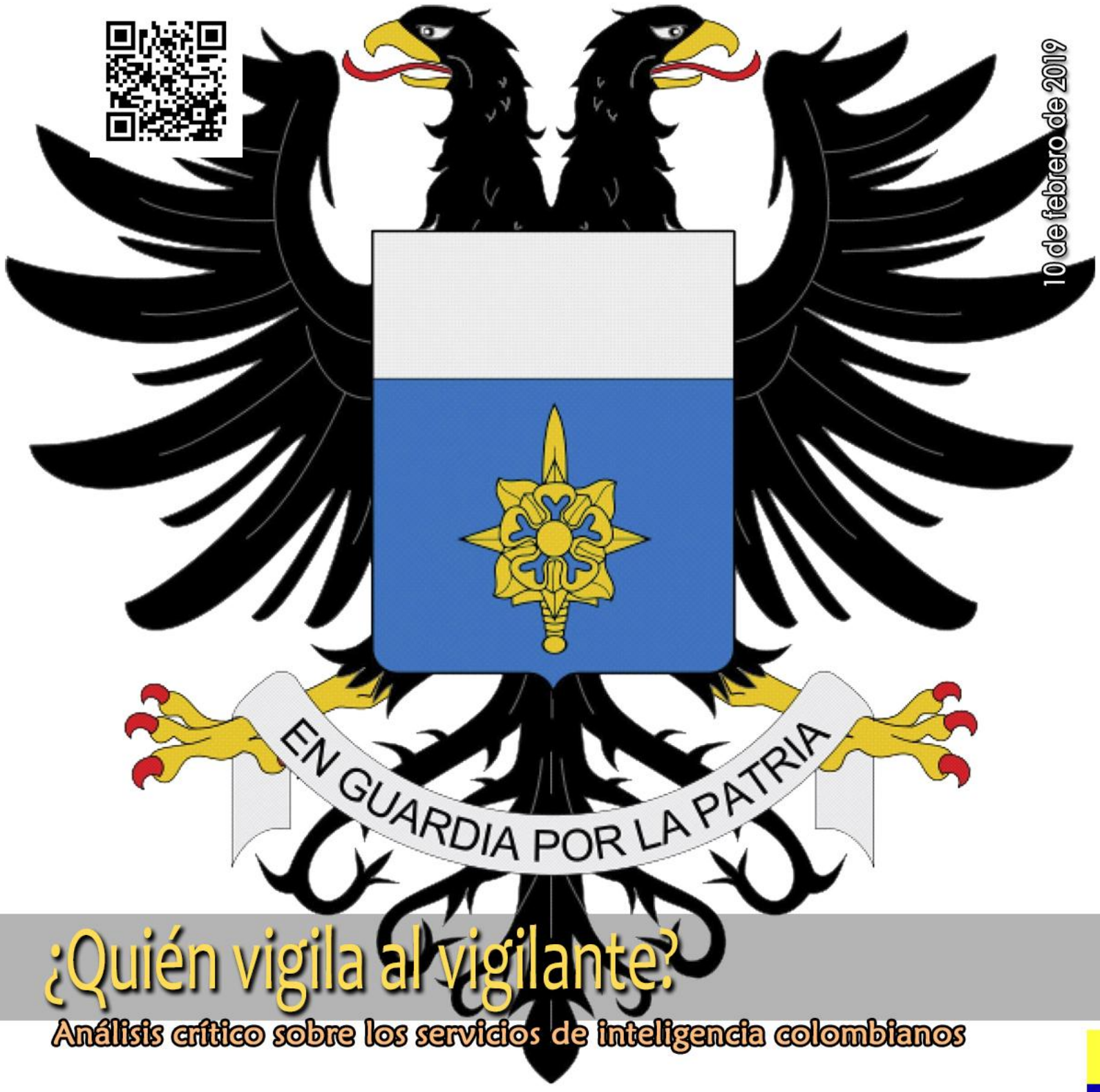
TRIARIUS

Observatorio Internacional sobre el Terrorismo y las Nuevas Amenazas

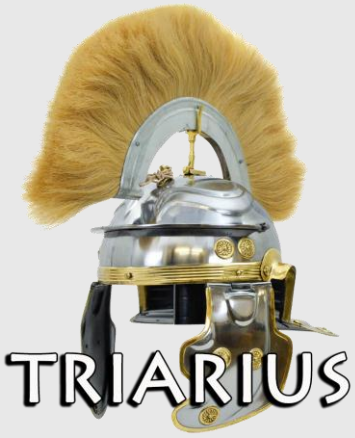
Volumen 3 - Edición Especial Nº 21



10 de febrero de 2019

¿Quién vigila al vigilante?

Análisis crítico sobre los servicios de inteligencia colombianos



Medellín - Colombia
Edición Especial No. 21
10 de febrero de 2019

Editor
Douglas Hernández

Autor de esta obra
Douglas Hernández (Colombia).

Fundador y director del website
www.fuerzasmilitares.org

Esta es una edición especial publicada por el Observatorio Internacional sobre el Terrorismo y las Nuevas Amenazas. Complementa el Boletín que se publica regularmente cada 15 días.

Información de Contacto:

Douglas Hernández
Medellín, Colombia
Movil: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com

Presentación

El presente es un ejercicio académico, realizado en el marco del Master en Seguridad de la Información, del United States Security College. Abarca algunos aspectos básicos sobre la ciberseguridad, y profundiza en el tema del mal uso de las capacidades de ciberinteligencia por elementos de los organismos de seguridad colombianos.

En el contexto de la comunidad de inteligencia colombiana, se plantea una pregunta clave: ¿quién vigila al vigilante?, aspecto de mucha importancia en la actualidad, habida cuenta de los distintos problemas éticos que se han venido presentando en este país, donde un conjunto de funcionarios ha cometido delitos directamente relacionados con el mal uso de los recursos, habilidades, e información de inteligencia.

En este trabajo se relacionan algunos de esos bochornosos hechos con el fin de ejemplificar lo que no se debe hacer, y se plantean algunas posibilidades de mejora.

¡Conocer para vencer!

Douglas Hernández
Editor

¿Quién vigila al vigilante?

Por Douglas Hernández[1]

Resumen

Luego de una contextualización útil a quienes no manejan los temas de la ciberseguridad, en este artículo se hace un repaso a las ciberamenazas que podrían afectar a la sociedad colombiana. También se pasa revista a los organismos encargados de detectar y detener a los ciberdelincuentes, ojalá antes de que cometan el cibercrimen. Para concluir con una reflexión sobre la ética que debe prevalecer entre los integrantes de dichos organismos de seguridad, para no terminar ellos mismos abusando de sus capacidades y convirtiéndose en ciberdelincuentes.

Palabras Clave

Cibercrimen, Ciberdelincuente, Ciberseguridad, Ciberdefensa, Ética

Abstract

After a useful contextualization to those who do not handle cybersecurity issues, this article reviews the cyberthreats that could affect Colombian society. Also are reviewed the agencies charged with detecting and detaining cybercriminals, hopefully before they commit cybercrime. To conclude with a reflection on the ethics that should prevail among the members of these intelligence organizations, so as not to end up abusing themselves of their abilities and becoming cybercriminals.

Keywords

Cybercrime, Cybercriminal, Cybersecurity, Cyberdefense, Ethics

Introducción

La modernidad ha traído importantes cambios para la humanidad -que en buena medida han sido positivos-. Sin embargo, los adelantos científicos y técnicos que se han presentado en todos los ámbitos del quehacer humano tienen un lado oscuro. Tal es el caso de la electrónica, la informática y las Tecnologías de la Información y la Comunicación. La facilidad existente para el manejo, flujo y almacenamiento de grandes volúmenes de información, en mayor o menor medida sensible, hace que sea necesario protegerla, no solo de eventualidades de orden natural o accidental, sino también de personas u organizaciones con habilidad técnica y malas intenciones.

Es necesario entonces que las organizaciones públicas y privadas creen un Sistema de Gestión de Seguridad de la Información (SGSI), que les permita identificar sus vulnerabilidades y aplicar los apropiados correctivos. De igual forma, es indispensable que las autoridades policiales y judiciales se mantengan actualizadas y dispuestas a prevenir y/o reprimir los delitos que se cometan en o desde el ciberespacio. Debe haber unidades altamente especializadas encargadas de vigilar y prevenir el cibercrimen. Sin embargo, ese tipo de unidades se vuelven a su vez una potencial amenaza, de ahí que quepa preguntarse, ¿Quién vigila al vigilante?

[1] Douglas Hernández (Colombia) es sociólogo, magister en educación, doctorando en gerencia, masterando en ciencias de la seguridad y masterando en seguridad de la información. Posee un diplomado en relaciones internacionales. Se desempeña como docente de posgrado en la Universidad de Antioquia.

Metodología

El presente artículo es producto de una investigación documental en fuentes públicas (Open Source Intelligence, OSINT).

Breve Marco Conceptual

Con el fin de ilustrar a los lectores que no estén familiarizados con las temáticas abordadas en este documento, a continuación se presenta un breve glosario de términos. Las definiciones no son exhaustivas ni profundas, pues no se considera necesario para los objetivos que se pretende alcanzar. El listado no está en orden alfabético, sino en un orden lógico.

***Ciberespacio*:** Es aquel entorno no físico que se crea al interoperar en una red de computadores u otros dispositivos capaces de conectarse a esa red.
***Cibercrimen*:** Es la violación de la ley en o desde el ciberespacio.
***Ciberterrorismo*:** Consiste en usar el ciberespacio o los dispositivos conectados a la red, para desarrollar actividades que causen terror en una gran masa poblacional, teniendo como fin un objetivo de tipo político.
***Ciberguerra*:** Es una guerra que se desarrolla en el ciberespacio.
***Ciberguerrero*:** El que lucha una ciberguerra.
***Ciberseguridad*:** Medidas destinadas a proteger los datos, los bienes, y a las personas, del accionar de cibercriminales.
***Ciberdefensa*:** Medidas destinadas a mantener la cibersoberanía, y contrarrestar el accionar de ciberguerreros de Estados hostiles o pertenecientes a grupos organizados no estatales que pretendan vulnerar los intereses nacionales de carácter estratégico. También se refiere a las medidas tomadas para contrarrestar el ciberterrorismo.
***Cibersoberanía*:** Capacidad para operar en el ciberespacio con libertad de acción, a resguardo de ciberterrorismo, cibercrimen, o cualquier tipo de coacción que limite esa libertad, más allá de los límites que imponen las buenas costumbres y las leyes.
***Sistema de Gestión de Seguridad de la Información (SGSI)*:** Conjunto de medidas racionales y sistemáticas que se toman al interior de una organización para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información que allí se maneja. (Ver la norma ISO 27001).
***Activo de Información*:** Son los recursos registrados en el Sistema de Gestión de Seguridad de la Información y que son necesarios para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección
***Amenaza*:** (Threat) Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. (ISO/IEC 13335-1:2004).
***Vulnerabilidad*:** (Vulnerability) Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. (ISO/IEC 13335-1:2004).
***Riesgo*:** (Risk) Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias. (ISO Guía 73:2002)
***Magerit*:** Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica de España, para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información. Inicialmente la metodología estaba está enfocada a las Administraciones Públicas, pero se ha popularizado también en lo empresarial.
***Información*:** Noticia de un hecho en su sentido más amplio. El concepto información debe entenderse, por tanto, como el elemento de partida para la elaboración de inteligencia.

***Inteligencia*:** Es el resultado de valorar, analizar, integrar e interpretar la información.
***Fuente*:** Persona, animal, cosa o fenómeno, del que se obtiene información.
***Informantes*:** Persona que consciente o inconscientemente proporciona información.
Ciclo de Inteligencia: Es el proceso mediante el cual se crea inteligencia. En su definición tradicional, se trata de cinco pasos por medio de los cuales se genera conocimiento de interés, útil y verdadero, que se ajusta a los requerimientos de información establecidos por un destinatario final (decisor), a quien se difundirá de manera selectiva el resultado final. Los cinco pasos son: Planeación, Recolección de Información, Análisis, Difusión, Explotación.
***Espionaje*:** Sinónimo de inteligencia actualmente desuso y considerado despectivo.
***Vigilancia*:** Acción de observar metódicamente las actividades de personas o grupos. Sinónimo de monitorear.
"*Chuzada*": Forma coloquial colombiana de referirse a interceptaciones ilegales, bien sea de la línea telefónica, los dispositivos electrónicos, o a través de la colocación subrepticia de micrófonos o grabadoras.
***Fraude (electrónico)*:** Engaño con la intención de conseguir un beneficio económico. En este contexto, este engaño ocurre en el ciberespacio o a través de este.
***Estafa*:** El Código Penal Colombiano tipifica la estafa cuando se obtiene provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños. Sinónimo de fraude.
***Ingeniería Social*:** Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Técnica empleada por personas malintencionadas para obtener acceso, privilegios o información, en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organización comprometida a riesgo o abusos. La ingeniería social se sustenta en el principio de que los usuarios son el eslabón débil de cualquier sistema.
***Phishing*:** consiste en el envío de correos electrónicos o mensajes de texto que aparentan provenir de fuentes confiables (por ejemplo, bancos o empresas reconocidas), y que intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. Estos mensajes falsos, suelen incluir un enlace que lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada, misma que en realidad va a parar a manos del estafador.
***Suplantación*:** El phishing también es conocido como suplantación de identidad.

Breve Marco Legal y Normativo

A los efectos de este artículo, las siguientes son las normas de interés:

- Constitución Política de Colombia.
- Ley 599 del 2000 - Código Penal Colombiano.
- Ley 1407 del 2010 - Código Penal Militar Colombiano.
- Ley 1437 del 2011 - Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1621 del 2013 - Ley de Inteligencia y Contrainteligencia.
- Ley 1273 del 2009 - Ley de Protección de la Información y de los Datos.
- Ley 1341 del 2009 - Ley de las Tecnologías de la Información y las Comunicaciones, TIC.
- Conpes 3701 de 2011 - Lineamientos de política para la Ciberseguridad y Ciberdefensa.
- ISO 27001:2003 Sistemas de Gestión de la Seguridad de la Información.

Antecedentes

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, MINTIC (2016), señaló que el Centro Cibernético Policial recibió cerca de 34 denuncias semanales durante el año 2016, atendiendo distintos tipos de ataques contra los sectores económico, financiero, social y gubernamental. El Centro Cibernético Policial fue creado para enfrentar el cibercrimen y las ciberamenazas que van incrementándose a medida que la tecnología avanza.

> *El contexto del cibercrimen aborda todo tipo de esferas; en ese sentido firmas de auditoría y el Centro Cibernético Policial argumentan que el 46 % de los crímenes informáticos se dan por la carencia de elementos de seguridad, asimismo existen cuatro tipos de crimen que afecta el sector económico: malversación de activos, fraude financiero, corrupción y cibercrimen (MINTIC, 2016, s/p).*

Semana (2017), nos señala que para ese año el cibercrimen se incrementó. Según esta fuente los delitos subieron un 28%, causando pérdidas por un monto superior a los 50.000 millones de pesos (aproximadamente 18 millones de dólares). Durante el 2017 fueron capturados 459 cibercriminales, por diversos delitos.

Una fuente de preocupación constante para las autoridades colombianas, es el tema de los delitos contra los niños y adolescentes. Por ejemplo, para el 2017 la Policía Nacional de Colombia bloqueó 3.891 páginas que alojaban contenidos considerados de pornografía infantil y capturó a 56 ciudadanos por dicho delito. Pero están surgiendo otras amenazas no convencionales a las que también hay que prestar atención. En el 2017 uno de esos fenómenos fue "reto de la ballena azul", un absurdo juego que se propagó por la red y en el que los menores eran retados a hacerse daño progresivamente hasta ser llevados al suicidio. Las autoridades colombianas emitieron durante el 2017, un total de 508 alertas por ese juego, que llegaron a 6 millones de personas, y además se identificó y desactivó a tres grupos que lo promovían.

Otra manifestación importante del cibercrimen en Colombia es la estafa. En el año 2017, un total de 6.372 ciudadanos denunciaron haber sido estafados a través del Internet, por un monto que supera los 15.000 millones de pesos (aproximadamente 5.4 millones de dólares), estas estafas se dieron en el marco de compras virtuales que fueron pagadas, pero en las que el cliente nunca recibió el producto. De manera adicional, cerca de 2.000 personas denunciaron a las autoridades que habían sido asaltadas por medio de llamadas telefónicas y mensajes de texto.

Además de lo anterior, 182 ciudadanos denunciaron haber sido estafados a través de operaciones con bitcoin, en una modalidad de captación ilegal al modo de las pirámides que promovía la empresa DMG[2] en el país. Se trataría pues de una ciberpirámide que operaba en 11 ciudades de Colombia. Por esta estafa las víctimas perdieron al menos 1.500 millones de pesos (unos 535 mil dólares).

Los cibercriminales son cada vez más capaces y más osados. De ahí que tanto el Estado como las grandes corporaciones hayan sido también víctimas de cibercrímenes. La Policía Nacional informó que debido a accesos abusivos a los sistemas informáticos de diferentes alcaldías colombianas, se perdieron al menos 50.000 millones de pesos -aproximadamente 18 millones de dólares-. (Semana, 2017, s/p).

[2] Empresa colombiana que se presentaba formalmente como una comercializadora de bienes y servicios a través de tarjetas prepago, que revertía a sus clientes pagos por publicidad en un esquema de mercadeo multinivel. Su fundador, representante legal y principal accionista, fue el ciudadano David Murcia Guzmán (DMG). DMG fue intervenida y disuelta por las autoridades colombianas el día 18 de noviembre de 2008, seguida por acciones similares en Panamá, Venezuela y Ecuador donde tenía sucursales.

Además de los ciberataques realizados por cibercriminales criollos, el país también ha sido víctima de grandes ataques cibernéticos originados en el exterior, o que han tenido un impacto global. Por ejemplo, durante el 2017 se difundió un malware que secuestraba con fines extorsivos los datos de los dispositivos que atacaba, al que se llamó "Wannacry", Colombia fue uno de los 150 países afectados. La Policía Nacional generó 59 alertas por estos ataques globales, y atendió a 52 víctimas del malware reseñado.

En el consolidado del 2017 las autoridades reportan la captura de 459 personas y el desmantelamiento de 30 organizaciones dedicadas al cibercrimen. En materia de prevención, las campañas de la Policía Nacional -a través de la DIJIN[3]- alcanzaron a unos 3,6 millones de personas, y se capacitó a otras 1.192 en la prevención del cibercrimen.

Índice Mundial de Seguridad Cibernética

Las Naciones Unidas poseen un organismo especializado llamado *Unión Internacional de Telecomunicaciones* (ITU)[4] que agrupa a 193 países miembros, este organismo publica un documento llamado *Índice Mundial de Seguridad Cibernética*, que mide el nivel de compromiso de sus afiliados en ese campo y les ayuda a diseñar estrategias para enfrentar las nuevas amenazas. De forma adicional este estudio muestra la mejora y el fortalecimiento de los indicadores técnicos, organizacionales, y legales, así como la cooperación internacional de cada país en el terreno de la seguridad cibernética. En la edición del 2017 del Índice Mundial de Seguridad Cibernética, Colombia ocupó el puesto 46 a nivel mundial y el puesto número 6 a nivel de América.

El Índice Mundial de Seguridad Cibernética evalúa 31 indicadores, a los que asigna una clave de colores, al modo de un semáforo. El color rojo es para los indicadores que no aplican en el país de referencia, el color amarillo es para aquellos que se están implementando hace poco, y el verde para aquellos que aplican en su totalidad en el país evaluado. Ospina (2017) nos señala lo siguiente:

> *De los 31 indicadores, Colombia tiene 17 en color verde, cinco en amarillo y nueve en rojo. En aspectos legales, nuestro país cuenta con una legislación en contra del cibercrimen y en pro de la ciberseguridad. "Colombia se convirtió en uno de los primeros países del mundo cuando, en 2009, promulgó una ley específicamente dirigida al ciberespacio. Esta se llama Ley 1273 'Protección de la información y los sistemas de datos'". (s/p)*

A continuación, podemos apreciar la evaluación de Colombia para cada uno de los ítems considerados en el Índice.

Global Security Index 2017

Scorecard Colombia	
Cybercriminal Legislation	
Cybersecurity Legislation	
Cybersecurity Training	
Legal Measures (suma los items superiores)	
National CERT/CIRT/CSIRT	
Government CERT/CIRT/CSIRT	
Sectorial CERT/CIRT/CSIRT	
Standards for Organization	

[3] Dirección de Investigación Criminal e INTERPOL. La entidad conserva su antigua sigla, DIJIN, que significa Dirección Central de Policía Judicial e Inteligencia. https://www.policia.gov.co/dijin

[4] En este enlace puede visitarse el website de la entidad: https://www.itu.int/es/Pages/default.aspx

Standards for Profesionals	
Child On Line Protection	
Technicals Measures	
Strategy	
Responsible Agency	
Cibersecurity Metrics	
Organizational Measures	
Standarization Bodies	
Cybersecurity Good Practices	
R&D Programmes	
Public Awareness Campaigns	
Professional Training Courses	
Educationn Programmes	
Incentive Mechanisms	
Homegrown Industry	
Capacity Building	
Bilateral Agreements	
Multilateral Agreements	
International Participation	
Public-Private Partnerships	
Inteagency Partnerships	
Cooperation	
GCI (resultado general)	

Adaptado del Índice Mundial de Seguridad Cibernética 2017 (ITU, 2017, p.29)

Así como en el sector educativo se toman como referencia unas pruebas internacionales para verificar los avances en la calidad de la educación que se imparte en Colombia (Talis, Pisa, Erce), en el sector de ciberseguridad el *Índice Mundial de Seguridad Cibernética* ofrece un referente válido para medir los avances y retrocesos en la materia. El gobierno nacional y los expertos en ciberseguridad deben estar atentos cada año a la publicación del índice y ejecutar las acciones y recomendaciones que le permitan al país mejorar en este campo tan dinámico, y que hoy en día reviste un carácter estratégico.

Unidades Especiales de Ciberseguridad en Colombia

Según Ospina (2017) en el Índice Mundial de Seguridad Cibernética, se señala que en Colombia operan diferentes equipos de respuesta para emergencias cibernéticas. Entre ellas:

- ColCERT del Ministerio de Defensa.
- SOC-CCOC Comando de Operaciones Cibernéticas de las Fuerzas Militares.
- CSIRT de la Policía Nacional.
- CSIRT-ETB de la Empresa de Telecomunicaciones de Bogotá.
- CCIRT-CCIT de la Cámara Colombiana de Informática y Telecomunicaciones.

Sin embargo, en la valoración que se hace en el Índice mencionado, Colombia tiene dos calificaciones negativas debidas a la carencia de "un centro de respuesta a ataques en los sectores empresariales y en la protección a menores en la red[5]." (Ospina, 2017, s/p).

Efectivamente, en el documento Conpes 3701 de 2011, citado por Cáceres (2017) se establece la creación de algunas entidades del gobierno que atenderán las ciberamenzas, así:

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa.
- El Comando Conjunto Cibernético de las Fuerzas Militares, (CCOC) que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.
- El Centro Cibernético Policial, (CCP) que estará a cargo de la prevención e investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un Comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos.

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT (2018) manifiesta en su website oficial (http://www.colcert.gov.co) que su misión es la siguiente:

> *El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. (s/p)*

Nos dice la misma fuente que sus objetivos son:

- *Coordinar y asesorar a CSIRT's[6] y entidades tanto del nivel público, como privado y de la sociedad civil para responder ante incidentes informáticos.*
- *Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.*
- *Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta técnica.*
- *Promover el desarrollo de capacidades locales/sectoriales, así como la creación de CSIRT's sectoriales para la gestión operativa de los incidentes de ciberseguridad en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.*
- *Desarrollar y promover procedimientos, protocolos y guías de buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad para las infraestructuras críticas de la Nación en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.*
- *Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad.*

[5] Sin embargo, este último punto debería ser reevaluado, pues como ya se mencionó antes en este artículo, para el 2017 la Policía colombiana habría bloqueado a 3.891 websites que alojaban contenidos considerados de pornografía infantil y reportó la captura de 56 personas por dicho delito.

[6] Computer Security Incident Response Team.

- *Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.*
- *Fomentar un sistema de gestión de conocimiento relativo a la ciberdefensa y ciberseguridad, orientado a la mejora de los servicios prestados por el ColCERT.*

Para atender los ciberdelitos, en Colombia la Policía Nacional ha encargado de esa función a la Dirección de Investigación Criminal e INTERPOL, mejor conocida por las siglas DIJIN. Esta entidad trabaja en tres aspectos de suma importancia:

- **Preventivo:** A través del website: www.delitosinformaticos.gov.co, expertos en el cibercrimen atienden las inquietudes de los ciudadanos y dan recomendaciones para no ser víctima de los ciberdelincuentes.
- **Investigativo:** Coordinando todas las actividades con la Fiscalía y las autoridades competentes para recopilar el material probatorio.
- **Político:** Participando en la promulgación y elaboración de proyectos de ley que permitan tipificar estas prácticas y disminuir este tipo de delincuencia.

Gracias a la existencia del documento Conpes 3701 del 2011, la Ley 1273 de 2009, la dinámica ejecutoria del MinTic, y la existencia de Colcert, el CCOC y el CCP, la ciberseguridad en el país se ha fortalecido.

Para sumar esfuerzos y difundir información de interés, se han venido desarrollando anualmente distintos eventos, como foros, seminarios y encuentros internacionales, sobre el tema de la ciberseguridad. El más reciente sea quizá el IV Foro de Seguridad Digital 2017, realizado en agosto de ese año y que fue instalado por el entonces Viceministro de Defensa Anibal Fernández de Soto en el Hotel Tequendama de Bogotá, según señala Colombia Estéreo (2017). La cuestión electoral y de cambio de gobierno, quizá motivo que en el 2018 no se diera continuidad a este proceso.

Valga anotar que la *Escuela Superior de Guerra de Colombia* (ESDEGUE) ofrece una Maestría en Ciberseguridad y Ciberdefensa[7], lo que da cuenta de la importancia que se da a estos temas desde el alto gobierno del país.

Colombia parece haber dado importantes y lógicos pasos en la dirección correcta, y además ha creado un ecosistema de alto nivel, para la ciberdefensa y la ciberseguridad, que crece y se fortalece continuamente, y al hacerlo, aumenta también la ciberseguridad y la cibersoberanía nacional. Sin embargo, los ciberdelincuentes evolucionan constantemente y aplican nuevas técnicas, lo cual requiere una constante actualización de las autoridades. Más adelante veremos lo que pasa cuando las autoridades se corrompen y en lugar de cumplir con su deber, ellos mismos se tornan en ciberdelincuentes.

Ciberdelincuentes colombianos

En Colombia ha habido una serie de casos emblemáticos, en donde ha sido posible individualizar al ciberdelincuente.

Ávila (2016) reseñó en un artículo para El Tiempo a 4 ciberdelincuentes que son de interés para este trabajo.

El primero de ellos se hacía llamar “Oroboruo”, a quien se señala de ser el autor material de 3.193 ataques a 1.374 dominios, muchos de ellos del gobierno colombiano, principalmente inyectando códigos maliciosos o desconfigurándolos. Precisamente, el caso más sonado fue el

[7] http://www.esdegue.mil.co/maestria/ciber

hackeo a la página de la Registraduría Nacional del Estado Civil[8], en los días previos al plebiscito por la paz[9].

Este ciudadano, de nombre *Juan Esteban Ramírez Gil* y de 27 años de edad para el momento de su detención (02OCT2016), es oriundo de Medellín, Antioquia. Más precisamente del barrio Buenos Aires. Cuando fueron a capturarlo en su residencia, las autoridades descubrieron que Ramírez pertenecía a un grupo autodenominado "*Colombian Hackers*"[10], organización que alardeaba de sus actividades ilegales en un foro denominado *Zone-H*[11], donde se encontró la lista de objetivos que alías "Oroboruo" habría atacado a lo largo de carrera como hacker, incluyendo el ataque a la página de la Registraduría, canales de televisión, páginas de apuestas, emisoras, organizaciones varias, y en particular entidades del gobierno. Según dicho registro, su primer ataque fue a la Alcaldía de Ibagué el 23 de octubre del 2015, y el último a la Alcaldía de Cúcuta.

Al hacker se le incautaron 3 discos duros, 52 CD's, una antena para amplificar señales inalámbricas, un portátil y 101 manuscritos con apuntes donde documentaba sus actividades, instrucciones y comandos para acceder ilegalmente a redes inalámbricas, modificar bases de datos, o probar vulnerabilidades de sistemas de información. Este material lo estaría compartiendo por Internet con otros cibercriminales.

Este cibercriminal fue capturado por la Policía Nacional de Colombia, y siendo un delincuente de alto perfil el propio Director de la Policía, General Jorge Hernando Nieto Rojas, se pronunció en los medios para anunciar que sería puesto a disposición de la Fiscalía General de la Nación, y "procesado por los delitos de acceso abusivo a un sistema informático y daño informático."

Otro cibercriminal colombiano de alto perfil, es el bogotano *Mario Simbaqueba Bonilla*, de 40 años al momento de su captura. Esta persona residía en Estados Unidos a comienzos del año 2000, cuando creó un programa que lograba capturar la información de los computadores de algunos centros financieros. De esta forma logró obtener los datos de las tarjetas de crédito de más de 600 personas a las que estafó.

Una de sus víctimas trabajaba en El Pentágono[12]. Al ingresar a sus cuentas a través de unos de los computadores infectados, abrió la puerta a este hacker, quien tuvo acceso a los sistemas informáticos del Departamento de Defensa de los Estados Unidos por cerca de 48 horas, hasta

---

[8] La Registraduría Nacional del Estado Civil es una entidad con autonomía administrativa, contractual y presupuestal, organizada de manera desconcentrada, que tiene a su cargo el registro de la vida civil e identificación de los colombianos y la realización de los procesos electorales y los mecanismos de participación ciudadana, con plenas garantías para los colombianos. Su website oficial es el siguiente: https://www.registraduria.gov.co/

[9] El plebiscito sobre los acuerdos de paz de Colombia de 2016 fue el mecanismo de refrendación para aprobar los acuerdos entre el gobierno de Colombia y la guerrilla de las Fuerzas Armadas Revolucionarias de Colombia (FARC). Las votaciones se realizaron el domingo 2 de octubre de 2016. El objetivo de esta consulta era que la ciudadanía expresara su aprobación o rechazo a los acuerdos que se firmaron entre el gobierno y las FARC en La Habana, Cuba. Para que el acuerdo fuese válido, el "Sí" debería contar con, mínimo, el 13% del censo electoral (4.396.626 votos), y superar en número de votos al "No". El "No" se impuso al "Sí" con 6.431.376 votos (el 50,21 %) contra 6.377.482 votos (49,78 %). El detalle de la votación, puede verificarse en este website: https://elecciones.registraduria.gov.co/pre_plebis_2016/99PL/DPLZZZZZZZZZZZZZZZZZ_L1.htm

[10] El siguiente link lleva a una comunidad de twitter homónima que existe desde el 2011, presumiblemente sea el grupo de referencia: https://twitter.com/colhackers?lang=es

[11] El website existe. Puede verse en este enlace: http://www.zone-h.org/ al momento de consultarlo (06SEP2018) tenía 4 administradores y 142.307 usuarios registrados. Señalan también haber adelantado 13.444.346 ataques digitales.

[12] En inglés, The Pentagon, es el edificio sede del Departamento de Defensa de los Estados Unidos. El edificio tiene forma de pentágono, de ahí su nombre, en él trabajan aproximadamente 23.000 empleados militares y civiles, y cerca de 3.000 miembros de personal de apoyo. Se encuentra en el condado de Arlington, Virginia.

que fue detectado y bloqueado. Según relató, siempre según Ávila (2016), tuvo la oportunidad de hurtar 100 millones de dólares del Departamento de Defensa de los Estados Unidos, pero decidió no hacerlo. De todas formas, su ingreso a esa red informática lo puso en la mira de las autoridades de los Estados Unidos.

Simbaqueba, se dedicó por un tiempo a viajar por el mundo, con el dinero obtenido con sus cibercrímenes. Sin embargo, encontrándose en Bogotá fue objeto de una trampa en la que participó una mujer, por medio de la cual se le incitó a viajar a los Estados Unidos. Cuando aterrizó fue capturado inmediatamente y puesto a la orden de la Fiscalía Federal del distrito sur de Florida, misma que le imputó 16 cargos por robo de identidad y dinero, que acarrean condenas de cinco a 15 años de prisión. Simbaqueba aceptó los cargos y cumplió una condena de cerca de 10 años de cárcel.

Un tercer caso que ha sido noticia nacional, es el de Jaime *Alejandro Solano*, ciudadano colombiano oriundo de la ciudad de Neiva y de 26 años al momento de su captura, quien se dedicaba a robar las millas de personajes famosos, reconocidos nacional e internacionalmente, entre los que se encontraban Juanes, Sofía Vergara, Silvestre Dangond, Laura Acuña, Iván Villazón, Carolina Cruz, Luly Bosa, Kathy Sáenz, Silvia Corzo y Claudia Gurisatti.

Su modus operandi comenzaba con la obtención de algunos datos básicos, mismos que obtenía suplantando telefónicamente a empleados de una aerolínea. Para pasar luego a realizar phishing, ciberdelito que consiste en suplantar una página real con una falsa sobre la que se tiene pleno control, en este caso se suplantó el website de LifeMiles. Procedió luego el cibercriminal a enviar correos a sus víctimas solicitando actualización de datos.

De esta forma logró convertir las millas y viajó a destinos nacionales e internacionales. Semana (2018) señala que “entre sus destinos estuvieron África, Asía, Miami, Egipto y México. Además, aprovechaba los fines de semana para ir a los destinos favoritos de los turistas en Colombia como Cartagena, Santa Marta y San Andrés.” (s/p)

Pero como si fuese poco, cuando se capturó a Solano a mediados del año 2015, las autoridades determinaron que por medio de distintas técnicas el cibercriminal también obtenía datos de tarjetas de crédito, con las que pagaba los impuestos de los tiquetes que compraba con las millas hurtadas.

Fue capturado por segunda vez en marzo del 2018, al haber continuado con el ilícito, volviendo a ser noticia.

> *El joven fue apodado como el “rey de las millas” y fue capturado por la Policía Nacional en el aeropuerto El Dorado, justo cuando se preparaba para abordar un vuelo con destino a Cartagena para pasar la Semana Santa. Llevaba una identidad falsa pues contaba con medida domiciliaria privativa de la libertad desde el año 2015, cuando había sido capturado por varios ciberdelitos.*
> *“Estaba con el beneficio de prisión domiciliaria condenado por transferencia no consentida de activos y violación de datos personales”, explicó el director de la Dijín, José Luis Vargas. (Semana, 2018, s/n)*

Otro ciberdelincuente de alto perfil en Colombia, fue un menor de edad natural de Barranquilla, cuyo nickname era 'R4lph_is_here', debido a la reserva de ley para proteger a los menores de edad, no fue posible conocer su nombre real. Sin embargo, por un artículo de El Tiempo (2014) se sabe que su primer nombre es Rafael, que tiene un diploma del SENA en Programación y Sistemas, y que al momento de su captura estaba estudiando dos ingenierías en una universidad de Barranquilla, Industrial y de Sistemas.

Este joven de 17 años al momento de su captura, hacía parte del grupo Colombian Hacker desde los 14 años. De acuerdo a las investigaciones de las autoridades, su prontuario incluía 170 violaciones a la seguridad de páginas gubernamentales, entre 2011 y 2014.

> *Ataques como esos, tipo 'Anonymous', eran el sello de un joven barranquillero que hoy tiene 17 años y que logró, entre julio del 2011 y marzo del 2014, violar la seguridad de 170 páginas electrónicas de entidades del Estado colombiano, incluida la del Ministerio de Defensa. En esas incursiones cambió información, borró archivos, publicó datos reservados y hasta estuvo a punto de tumbar los sitios web de la Registraduría y el Consejo Nacional Electoral en las elecciones de marzo. (El Tiempo, 2014, s/p)*

Su acción más destacada fue el ataque al website de la Procuraduría General de la Nación[13], en la época en que estaba en curso la destitución del Alcalde de Bogotá, Gustavo Petro. 'R4lph_is_here' reemplazó el web oficial por una imagen que decía "Petro no se va".

El menor fue capturado en su casa de Barranquilla, y puesto a disposición de las autoridades pertinentes. Se desconoce cual fue la sanción que recibió.

El caso de Andrés Felipe Sepúlveda

Este es un caso reciente y quizá el más emblemático, en relación con el objeto del presente artículo.

Sepúlveda, capturado el 5 de mayo del 2014, fue protagonista de un escándalo referido a las elecciones presidenciales del 2014 en Colombia. En esa oportunidad disputaban la presidencia del país en segunda vuelta, Juan Manuel Santos y Óscar Iván Zuluaga. Al mismo tiempo se desarrollaba el proceso de paz en La Habana entre el Gobierno Colombiano y el grupo FARC, siendo Santos presidente en ejercicio.

Al allanar la oficina de Sepúlveda, se le decomisaron 8 computadores, varias USB, reportes sobre campañas políticas, listados de desmovilizados de la guerrilla, y documentos de inteligencia sobre el proceso de paz con las FARC, incluyendo archivos de asuntos técnicos de la Mesa de Diálogos, así como fotografías que se enviaron desde y hacia correos de las FARC.

Las autoridades señalaron que con esta información el hacker tenía la misión de sabotear el proceso de paz con las FARC. La polémica se incrementó al determinarse que Sepúlveda se desempeñaba al momento de su captura como contratista en la campaña de Óscar Iván Zuluaga, en calidad de responsable de la seguridad cibernética y manejo de redes sociales. Este personaje habría trabajado en oportunidades anteriores en la campaña de Álvaro Uribe (2005-2006) y de Juan Manuel Santos (2010), en equipo con el también polémico asesor político venezolano J.J. Rendón[14].

> *Sepúlveda, quien completa cuatro años preso y está en la cárcel de Picaleña en Ibagué, terminó por aceptar cargos criminales por cinco delitos, entre ellos espionaje. Intentó buscar los beneficios de la Justicia Especial para la Paz, aspiración que le fue negada por un juez de Bogotá, y podría empezar a pedir su libertad condicional a más tardar en dos años. (El Tiempo, 2018, s/p)*

[13] https://www.procuraduria.gov.co/portal/

[14] Juan José Rendón, venezolano, más conocido como J.J. Rendón, de profesión psicólogo, es un asesor en estrategia política, que ha conseguido cierta notoriedad como opositor al gobierno venezolano, y por haber estado involucrado en distintos escándalos. Ejerce como docente en el Centro Interamericano de Gerencia Política, y es el director de la Asociación Latinoamericana de Consultores Políticos (ALACOP).

Entre los delitos cometidos por Sepúlveda se cuentan acceso abusivo a sistemas informáticos, uso de software malicioso, violación de datos personales, y concierto para delinquir. En un acápite posterior se profundiza sobre este caso.

Espionaje por cuenta de organismos de inteligencia del Estado

Laverde (2014) en un artículo para El Tiempo, se refiere al tema del espionaje a los negociadores de paz en La Habana, y a otros funcionarios del gobierno de Juan Manuel Santos. Concretamente señala:

> *Todas las agencias de inteligencia del país se han visto salpicadas en su momento por episodios similares que siempre han sido desestimados con una frase que ya hizo carrera en la historia del cinismo: "Se trata de casos aislados". (s/p)*

Ciertamente el espionaje (o la obtención de información de inteligencia) es algo común, e incluso necesario para la seguridad nacional. Todos los países lo practican, aunque no lo reconozcan abiertamente. En algunos casos, investigaciones periodísticas han dejado en evidencia operaciones de espionaje ilegales y contra ciudadanos o autoridades del propio país al que sirve la agencia que viola la ley.

Un ejemplo reciente de ello, tiene que ver con las revelaciones de Edward Snowden, ex agente de inteligencia, que mostraron que agencias de Inteligencia de los Estados Unidos espiaban a sus propios aliados. Poniendo estas revelaciones en aprietos a Barack Obama, para ese momento presidente de ese país, quien argumentó: *"No se puede tener un 100% de seguridad y un 100% de privacidad. Hay que hacer concesiones y este tipo de concesiones nos ayudan a prevenir ataques terroristas"* (Obama, citado por Laverde, 2004. s/f).

> *Siempre ha existido en los organismos de inteligencia una política para evadir cualquier responsabilidad en caso de ser descubiertos. La investigadora Patrice McSherry encontró un documento de junio de 1948 del Consejo de Seguridad Nacional de Estados Unidos en donde se evidencia la guerra encubierta: "(Se autorizó) un vasto programa clandestino de propaganda, guerra económica, acciones directas preventivas, incluidas acciones de sabotaje, antisabotaje, demolición y medidas de evacuación (a ser realizado de manera tal que) cualquier responsabilidad del gobierno de los Estados Unidos por ellas no sea evidente para personas no autorizadas y que, en caso de ser descubiertas, el gobierno de Estados Unidos pudiese negar en forma plausible toda responsabilidad". (Laverde, 2004, s/f)*

Colombia no es la excepción. Ha habido en el país repetidos escándalos tras descubrirse que organismos de inteligencia -o personal de inteligencia- han actuado por fuera de la ley con el propósito de espiar ilegalmente a ciudadanos colombianos de alto perfil, sirviendo a intereses particulares. Dentro de sus víctimas, tenemos a congresistas, magistrados, defensores de derechos humanos, personajes de la izquierda democrática, entre otros. Debido a una serie de excesos previos, el Congreso de la República de Colombia promulgó en abril del 2013 la llamada *"Ley de Inteligencia"* intentando establecer límites claros a las diferentes agencias de inteligencia, que siempre se movieron en zonas grises de las leyes existentes. Precisamente la Ley Estatutaria 1621 del 17 de abril del 2013, se promovió luego del escándalo de espionaje que tuvo como epicentro al Departamento Administrativo de Seguridad (DAS) entre 2003 y 2009.

Este escándalo inició a raíz de una serie de denuncias de la revista colombiana Semana, donde se señalaba que el DAS había "chuzado", perseguido y actuado persistentemente para desacreditar a defensores de derechos humanos, sindicalistas, periodistas, y miembros de

Organizaciones No Gubernamentales (ONGs). Como si fuese poco, el organismo de inteligencia del Estado, habría infiltrado la Corte Suprema de Justicia (CSJ) para espiar y monitorear a los magistrados de ese organismo a los que se consideraba "enemigos del ejecutivo". Todo esto dentro del llamado "*Plan Escalera*". En este contexto se grabaron sesiones reservadas de la CSJ, se fotocopiaron o extrajeron expedientes referidos al escándalo de la llamada "*parapolítica*"[15], referidos a sujetos que terminaron presos y eran aliados del gobierno del Presidente Álvaro Uribe Vélez. Laverde (2014) nos dice al respecto:

> *Como consecuencia de las investigaciones de la Fiscalía se supo que el exdirector del DAS Jorge Noguera, el exsubdirector José Miguel Narváez y otros altos funcionarios crearon una célula clandestina de espionaje denominada G-3 que operó entre marzo de 2003 y noviembre de 2005, con 15 detectives que hacían parte de su estructura y que funcionaban en el piso octavo y décimo del DAS. Se descubrió que tenían operaciones para enlodar a ONGs, como la llamada Operación Transmilenio contra el colectivo de abogados José Alvear; que se impulsó un desprestigio en contra de la Corte Interamericana de Derechos Humanos; que se espió a la premio Nobel de Paz iraní Shirin Ebadi en 2004 durante su visita a Colombia y que, incluso, se llegó al despropósito de crear un manual para amenazar que fue elaborado para intimidar a la periodista Claudia Julieta Duque, quien documentó que en el asesinato del humorista Jaime Garzón[16] en 1999, el DAS desvió el expediente para que quedara en la impunidad. (s/p)*

Si todo lo reseñado hasta aquí es cierto, podría resultar escalofriante para algunas personas, y sería sin duda un abuso de los recursos del Estado para perseguir enemigos políticos y favorecer la propia postura de quienes detentaban el poder. Y sin embargo esto no es todo, Laverde (2014) profundiza aún más:

> *Toda la persecución del DAS fue documentada y se constató que los "blancos políticos" eran opositores al gobierno de Álvaro Uribe; que incluso se siguieron (sic) a magistrados de la Corte Constitucional en el año 2005 cuando ese alto tribunal discutía la constitucionalidad del acto legislativo que aprobó la reelección; que se espió a la Corte Suprema cuando ésta indagaba en 2008 el escándalo de la 'yidispolítica' denunciado por la congresista Yidis Medina. Según ella, el gobierno Uribe le ofreció prebendas burocráticas a cambio de su voto positivo por la enmienda constitucional. El DAS la siguió a ella y a los magistrados. De hecho, la detective Alba Luz Florez, más conocida como la 'Mata Hari', enamoró a un capitán de la Policía con el que había salido, Julián Leonardo Laverde, quien oficiaba como jefe de seguridad del Congreso, para que le ayudara a reclutar fuentes al interior de la Corte. Fue así como contactó al escolta del magistrado Iván Velásquez, David*

[15] Tal es el nombre con el que se conoce en Colombia al escándalo político desatado a partir de 2006 por la revelación de los vínculos de algunos políticos con los grupos paramilitares, con posterioridad al proceso de desmovilización de las denominadas Autodefensas Unidas de Colombia. En Colombia se llama "paramilitares", "paras" o "paracos" a los grupos armados ilegales de extrema derecha que se autodenominan como autodefensas y que están generalmente ligados al narcotráfico.
Para el año 2013 habían sido condenados 60 congresistas por sus vínculos con grupos armados ilegales dentro de este proceso. Igualmente habían sido condenados numerosos funcionarios del Estado así como alcaldes y gobernadores de diferentes regiones del país

[16] Jaime Hernando Garzón Forero (Bogotá, 24 de octubre de 1960 - 13 de agosto de 1999) fue un abogado, pedagogo, periodista, mediador de paz colombiano, activista, locutor, actor y humorista colombiano. El 13 de agosto de 1999 fue asesinado en Bogotá por dos sicarios cerca de los estudios de la emisora Radionet donde trabajaba. En diferentes ocasiones, Garzón había expresado que era víctima de amenazas de muerte.

García, y a los oficiales Manuel Pinzón y Franklin Grijalba; este último jefe de seguridad de todos los magistrados de la Corte.

Alba Luz Flórez, a quien se denominó la "Mata Hari"[17] por sus actividades de espionaje, relató en sus declaraciones, haber establecido una red de contactos en la CSJ que incluía a operarias de servicios generales, encargadas entre otras cosas de servir las bebidas en las salas donde sesionaba la Corte, y allí colocaban oportunamente y de manera ilegal pequeñas grabadoras para lograr conocer lo que allí decían los 23 magistrados en sus reuniones reservadas. El principal argumento de Flórez para intentar convencer a los oficiales de policía de unirse a su red, era que la Corte estaba actuando como enemiga del gobierno del Presidente Uribe, y que su lealtad debía ser para el Presidente y no para sus protegidos (en el caso de los escoltas y miembros de esquemas de seguridad).

A raíz de este escándalo, distintos miembros de la plana mayor del DAS terminaron destituidos por la Procuraduría, procesada por la Fiscalía y encarcelada. Entre ellos la exdirectora del DAS María del Pilar Hurtado, el exdirector de inteligencia Fernando Tabares, el exsubdirector de contrainteligencia Jorge Lagos, y la exsubdirectora de operaciones Martha Leal.

Valga anotar que Lagos y Tabares, declararon en su oportunidad que el exsecretario general de la Presidencia de la República Bernardo Moreno se había reunido con ellos y con María del Pilar Hurtado en el *Club Metropolitan* de Bogotá en septiembre de 2007, donde Moreno les dijo concretamente que: "el interés del señor presidente de la República era que el DAS lo mantuviera informado sobre cuatro temas: la Corte Suprema de Justicia, la senadora Piedad Córdoba[18], el senador Gustavo Petro[19] y el periodista Daniel Coronell[20]" (Laverde, 2014, s/p)

Valga anotar que el expresidente Álvaro Uribe ha negado enfáticamente tener responsabilidades en este caso. Por el contrario, ha afirmado que durante su mandato siempre le dio garantías a la oposición política. Sin embargo, subsisten las dudas, al entender que el DAS dependía directamente del Poder Ejecutivo, y si estaban enfocados en esos blancos debía ser por alguna razón de interés del alto gobierno, a quien rendían cuentas sobre sus actuaciones y entregaban la inteligencia que producían.

En el rastreo histórico que hace Laverde (2014) en su artículo, hay más tela para cortar:

Pero este episodio del DAS no fue el único en la larga lista de abusos de los organismos de inteligencia. Hoy se indaga si agentes del DAS participaron en los magnicidios de los candidatos presidenciales Luis Carlos Galán (18 de agosto de 1989), Bernardo Jaramillo Ossa (22 de marzo de 1990) y Carlos Pizarro (26 de abril de 1990). Años después, durante el gobierno del presidente Samper, estalló el escándalo 8.000 por la narcofinanciación del cartel de Cali a esa campaña. Muchos conocedores sostienen que las agencias del Estado

[17] Nombre con el que fue conocida la famosa espía holandesa Margaretha Geertruida Zelle, durante la Primera Guerra Mundial.

[18] Piedad Esneda Córdoba Ruíz (Medellín, 25 de enero de 1955), es una abogada y política colombiana de izquierda, frecuentemente señalada de tener estrechos vínculos con grupos armados ilegales como las FARC. Fue senadora de 1994 al 2010. Presentó su candidatura a las elecciones presidenciales del 2018, pero se retiró el 9 de abril argumentando que no había condiciones de igualdad entre los candidatos.

[19] Gustavo Francisco Petro Urrego (Ciénaga de Oro, Córdoba, 19 de abril de 1960) es un economista y político colombiano. Fue alcalde de Bogotá y senador de la República. Candidato para la presidencia de Colombia en 2010 y 2018.

[20] Daniel Alfonso Coronell Castañeda (Bogotá, 25 de octubre de 1964) es un periodista colombiano. Ejerce como vicepresidente y director de noticias de Univisión, la cadena hispana de televisión en Estados Unidos. Es columnista de la revista Semana de Colombia, donde frecuentemente escribe polémicos artículos de opinión. Ha sido un crítico acérrimo de Ávaro Uribe Vélez.

> *se encargaron de espiar a los opositores del jefe de Estado. Durante la administración Pastrana también se denunció que un exdetective de inteligencia del DAS señaló que desde ese organismo se chuzaron a periodistas del noticiero Hora Cero, a dirigentes como Horacio Serpa, al vicefiscal Jaime Córdoba y a otros funcionarios. Este caso se fue desvaneciendo con los años y poco se supo del llamado expediente del 'Chuzo-gate'. (s/p)*

En el año 2007, siendo presidente Álvaro Uribe, se generó otro escándalo por denuncias de la revista Semana. Esta vez se supo que la Dirección de Inteligencia de la Policía Nacional "chuzó" de manera ilegal a opositores del gobierno. La divulgación del caso tuvo distintas consecuencias, la más notoria fue un "remezón" de la cúpula de la Policía Nacional en el que 12 Generales salieron de la institución. Fue allí donde el General Óscar Naranjo fue llamado nuevamente al servicio activo y nombrado Director de la Policía (inició el 17 de mayo de 2007, y fue relevado el 12 de junio de 2012). No se volvió a dar relevancia a este caso en los medios de comunicación.

Si bien el Departamento Administrativo de Seguridad (DAS), fue disuelto en el 2011, y se promulgó la Ley de Inteligencia en el 2013, los escándalos referidos a espionaje ilegal no pararon.

> *(…) se descubrió que, con órdenes falsas, el magistrado Iván Velásquez fue chuzado por la Policía y hace un año el escritor Gustavo Álvarez y el periodista Hernán Peláez, director de La Luciérnaga de Caracol Radio, denunciaron haber sido interceptados por funcionarios de la Agencia de Inteligencia, que reemplazó al DAS. Pero, quién dio las órdenes, se pregunta con insistencia después de cada escándalo. Nadie da razón. (Laverde, 2014, s/p).*

Valga anotar que el escándalo por las "chuzadas" ilegales a los negociadores de La Habana, con el involucramiento del hacker Andrés Sepúlveda, se destapó en el 2014. La agencia que reemplazó al DAS es la Dirección Nacional de Inteligencia (ANI).

El Caso Andrómeda

Andrés Sepúlveda fue uno de los principales protagonistas del llamado Caso Andrómeda. En el 2014 la revista Semana reveló que en un local comercial de Bogotá, funcionaba una red de inteligencia que realizaba interceptaciones ilegales a los integrantes de los equipos negociadores dentro del proceso de paz que adelantaba el gobierno nacional con el grupo FARC en La Habana, Cuba. El 23 de enero de 2014 el lugar fue allanado por la Fiscalía. Cuando los medios dieron a conocer la historia, el jefe de Inteligencia del Ejército Nacional, negó rotundamente la existencia de esa central de inteligencia, sin embargo, a las pocas horas fue relevado de su cargo. Con el pasar de los días, más oficiales del Ejército fueron viéndose involucrados en el asunto. El director de la Central de Inteligencia Técnica del Ejército, General Jorge Andrés Zuluaga, también fue relevado de su cargo. Ninguno de los dos fue retirado del Ejército de inmediato, pero si eventualmente. Ambos oficiales aseguraron no haber participado en irregularidades.

En febrero de 2014 el Ministro de Defensa de Colombia anunció la destitución del jefe de Inteligencia del Ejército, General Mauricio Ricardo Zúñiga, y el director de la Central de Inteligencia Técnica del Ejército (Citec), General Jorge Zuluaga. Esto tras conocerse las primeras pruebas de la participación activa de militares colombianos en el espionaje a los negociadores de paz, en el proceso que adelantaba el gobierno de Juan Manuel Santos con el grupo FARC en La Habana.

La sala de interceptación de la operación "Andrómeda", funcionaba bajo la fachada de un hackerspace[21] llamado Buggly, en el barrio Galerías de Bogotá. Este local, que tenía diversas

[21] Un hackerspace (en inglés, espacio de hackers), hackspace, o hacklab (laboratorio hacker), es un sitio físico donde gente con intereses en ciencia, nuevas tecnologías, electrónica o artes digitales, se puede conocer, socializar y colaborar entre sí.

facilidades para atraer a la comunidad hacker de Bogotá, era atendido por el cabo primero de inteligencia Luis Humberto Moreno Montes, quien se hacía llamar por el nickname de "*Bender*", él era la persona visible del proyecto, la cara amable que no ocultaba para nada su verdadero nombre y se hacía fotografiar sin reparos, mientras asistía a eventos de la comunidad hacker. Detrás de él, en una posición más reservada, compartían responsabilidades un cabo segundo, y un mayor del Ejército Nacional. El local cerró el 03FEB2014, y el personal que trabajaba en este lugar en actividades de inteligencia fue trasladado a otras unidades y dependencias. Peñarredonda (2015), señala:

> *El sitio estaba ubicado en una casona del barrio Galerías, un barrio concurrido pero tranquilo de Bogotá. Lo tenía todo: equipos y redes de última tecnología, salones y espacios amplios, videojuegos -desde 'maquinitas' retro hasta consolas de última generación- y un restaurante, como para nunca tener que salir de ahí. (…)*
> *La razón de ser de Buggly era construir una comunidad de seguridad informática. Hacían sesiones de seguridad, compartían información y ponían a un montón de chicos a solucionar retos técnicos sin ninguna malicia, solo para 'compartir el conocimiento'. (…)*
> *La fachada exigía que Buggly se dedicara, especialmente, a atraer miembros a la comunidad de hacking ético y a obtener sus conocimientos. Por eso las fiestas, la generosidad y los brazos abiertos: servían para saber qué habilidades específicas tienen algunos hackers y luego reclutarlos. (s/f)*

Los medios de comunicación realizaron denuncias públicas de lo que fueron descubriendo. En este caso Blu Radio[22] presentó a la opinión pública un dossier que mostraba fotografías de los hacker -que ellos mismos publicaron en Facebook- en donde se apreciaba la presencia de militares uniformados en el lugar. Blue Radio logró recolectar al menos 24 fotografías antes de que los involucrados en el escándalo cancelaran sus cuentas en redes sociales.

En este contexto, la Corte Constitucional de Colombia solicitó formalmente al Gobierno Nacional, al Congreso y al Sector Defensa asumir responsabilidades en este caso, que involucró a un sector del Ejército Nacional en escuchas ilegales contra líderes de izquierda y el equipo negociador del gobierno, en los diálogos con las FARC en La Habana. Entre los escuchados ilegalmente estaban el jefe negociador, Humberto de la Calle; el alto comisionado para la Paz, Sergio Jaramillo; y el director de la Agencia Colombiana para la Reintegración (ACR), Alejandro Eder.

La Corte recordó que como Colombia es un Estado Constitucional de Derecho "las atribuciones de las autoridades públicas deben ceñirse estrictamente a la Constitución y la ley, siendo responsables por omisión o extralimitación en el ejercicio de sus funciones".

El presidente de la Corte Constitucional, Jorge Iván Palacio, dijo en un comunicado que la Procuraduría y la Fiscalía deben iniciar y culminar "pronta y eficazmente las investigaciones en orden a cumplir y vigilar la garantía efectiva de las libertades ciudadanas".

En el año 2015 se creó un *Comité de Alto Nivel*, que estaba conformado por los Inspectores de todas las Fuerzas Militares y también de la Policía Nacional, más el Director de Asuntos Legales del Ministerio de Defensa, para analizar al asunto Andrómeda y proponer cursos de acción al Alto Mando. Como resultado, señala El País (2015):

> *El vicealmirante César Augusto Narváez, inspector General de las Fuerzas Militares, aseguró (…) que en desarrollo de las investigaciones se realizaron 268 pruebas de credibilidad a todo el*

[22] Blu Radio es una cadena de radio colombiana de noticias, propiedad de Caracol Televisión, que pertenece al grupo Valórem. https://www.bluradio.com/

personal de Inteligencia. Producto de este procedimiento, dijo Narváez, fueron relevados 10 oficiales, ocho suboficiales, un patrullero y un funcionario administrativo, además del retiro de cinco militares. También se iniciaron 6 investigaciones disciplinarias, 4 por el caso de Andrés Sepúlveda y 2 por el caso de documentos secretos y la supuesta lista de inteligencia militar, en las que hasta el momento se encuentran vinculados 11 funcionarios de la Fuerza Pública. (s/n)

A su vez, la Fiscalía procedió con la condena de quien fue identificado como el hacker principal en este episodio, Andrés Sepúlveda. Como ya se mencionó, se le imputaron los cargos de concierto para delinquir, acceso abusivo informático, violación de datos personales agravado, espionaje y uso de software malicioso.

Sepúlveda fue capturado en mayo del 2014, cuando hacía parte de la campaña presidencial de Óscar Iván Zuluaga, candidato apoyado por Álvaro Uribe.

Además de Andrés Sepúlveda, otras personas involucradas en el caso Andrómeda también fueron condenadas por similares delitos, pero él se tornó en el caso emblemático. Debido principalmente a su doble situación: por un lado, trabajando con una central de inteligencia que espía el proceso de paz, presuntamente con la intención de sabotearlo, y por el otro su relación con la campaña de Zuluaga, y por tanto con Álvaro Uribe que era su jefe político. Se presume pues que era Uribe quien estaba detrás de todo, intentando perjudicar al gobierno de Santos, a quien acusa de haberle traicionado, siendo él el que lo llevó al poder. No ha podido probarse que Álvaro Uribe fuese quien orquestó todo.

Andrés Sepúlveda fue contratado por Luis Alfonso Hoyos, para trabajar en la campaña de Zuluaga, y por David Zuluaga, hijo del excandidato presidencial. Hoyos fue funcionario del gobierno de Uribe y era asesor en la campaña de Óscar Iván Zuluaga. En agosto de 2015, la Fiscalía General de la República le imputó a Hoyos los cargos de espionaje, concierto para delinquir, cohecho, acceso abusivo a sistemas informáticos, uso de software malicioso y violación de datos personales. Similarmente a lo imputado a Andrés Sepúlveda. Sin embargo, Luis Alfonso Hoyos viajó a Estados Unidos y pidió asilo político. A Óscar Iván Zuluaga se le inició una investigación, asumiéndose que él era responsable por su propia campaña y que algo tendría que ver con el tema de los hackers. Sin embargo, finalmente la Fiscalía archivó la investigación en su contra al establecer que no había pruebas que lo relacionarán con Sepúlveda, o al menos no con sus actividades ilícitas, ya que se reveló un video de una reunión donde aparece reunido con el Hacker. Óscar Iván Zuluaga siempre negó haber solicitado o recibido de manera consciente información ilegalmente obtenida.

> *Según ente investigador, quienes conocieron de primera mano la información que obtenía Sepúlveda de manera ilegal fue Hoyos y, al parecer, también David Zuluaga, quien ahora vive en Estados Unidos. Este último ya ha rendido interrogatorios, pero, oficialmente, no está siendo investigado. La cooperación de Sepúlveda con la justicia permitió otras condenas: de Wilson Torres Wilches, exagente de la DNI; de Luis Humberto Moreno, cabo del Ejército; de Michael Usme Charry, exjefe del grupo antiterrorismo de la Sijín Bogotá; de David Parra Amín, expatrullero de la Sijín; y del hacker ecuatoriano Daniel Bajaña, quien interceptó el correo de Francisco Santos, quien había aspirado a ser el candidato del Centro Democrático. (El Espectador, 2018, s/p)*

El hecho de que Wilson Torres Wilches, estuviese involucrado en este escándalo, siendo para ese entonces agente de la Dirección Nacional de Inteligencia (DNI), es una de las aristas del caso que nunca se aclaró del todo. El Almirante Álvaro Echandía, era el director de la DNI cuando ocurrieron los hechos. Se le abrió investigación, que eventualmente fue archivada en febrero de

2017. Luego, a finales de ese mismo año Echandía fue nombrado como cónsul colombiano en Washington D.C.

Lo más reciente dentro de este caso, es la decisión de la Procuraduría en el 2018 de formular pliego de cargos contra un oficial y dos suboficiales del ejército actualmente retirados. Ellos son: un oficial de grado Mayor, quien comandaba la Operación Andrómeda, y los Cabos de Inteligencia Luis Humberto Moreno Montes y Carlos Alberto Betancur Sánchez. Ninguno de los tres tiene por el momento investigación abierta en Fiscalía. (El Espectador, 2018, s/p). De los tres, el oficial pasó a retiro el 11 de febrero de 2015, Moreno pasó a retiro el 15 de enero del 2015, y Betancur continúa en situación de actividad.

Andrómeda, antecedentes y consecuencias

- Al final del segundo mandato de Álvaro Uribe Vélez, él y sus allegados consideran oportuno continuar la Política de Seguridad Democrática.
- Se propone a Juan Manuel Santos Calderón, Ministro de Defensa del gobierno de Uribe, como el candidato a la presidencia que sucedería a Uribe y continuaría "su legado".
- Efectivamente Juan Manuel Santos Calderón gana las elecciones y se convierte en Presidente de Colombia.
- Eventualmente ocurre un distanciamiento entre Santos y Uribe.
- Juan Manuel Santos promueve un proceso de paz con las FARC, que no es del agrado de Uribe y de sus seguidores más cercanos.
- Uribe acusa a Santos de haberlo traicionado, y haber traicionado sus ideales.
- El Presidente Santos adelanta la primera etapa del proceso de paz con las FARC, en La Habana (Cuba), de manera confidencial. Cuando se determina una agenda viable, entonces hay mayor apertura.
- Las Fuerzas Militares se muestran molestas con el proceso de paz. Lo cual se evidencia por medio de las declaraciones y escritos de los gremios de oficiales y suboficiales en uso de buen retiro, quienes técnicamente son "voceros informales" de los militares activos, los que por ley no pueden manifestarse ni repudiar las acciones de su Comandante en Jefe.
- El expresidente Uribe, constantemente "trina" críticas al proceso de paz, y sobre un supuesto maltrato a las Fuerzas Militares por parte del Gobierno Nacional. Está enterado de acciones, combates, y coordenadas, que solo conoce personal militar activo, lo que hace suponer que algunos militares en servicio activo le filtraban información reservada.
- Terminado su primer mandato, Santos se lanza a la relección, usando como bandera política la continuación y conclusión positiva del proceso de paz en curso con el grupo FARC. Es decir "la paz". Su propaganda incluye videos en los que se pregunta a las madres si ellas prestarían a sus hijos para la guerra. Lo cual resulta ser muy efectivo.
- La oposición, en cabeza de Álvaro Uribe, apoya al candidato Óscar Iván Zuluaga. En este momento histórico la campaña tornó en una dicotomía que proponía a los electores un futuro con paz o con guerra. Ante esto y la suposición lógica de que la gente optaría por la paz, la campaña de Zuluaga adopta un eslogan que reza "paz, sí, pero sin impunidad".
- Esta campaña presidencial giró principalmente en torno al Proceso de Paz de La Habana. En este contexto se presenta el escándalo de Andrómeda.
- Se entiende de lo sucedido que los negociadores del gobierno y del grupo FARC estaban siendo espiados ilegalmente por una agencia que operaba clandestinamente desde Bogotá, y su propósito sería presumiblemente sabotear dicho proceso de paz y torpedear la campaña de Juan Manuel Santos. Ambas cosas de interés para el uribismo.
- Puede suponerse que el Presidente Santos no se espiaría a sí mismo.
- Sepúlveda es clave porque estaba relacionado con la agencia de inteligencia que espiaba los diálogos de paz y al mismo tiempo con la campaña de Óscar Iván Zuluaga.

- Sepúlveda fue contratado por el hijo de Óscar Iván Zuluaga, y por un exfuncionario del gobierno de Uribe, llamado Luis Alfonso Hoyos.
- Sepúlveda fue capturado por las autoridades y se hace pública la "Operación Andrómeda".
- Ahora se sabe que la agencia era operada por militares activos pertenecientes al Ejército de Colombia.
- Además de Sepúlveda, se realizan otras capturas adicionales, incluyendo militares, policías y civiles.
- Se lleva a cabo un proceso penal, y los indiciados son condenados por distintos delitos.
- Juan Manuel Santos gana las elecciones presidenciales de Colombia y accede a un segundo mandato.
- El Gobierno Nacional continúa el proceso de paz con el grupo FARC, entendiéndose que el triunfo en las elecciones es un mandato del pueblo.
- El proceso de paz con las FARC llega a unos acuerdos finales, que son sometidos a un plebiscito, en el que se le pregunta al pueblo colombiano si está de acuerdo con lo pactado.
- La campaña de descredito adelantada por el uribismo ("paz sí, pero sin impunidad") y una guerra sucia mediática de desinformación masiva, lleva a que en el plebiscito gane el "No". Pocos votantes leyeron los acuerdos (expresados en un documento bastante extenso), por lo que se orientaron por los señalamientos de sus líderes políticos, por algunos slogans, y por "memes" de redes sociales.
- A pesar del revés sufrido en el Plebiscito, el Presidente Santos logra ratificar los acuerdos por otros medios.
- Las FARC se concentran, se desarman y se desmovilizan, bajo supervisión internacional. Valga anotar que algunos Frentes de las FARC se declaran en disidencia y no se someten al proceso de paz.
- Juan Manuel Santos gana el Premio Nobel de la Paz, pero en lo interno su popularidad llega a niveles muy bajos.
- En las elecciones presidenciales del 2018, nuevamente Álvaro Uribe propone un candidato que revisará los acuerdos de paz con el grupo FARC. Él es Iván Duque. Los otros candidatos se manifiestan a favor de consolidar el proceso de paz.
- Iván Duque resultó electo en segunda vuelta, teniendo como contendor al economista Gustavo Petro, en representación de la izquierda.
- En el momento presente, existe la posibilidad de que los acuerdos alcanzados con las FARC, se disuelvan, y el país retorne a los niveles de violencia anteriores.

Corrupción en la Inteligencia de las Fuerzas Militares

En abril de 2018 el Ministro de Defensa de Colombia -para ese momento-, Luis Carlos Villegas, informó que los gastos reservados de las Fuerzas Militares empleados para inteligencia y pagos por información de interés, entre 2009 y 2018 sumaron 8.900 millones de pesos (aproximadamente 3,18 millones de dólares), y que parte de esos recursos estaban bajo investigación por su presunto desvío a los bolsillos de los militares encargados de manejar informantes. (El Tiempo, 2018-b, s/p).

El ministro señaló que se había tenido conocimiento de las presuntas irregularidades en diciembre de 2017, y que desde ese momento se abrió una investigación interna, liderada por el General Alberto Mejía, comandante de las Fuerzas Militares. En palabras del Ministro:

> *"Con la inspección de las Fuerzas Militares se realizó la investigación con hallazgos muy serios (…) Se entregó un informe a la Procuraduría y a la Fiscalía, se entregó toda la información sobre los posibles responsables. Esa documentación hace parte de la reserva. Por tratarse de un tema de seguridad nacional" (El Tiempo, 2018-b, s/p).*

En abril del 2018 y tras esos hallazgos, se tomó la decisión de eliminar el Comando Conjunto de Inteligencia y la Regional de Inteligencia, dependencias que estaban adscritas al Comando General de las Fuerzas Militares. Señalándose además que el personal que deba cumplir funciones análogas a aquellos que cometieron el delito de apropiarse de unos dineros que tenían una destinación oficial, serán sometidos a controles de contrainteligencia, y al polígrafo[23]. "Además, Villegas indicó que se va a verificar si usaron los equipos de inteligencia para hacer algún tipo de interceptaciones y cuál era su fin." (El Tiempo, 2018-b, s/p).

La Procuraduría solicitó al Ministerio de Defensa suspender hasta por 30 días el manejo de los gastos reservados del sector inteligencia, lo que fue autorizado por el Ministro de Defensa para facilitar las investigaciones. Además, como producto de la investigación interna, a finales de mayo fue presentado el informe del Inspector de las Fuerzas Militares sobre estos hechos de corrupción al interior de las Fuerzas Militares, mismo que presenta no solo una descripción de los hechos y nombra responsables, sino que también formula conclusiones y recomendaciones al mando, para impedir o dificultar que hechos así vuelvan a repetirse. Varios de los implicados ya reconocieron a la Procuraduría y a la Fiscalía su participación en los hechos delictivos, buscando beneficios en el proceso.

El Ministro de Defensa indicó que los presuntos responsables de estos actos de corrupción, habían sido separados de sus cargos, para facilitar las correspondientes investigaciones, tanto internas como aquellas adelantadas por los entes de control. Como medidas adicionales, se señala que:

> *(…) el presupuesto de gastos reservados será supervisado por la Dirección de Control Interno Sectorial y se extremarán las medidas de control en materia de inteligencia militar y sus gastos, sin perjuicio a la seguridad nacional. (Sánchez, 2018, s/p).*

Podemos observar que en el más alto nivel de la comunidad de inteligencia del país, se estaban presentando actos de corrupción, lo que deja en entredicho la credibilidad y la ética que se supone estos funcionarios deberían manifestar. Habida cuenta de lo relatado antes en relación con las interceptaciones ilegales, es comprensible que el Ministro hubiese declarado también que se indagaba si estos sujetos habrían realizado alguna clase de interceptación ilegal. Al momento de escribir estas líneas, no se habían hecho mayores precisiones sobre el tema.

El Negocio de las "Chuzadas" en Colombia

En agosto de 2018, la Fiscalía General de la Nación desmanteló una red de inteligencia dedicada a realizar interceptaciones ilegales para vender la información a terceros. Este nuevo escándalo podría salpicar a distintos funcionarios del gobierno y a personajes de la vida política nacional. Lo cual ya inició con el llamado a interrogatorio del General Humberto Guatibonza de la Policía Nacional, hoy en retiro.

> *Así lo anunció (…) el fiscal general, Néstor Humberto Martínez, quien detalló que quien fuera comandante de la Policía de Bogotá entre mayo de 2014 y octubre de 2016, no forma parte de la red que fue desmantelada, pero "según las evidencias, formaría parte de las personas que solicitan servicios de estos centros de chuzadas ilegales y eso implicaría un grado de determinación. Para que aclare sus comportamientos fue que se llamó".*

[23] Aparato que registra las respuestas corporales de una persona cuando se la interroga y que permite detectar si miente; consiste en varios instrumentos combinados de forma que registren simultáneamente las fluctuaciones en la presión sanguínea, el pulso y la respiración ante las preguntas que se le formulan.

Estas declaraciones sustentaron el allanamiento de la firma A&G de su propiedad y en la interceptación por parte de la Fiscalía de Cali de las comunicaciones que sostuvo con el coronel (r) Jorge Humberto Salinas Muñoz, uno de los capturados en esta trama, con quien habría hablado del negocio, precios y clientes.

Aparte de Salinas Muñoz, los demás capturados también tuvieron alguna conexión de alto nivel con las Fuerzas Armadas y organismos de Inteligencia. Se trata de Carlos Andrés Pérez Cardona, coronel (r) del Ejército y jefe de seguridad de la Alcaldía de Ipiales (Nariño); Luis Mesías Quiroga Cubillos, mayor (r) del Ejército y María Alicia Pinzón Montenegro, exfuncionaria del Ministerio de Tecnología de la información y Comunicaciones. (Amorocho, 2018, s/p).

Las cuatro personas mencionadas en la cita, fueron enviadas a la cárcel por orden del juez 29 Penal Municipal de Cali. El Fiscal General señaló que entre las personas que compraron información ilegalmente obtenida a esta "empresa" estarían ciudadanos, políticos, empresarios, e incluso agentes del Estado. Todos los implicados serán judicializados. Señalando además que "estas expresiones del delito surgen porque hay una demanda creada" (Amorocho, 2018. s/p).

Al parecer tres Magistrados del Tribunal de Nariño habrían sido víctimas de la escucha ilegal. Frente a este caso, la Fiscalía trata de establecer desde cuándo y por cuanto tiempo se realizaron interceptaciones ilegales contra dichos funcionarios. Además de cuál sería el propósito de la misma.

Esta empresa criminal habría ofrecido sus servicios a las Fuerzas Armadas de Ecuador, mismas que rechazaron el ofrecimiento.

El Ejército Nacional de Colombia expresó en un comunicado a la opinión pública que rechazaba estas conductas que involucran a tres oficiales retirados. Este es el texto de dicho comunicado:

El Comando del Ejército Nacional, con relación a la información difundida por la Fiscalía General de Nación el día sábado 4 de agosto del año en curso, sobre una presunta red de interceptaciones ilegales, se permite informar a la opinión pública que:

1. *Los señores oficiales retirados de la Fuerza, relacionados en la investigación, son el teniente coronel Carlos Andrés Pérez Cardona, retirado el 21 de marzo de 2017; mayor Luis Mesías Quiroga Cubillos retirado el 3 de octubre del 2016 y el teniente coronel Jorge Humberto Salinas Muñoz retirado por voluntad propia en el año 2014.*
2. *Este Comando rechaza de manera categórica todo tipo de conductas y acciones contrarias a lo preceptuado en la Constitución Política y la Ley, por parte de cualquier miembro de la Institución, así tenga condición de retirado como en este caso.*
3. *El Ejército Nacional en cumplimiento de las políticas de transparencia, condena estos hechos y reitera que no tolerará ninguna situación fuera de la ley, donde se encuentre vinculado alguno de sus integrantes, siendo implacable en la materialización de todas las acciones judiciales a las que haya lugar.*
4. *Así mismo, reitera que cualquier irregularidad que sea de su conocimiento será informada oportunamente a las autoridades disciplinarias y penales competentes, y se tomarán las medidas administrativas a que haya lugar, para corregir cualquier situación irregular.*
5. *Al tiempo, el Ejército Nacional suministrará toda la información requerida para apoyar a la Fiscalía General de la Nación en este hecho. (Ejército Nacional, 2018, s/p)*

María Alicia Pinzón Montenegro, exfuncionaria del Ministerio de Tecnología de la Información y las Comunicaciones, era la supuesta hacker contratada para el robo de información. Las cuatro

personas serán investigadas por los delitos de acceso abusivo a un sistema informático agravado, utilización ilícita de redes de comunicaciones agravada, violación de datos personales agravados, concierto para delinquir agravado, uso de software malicioso agravado y daño informático agravado.

Los capturados usaban como fachada a dos empresas de seguridad de la ciudad de Cali (Valle del Cauca). Sin embargo "el centro de operaciones criminales estaba en Ipiales, desde donde se habría acopiado información de inteligencia sobre movimientos, ubicación y operaciones de objetivos militares, políticos y sus familiares, y otras personalidades nacionales e internacionales". (El Espectador, 2018-b, s/p).

El Tiempo (2018), señala que, según las autoridades competentes, algunas de las modalidades delictivas de esta empresa eran:

- Venta de información judicial: La Fiscalía señala que políticos y personas vinculadas a actividades ilegales habrían acudido a la red para conseguir información sobre las investigaciones en su contra.
- Información a agencias de inteligencia: La red buscaba información de personas vinculadas a organizaciones ilegales e intentaba ofrecerla a autoridades en Colombia y en el exterior (Ecuador) que tienen programas de pago por datos que sirvan a sus investigaciones.
- Contrainteligencia empresarial: Los integrantes de la red se ofrecían para hacer seguimiento a la competencia de sus clientes para anticiparse a sus movimientos y reaccionar ante los negocios que estos estuvieran realizando.
- Espionaje interno: Hay documentados casos en los que la organización ofrece a reconocidas empresas la posibilidad de interceptar las comunicaciones de sus trabajadores para establecer si ellos estaban planeando robos dentro de las empresas.
- Parejas celosas: La red chuzaba los teléfonos y correos de las personas por pedido de sus parejas y entregaba, fotografías, chat y grabaciones de sus conversaciones comprometedoras. (s/p)

En la información incautada en los allanamientos, la Fiscalía encontró los datos de los clientes de este grupo y las actividades que contrataron, lo que permitirá judicializarlos por distintos delitos, entre ellos: utilización ilícita de redes de comunicaciones agravada, acceso abusivo a un sistema informático agravado y violación de datos personales agravados. Todo lo cual sería apoyado por el testimonio de la hacker María Alicia Pinzón Montenegro, quien está dispuesta a colaborar con las autoridades en busca de beneficios en su propio proceso, y ya se habría comprometido a dar toda la información sobre sus clientes y sus víctimas.

Violación a la ética, ¿hay que vigilar al vigilante?

Pudiese pensarse que la operación clandestina de vigilancia sobre el proceso de paz, tuvo su génesis al interior del propio Ejército. Institución que por 50 años combatió a las FARC, a un costo altísimo en cuanto a militares muertos, heridos, secuestrados y desaparecidos, y que con el manejo inicial del proceso de paz pudo sentirse relegado y en la oscuridad.

Los generales activos podían no querer el filtro de los oficiales en situación de retiro que fueron nombrados negociadores, sino que quizá preferían conocer exactamente qué era lo que se decía.

El gobierno nacional consciente de este malestar, no solo colocó a oficiales retirados del Ejército y de la Policía en el rol principal de negociadores, sino que también creó el Comando de Transición al interior de las Fuerzas Militares, para adelantar un proceso pedagógico y organizacional, para ir de la guerra a la paz. En este contexto se impone a los militares en actividad el distintivo *"Citación Presidencial a la Victoria Militar"*, y se crea el concepto del *"Héroe Multimisión"*, dando a entender que el proceso de paz significaba una victoria para los militares,

que las FARC se habrían visto obligadas a negociar por estar derrotadas en el campo de batalla, y por otro lado, atenuando el carácter contraguerrillero de las Fuerzas Militares de Colombia, abriendo la mente a nuevas misiones y posibilidades, incluyendo operaciones de mantenimiento de la paz bajo bandera de la ONU.

En fin, existe la posibilidad de que esta operación clandestina de vigilancia, haya sido adelantada de forma autónoma por el Ejército Nacional, con el fin de monitorear la evolución del proceso de paz, y de alguna forma incidir en él. No hay que perder de vista que si el proceso de paz con las FARC fracasaba, las Fuerzas Militares deberían seguir combatiendo a ese grupo armado ilegal, y no querrían hacerlo a partir de una posición de debilidad. Ante esta hipótesis, y aunque se trataría de una actividad de inteligencia ilegal, poco habría que objetar. Sin embargo, a todo esto se suman tres factores que generan dudas sobre la asepsia de la operación:

1. La certeza de que un grupo importante de oficiales y suboficiales en actividad no desean la paz, y habrían querido que el proceso de paz de La Habana fracasara.
2. La certeza de que algunos militares en actividad, con acceso a información reservada, la estaban filtrando a Álvaro Uribe Vélez, declarado opositor del Gobierno Nacional, y no-amigo de Juan Manuel Santos.
3. La cercanía entre la Operación Andrómeda y la campaña de Óscar Iván Zuluaga (el candidato de Uribe). Que hace pensar que el objetivo era sabotear el proceso de paz y a la campaña contraria.

De ahí que el tema sea tan polémico. Además de esto, tenemos los otros casos mencionados en este texto, donde personal militar, policial, o de organismos de inteligencia como el DAS o su sucesor el DNI, han faltado a su deber e incurrido en delitos asociados al mal uso de las habilidades y destrezas para la vigilancia, física o electrónica, que desarrollaron en función de sus cargos.

El gobierno de la República de Colombia tiene determinadas características que a los efectos de este análisis, se destacan a continuación:

- Democráticamente electo.
- Goza de plena legitimidad.
- Tiene respaldo internacional.
- Se maneja en el marco de la institucionalidad.
- Administra el presupuesto de la nación.
- Hay división/equilibrio de poderes.
- Hay participación ciudadana y control social a la gestión pública (veeduría).
- Es responsable por la seguridad y defensa del país.
- El Presidente de la República es el Comandante en Jefe de las Fuerzas Militares.
- Las Fuerzas Militares están subordinadas al poder civil.

La vigilancia (espionaje) es un procedimiento normal en todos los países, para el que hay personal especializado y equipos de última tecnología. El desarrollo de un procedimiento de vigilancia sobre un ciudadano, se aplica solo en el marco de investigaciones conocidas y aprobadas por las autoridades judiciales correspondientes, así como por el mando superior (para el caso de que la agencia que realiza la vigilancia pertenezca a las Fuerzas Militares o de Policía). Una operación de vigilancia implica varios asuntos a tener en cuenta:

- Se viola la privacidad del ciudadano objeto de la vigilancia (por eso se necesita autorización judicial).
- Se persigue recolectar pruebas en su contra y de presuntos cómplices.
- Hay una persona o grupo que recolecta la información (función operativa).
- Hay una persona o grupo que recibe la información recopilada y la analiza y la contrasta, produciendo inteligencia.

- Hay una institución que recibe la información de inteligencia, y que tiene como fin respaldar procesos judiciales.
- En el operativo participan funcionarios del Estado y/o contratistas.
- Se usan materiales y equipos del Estado (bienes públicos).
- Hay un supervisor que controla el buen uso de los dineros públicos, los equipos, y que direcciona a los funcionarios involucrados.
- En caso de que en el curso de una vigilancia legalmente justificada, se encontrasen pruebas o indicios de que el ciudadano objeto de la misma, o sus relacionados, están incursos en otros delitos, se informa a la autoridad correspondiente (Fiscalía, Procuraduría, o Contraloría) para que inicie la investigación a que haya lugar.
- Se recoge información personal sobre el ciudadano objeto de la vigilancia, que podría ir más allá del propósito que dio origen al operativo. Información que, sin constituir delito, podría ponerle en situación de vulnerabilidad en caso de que dicha información fuese hecha pública. Por ejemplo, infidelidades, pertenecer de manera oculta a la población LGTB, poseer costumbres sexuales poco ortodoxas, tener hijos por fuera del matrimonio, poseer propiedades que su pareja desconoce, entre otras posibilidades.
- Cabe preguntarse ¿cómo se garantiza la reserva en el curso de un operativo de vigilancia?, no solo del operativo mismo, sino también cómo se protege la información recolectada.

A propósito de este último punto, es donde surge la posibilidad de un mal uso del conocimiento, el personal, la información y los recursos públicos. Por ejemplo:

- En el operativo de vigilancia participa el agente X, quien cumple con todas las funciones asignadas, pero…
- Guarda copia de los archivos que se generan en el curso del operativo. Procediendo luego a entregarlos total o parcialmente a terceros, fuera de su agencia.
- La filtración puede tener este carácter:
    - Los filtra a los medios.
    - Los comparte con otras personas u organizaciones.
    - Los vende a personas u organizaciones nacionales.
    - Los vende a personas u organizaciones extranjeras.
- La motivación del agente X, podría ser:
    - Entrega la información por dinero.
    - La entrega por afinidad ideológica con el receptor.
    - La entrega para dañar la imagen de una persona o proceso, con quienes ideológicamente no comulga.
    - Es un doble agente.
    - Está siendo coaccionado por terceras personas u organizaciones.
    - Es una persona emocionalmente inestable o demente.
- Conoce sobre un delito y pide dinero a cambio de ocultarlo.
- Otra posibilidad es que el agente X proceda a extorsionar a la persona u organización que antes fue objeto de la vigilancia, amenazándole con revelar información confidencial que aunque no constituya delito, afectaría gravemente su imagen y relaciones.
- O puede directamente el agento corrupto, irrumpir en las cuentas bancarias de su víctima y robar su dinero, o sus propiedades de valor, previamente identificadas en el operativo de vigilancia.

Por otro lado están las operaciones clandestinas, que se realizan por cuenta y riesgo de determinadas agencias, sin autorización de autoridades judiciales y posiblemente sin conocimiento

del mando. Evidentemente este tipo de operaciones de inteligencia son las más peligrosas por cuanto carecen de mando y control, y no están subordinadas al cumplimiento de la normativa. También son operaciones de inteligencia clandestinas, las realizadas por personas u organizaciones a título privado, sobre otras personas u organizaciones de interés.
Parece evidente que sí hay que vigilar al vigilante. En un trágico círculo vicioso, surgen de inmediato dudas sobre quién debe ser el vigilante del vigilante…

Conclusiones

El ciberespacio ha creado un sinnúmero de posibilidades para la interacción entre personas y organizaciones, facilitando las comunicaciones y el comercio. Al mismo tiempo, se ha convertido en terreno fértil para el crimen, en sus más diversas modalidades. Además, a través de estos ambientes virtuales se pueden adelantar acciones terroristas, o poner en riesgo la economía de un país o su soberanía nacional.

Semejante abanico de amenazas hace necesario que las personas y las organizaciones tomen precauciones, y desarrollen *Sistemas de Gestión de Seguridad de la Información*, que contribuyan a minimizar el riesgo que corren sus activos de información. Pero al mismo tiempo, las autoridades policiales, militares y de inteligencia, deben prepararse para apoyar a su gobierno y a sus ciudadanos en el propósito de combatir el cibercrimen, el ciberterrorismo, y toda clase de ciberamenazas.

La población debe confiar en sus autoridades, por ello los servicios de inteligencia no deben cometer ninguna clase de ilícitos, como los descritos en este artículo. Los escándalos que aquí se han reseñado, y que han sido ampliamente explotados por la prensa amarillista, y por políticos oportunistas, bajan su nivel de credibilidad, y hacen que los ciudadanos se sientan (y en algunos casos estén) en estado de indefensión.

En general, los ciudadanos y las organizaciones deben tener en cuenta que ahora no solo deben cuidarse de los cibercriminales, ciberterroristas, y ciberguerreros enemigos, sino que existe la posibilidad de que también deban cuidarse de los cuerpos de seguridad del estado que normalmente habrían tenido el deber de protegerles. Semejante escenario obliga a tomar medidas efectivas, racionales, técnica y económicamente viables, que permitan asegurar sus activos de información, así como la información personal y privada que podría poner a la persona (o a las organizaciones) en condición de vulnerabilidad.

Si este artículo contribuye a crear conciencia sobre la necesidad de desarrollar apropiados *Sistemas de Gestión de la Seguridad de la Información*, habrá entonces cumplido su cometido.

Referencias

Ávila, C. (2016). La historia detrás de cinco 'hackers' colombianos y sus delitos. En El Tiempo. Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

Amorocho, J. (2018). El negocio de “chuzadas”, un nuevo escándalo que amenaza con crecer. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: http://www.elcolombiano.com/colombia/el-negocio-de-chuzadas-un-nuevo-escandalo-que-amenaza-con-crecer-YB9120504

Cáceres, J. (2017). Colombia, estrategia nacional en ciberseguridad y ciberdefensa. En *Air and Space Power Journal* p.85-89.

Consejo Nacional de Política Económica y Social (2016). Política Nacional de Seguridad Digital (Conpes 3854). Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

ColCERT (2018). Misión y Funciones del Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: http://www.colcert.gov.co

Colombia Estéreo. Colombia está a la vanguardia en la región en materia de ciberseguridad y el ministerio de la Defensa es garante de la soberanía digital. Recurso en línea. Consultado el 05ABR2016. Disponible en: https://www.emisoraejercito.mil.co/index.php?idcategoria=420653

Icontec (2006). Sistema de Gestión de la Seguridad de la Información (NTC-ISO/IEC-27.001). Icontec. Colombia.

International Telecommunications Union (2014). Cyberwellness Profile Colombia. Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Colombia.pdf

International Telecommunications Union (2017). Índice Mundial de Seguridad Cibernética. Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

ITU (2017). Índice Mundial de Seguridad Cibernética. International Telecommunication Union (United Nations). Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Ejército Nacional de Colombia (2018). Comunicado a la Opinión Pública. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.ejercito.mil.co/?idcategoria=440655&utm_source=dlvr.it&utm_medium=facebook

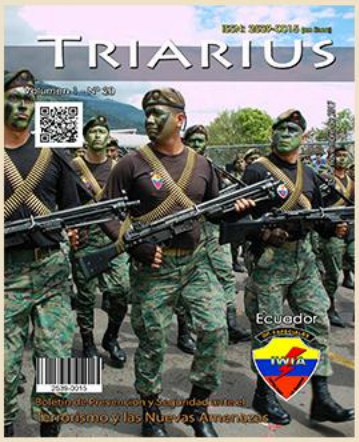
El Espectador (2018). Caso Andrómeda y sus interrogantes. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en https://www.elespectador.com/noticias/judicial/caso-andromeda-y-sus-interrogantes-articulo-731765

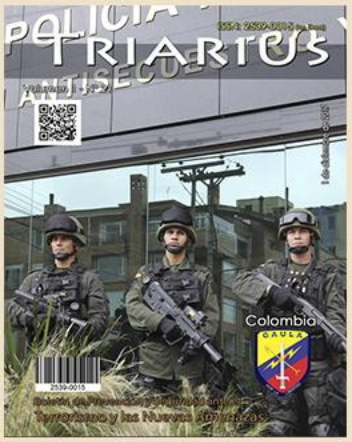
El Espectador (2018-b). Ejército contribuirá en investigación de red de “chuzadas” ilegales. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.elespectador.com/noticias/judicial/ejercito-contribuira-en-investigacion-de-red-de-chuzadas-ilegales-articulo-804517

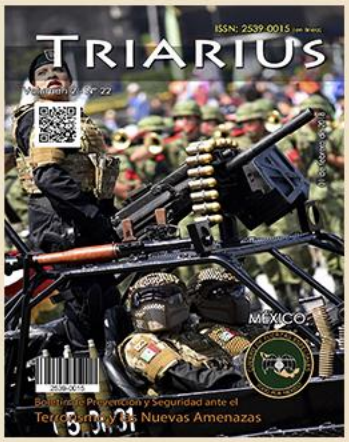
El Tiempo (2014). 'Hacker' que atacó 170 páginas web oficiales tiene 17 años. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-14603471

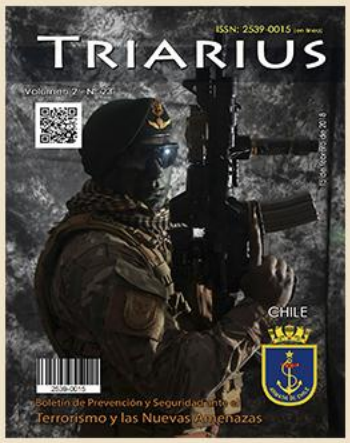
El Tiempo (2018). ¿Quiénes eran los clientes de la red de chuzadas ilegales? Recurso en línea, consultado el 20 de agosto de 2018. Disponible en:

https://www.eltiempo.com/justicia/investigacion/quienes-eran-los-clientes-de-la-red-de-chuzadas-ilegales-252430
El Tiempo (2018-b). Por caso de corrupción se acaba comando de inteligencia de FF.MM. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.eltiempo.com/justicia/investigacion/por-caso-de-corrupcion-se-acaba-comando-de-inteligencia-de-ff-mm-206578
El Tiempo (2018-c). La verdad judicial a 4 años del escándalo del 'hacker' Sepúlveda. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.eltiempo.com/justicia/delitos/hacker-andres-sepulveda-proceso-cuatro-anos-despues-219446
El País (2015). 20 uniformados relevados y cinco destituidos por caso 'Andrómeda'. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.elpais.com.co/colombia/20-uniformados-relevados-y-cinco-destituidos-por-caso-andromeda.html
Laverde, J. (2014). Colombia, un país de 'chuzadas' y espionaje. En El Tiempo. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en https://www.elespectador.com/noticias/judicial/colombia-un-pais-de-chuzadas-y-espionaje-articulo-472794
Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. En *Pensamiento Americano*, p. 71-82
MINTIC (2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME*. Recurso en línea. Consultado el 17ABR2018. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf
Ospina, S. (2017). Colombia ocupó el puesto 46 del estudio global de ciberseguridad. Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: http://www.enter.co/especiales/colombia-conectada/colombia-puesto-46-ciberseguridad/
Peñarredonda, J. (2015). Detrás de Buggly: La historia de la fachada Andrómeda. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: http://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/
Sánchez, O. (2018). Por corrupción, suprimen dos comandos de inteligencia militar. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: http://www.elcolombiano.com/colombia/reformas-en-el-ejercito-por-corrupcion-XF8564437
Semana (2017). El cibercrimen en 2017: la amenaza crece sobre Colombia. Recurso en línea, consultado el 17 de agosto de 2018. Disponible en: https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979
Semana (2018). El 'rey millas' que le dio la vuelta al mundo a cuenta de Sofía Vergara, Juanes y otros famosos. Recurso en línea, consultado el 20 de agosto de 2018. Disponible en: https://www.semana.com/tecnologia/articulo/jaime-alejandro-solano-moreno-el-rey-millas-que-viajo-por-cuenta-de-sofia-vergara-juanes-y-otros-famosos/561833









ISSN: 2539-0015 (en línea)

TRIARIUS

Boletín de Prevención y Seguridad ante el Terrorismo y las Nuevas Amenazas

¡Suscríbete!

...y recíbelo en tu e-mail cada 15 días, de manera gratuita.