control de Drogas (DNCD) y la Administración para el Control de Drogas (DEA por sus siglas en inglés) en operaciones antinarcóticos importantes para la nación y Latinoamérica, con el bajo perfil que la caracteriza.

Es muy válido mencionar también la creación del Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), como entidad subordinada a la Dirección Central de Investigaciones Criminales de la Policía Nacional, mediante la emisión de la Ley 53-07. El artículo 30 de esta Ley también la composición de una comisión internacional contra crímenes de alta tecnología.

Los ciberdelincuentes se aprovechan de debilidades que poseen los sistemas, producto de no tener un buen antivirus, el sistema no operativo no estar actualizado con las últimas técnicas de seguridad, instalan muchas aplicaciones de terceros sin conocerlas, entre otros.

Cuando la máquina logra infectarse, el ciberdelincuente toma el control de la máquina afectada. El delincuente captura la información de los correos enviados, donde se detallan las solicitudes, facturas, comprobantes de pagos números de cuentas, entre otros documentos. Posteriormente, el ciberdelincuente suplanta la identidad de la persona y manda un correo con una discrepancia de una letra, numero, un punto, etc. Esa discrepancia, que en muchas ocasiones, no es identificada por el usuario, hace que el ciberdelincuente logre desviar dinero a otra cuenta bancaria.

En lo que respecta a esta línea, llama la atención que los miembros del Crimen Organizado a través de "hackeos" y de ciberataques, pueden alterar o vulnerar también los sistemas del DICAT. De esta manera, pueden acceder a informaciones de investigaciones y otras de tipo confidencial, colocando en minusvalía al Estado.

Siguiendo con el orden de órganos que aportan a la Seguridad Nacional, se encuentra la Superintendencia de Vigilancia y Seguridad Privada (SSP), quien es una dependencia del Ministerio las Fuerzas Armadas que tiene por objeto promover, regular y fiscalizar las entidades, servicios o actuaciones del personal y medios en materia de Seguridad Privada y sus modalidades en todo el territorio nacional, normando las actividades de las empresas y personas que se dedican a las actividades de Seguridad Priva-

da en todas sus modalidades en todo el territorio nacional, en la forma establecida por los Reglamentos vigentes.

El 26 de abril de 1982, mediante el decreto No.3222, fue creada la Junta Reguladora de Empresas de Vigilantes Privados. Mediante el Decreto No. 1128-03 de fecha 15 de diciembre del 2003, publicado en el Gaceta Oficial No. 10244 de fecha 30-12-2003, se crea la SSP y se aprueba su Reglamento de funcionamiento.

La SSP juega también un rol muy importante en la seguridad nacional, principalmente en lo que respecta a la seguridad ciudadana. De aquí radica la importancia de tener a dueños de empresas de vigilantes que estén previamente depurados y autorizados por el Ministerio de Defensa para realizar sus actividades y que los vigilantes privados sean bien formados y entrenados, no solo en temas de seguridad física, sino también en educación cívica y valores patrios. Hago énfasis en esto, porque lamentablemente, la mayoría de los guardianes o vigilantes no gozaron de una educación robusta en su juventud por las precariedades que aún persisten en el sistema educativo de nuestro país o simplemente no asistieron a ningún centro educativo.

Aparte del tema de la educación cívica, entiendo que el factor "salario" tiene también mucha incidencia en el comportamiento de los guardianes de seguridad. Este aspecto es muy serio por el hecho que esos guardianes, como seres humanos que son, necesitan un sustento razonable para ellos y su familia. No vamos a entrar en detalles con este tema porque no es el enfoque del artículo, pero obviamente tendrían que analizarse en una mesa redonda con las compañías de guardianes, la SSP, entre otros actores de esta área, los efectos de adecuar presupuestos que contemplen revisiones de costos, gastos, etc. antes de realizar un aumento salarial y de proporcionar beneficios como buenos planes de salud y pensión a los mismos.

Conclusión

Sin deseo de sonar crudos, querremos concluir señalando que estamos frente a modelos sociales distintos a los que solíamos tener en pasadas generaciones. En esta era de la tecnología, los "Falsos Líderes" y "Personas Exitosas" disfrutando de paseos en lanchas, descorchando champañas o whiskies caros en una marina, club o bar, disfrutando en eventos sociales rodeados de mujeres hermosas, entre otras cosas, están a la orden del día en las redes sociales y muchos de ellos incluso son felicitados por sus acciones con un "like". En este sentido, pensamos que existen dos cosas muy distintas sin ánimo de criticar a la tecnología de la que todos, en cierta forma, nos beneficiamos: Una primera cosa es tener acceso a la tecnología y la informaciones, una segunda y, más importante que la primera, es saber digerir la información y tener una psicología con cimientos fuertes, que pueda sobrellevar y entender que muchas cosas que se notan a simple vista, son placebos.

Antes de la proliferación masiva de las redes sociales, pocas personas tenían voz; ahora mismo, ya todos la tienen en las redes. En el mundo de hoy todas las opiniones parecen contar y se cuestiona, incluso, la buena educación, el ser formal, el actuar, tomar decisiones en base a valores y el no "buscársela", hablando en buen dominicano. Como si fuera poco, también está bien de moda en el mundo el irrespeto a los símbolos patrios, bajo falsos pretextos.

¿Por qué damos un enfoque a las redes sociales y a la tecnología en esta problemática? Es simple, la nueva genera-

ción vive en torno a ellas. También guían el actuar e incluso el razonamiento de la gran mayoría de los jóvenes.

¿Qué podemos esperar? Entendemos que aún estamos a tiempo, pues muchos de los padres o tutores de la generación de los Millennials aún viven y podrían hacer un último esfuerzo de concientizarlos sobre la importancia de la ética, los valores y el respeto a los símbolos patrios para que estos, a su vez, puedan inculcarles conceptos a la generación de personas que nacieron desde el año 2000 en adelante. Si esto no se hace ahora, estamos seguros que estaremos viviendo en un mundo más distinto al que vivimos hoy en día, donde no existirán estructuras familiares sólidas y mucho menos la preocupación ciudadana de manera generalizada, por lo que significa realmente la seguridad de una nación.

También, tomando en consideración la situación que se presenta con los ataques cibernéticos en contra de las actividades propias del Estado, lo convierten desde el punto de vista de la Defensa en VULNERABLE, ya que puede ser objeto de ataques no solamente de un Estado vecino o de una Fuerza Armada, sino que también está propenso a que los integrantes del crimen transnacional organizado pueden alterar el buen funcionamiento de los distintos sistemas operativos de los diferentes entes del Estado, causando graves consecuencias a la Defensa Nacional.

El Gobierno está consciente de que enfrentar el desafío cibernético es y será difícil. La naturaleza inherente de la delincuencia informática hace que sea un nuevo paradigma para las fuerzas del orden. Se reconoce que hay deficiencias existentes en nuestra capacidad, procesos y tecnología para investigar y judicializar estos delitos. Además, se reconoce que la naturaleza transfronteriza de la delincuencia cibernética requiere una cooperación internacional para ayudar en los esfuerzos de fiscalización, mitigación y recuperación. En este sentido, se reconoce que la comunidad académica y el sector privado son actores fundamentales en la protección de nuestro ciberespacio.

Referencias Bibliográficas

Recuperado de https://es.wikipedia.org/wiki/COSO_(administraci%C3%B3n)

Recuperado de http://www.poderjudicial.gob.do/poder_judicial/info_gral/poder_ judicial.aspx

Recuperado de http://pgr.gob.do/procuraduria-especializada-de-antilavado-de-activos-2/

Recuperado de http://www.dni.gov.do

Recuperado de http://www.ssp.mil.do

Sansó-Rubert P., D. (2013). La seguridad ciudadana y las Fuerzas Armadas: Despropósito o último recurso frente a la delincuencia organizada? *Revista criminalidad*. 55 (2).