ESCUELA DE POSTGRADOS
FUERZA AÉREA COLOMBIANA

IV CONGRESO INTERNACIONAL DE SEGURIDAD INTEGRAL

FECHA: 06 OCTUBRE 2021

ORGANIZA:

MAESTRÍA EN DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL

COLADCA INTERNACIONAL

E-ISSN 2590-602X

Periodicidad anual

Sitio web

https://www.epfac.edu.co/memorias-0

Mayores informes

Carrera. 11 No. 102-50 Edificio ESDEGUE, Escuadrón de Investigaciones. Oficina 411. Bogotá D.C., Colombia. A.A.110111

Teléfonos: (057-1) 637 8927 – 6206518 Ext. 1700, 1719, 1722.

Correo electrónico: cienciaypoderaereo@gmail.com

Escuela de Postgrados de la Fuerza Aérea Colombiana

Director General
Coronel. Ervin Gaitán Serrano

Subdirector General
Teniente Coronel. Ciro Alberto Duarte Jaimes

Comandante Grupo Académico
Teniente Coronel. Andrés Felipe Maya

Jefe de Programa Maestría en Dirección y Gestión de la Seguridad Integral
Capitán Robinson Augusto Morales Carvajal

Coordinador Programa Maestría en Dirección y Gestión de la Seguridad Integral
Subteniente Javier Bustamante Parra

Memorias IV Congreso Internacional de la Seguridad Integral

Compiladores
Capitán Robinson Augusto Morales Carvajal
David Enrique López Cortés
Oscar Iván Parra Camacho

Diseño de piezas publicitarias
Escuela de Postgrados de la Fuerza Aérea Colombiana

Comité Científico
Capitán Robinson Augusto Morales Carvajal
Subteniente Javier Bustamante Parra
Aristides Baldomero Contreras Fernández
David Enrique López Cortés
Giovanna Estefanía Ramírez

Ponentes
Gastón Schulmeister
Gabriel Jiménez Almeira
Camilo Arzuza Bonett
Ariel Pedrozo
Andrea Ramírez

Información técnica
Fecha del Congreso:
Octubre 6 del 2021
Bogotá, D.C.
Colombia (Suramérica)

E-ISSN 2590-602X

Tabla de contenido

IV Congreso Internacional de la Seguridad Integral 5

Introducción 6

Palabras de Apertura 7

El impacto de la delincuencia organizada trasnacional a la seguridad de las Américas 9

¿Es ético el hacking? 14

Implementación de sistema de cifrado ELGAMAL en sistemas embebidos con Linux 17

Impulsores y barreras en la adopción del Operador Económico Autorizado por la seguridad de la cadena de suministros internacionales de empresas colombianas 26

Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance delictivo del cibercrimen en Colombia y la región. 33

Conclusión 37

ESCUELA DE POSTGRADOS
FUERZA AÉREA COLOMBIANA

IV Congreso Internacional de la Seguridad Integral

Fecha:
6 de octubre de 2021

Lugar:
Auditorio del Edificio 'CT Edmundo José Sandoval' y Transmisión por canal oficial de YouTube de la Escuela de Postgrados de la Fuerza Aérea Colombiana

Contexto:

El IV Congreso Internacional de la Seguridad Integral tiene lugar como apertura a la semana de la educación de la Escuela de Posgrados de la Fuerza Aérea Colombiana, llevada a cabo entre el 6 y 8 de octubre de 2021. Este evento se elaboró juntamente con la Comunidad Internacional en Gestión de Riesgos y Seguridad -COLADCA, con quien la EPFAC tiene convenio activo.

Objetivos:

- Establecer diálogos y vínculos con profesionales de la seguridad integral en Colombia, América Latina y Europa para incrementar las redes académicas de la EPFAC y de COLADCA.

- Compartir experiencias gubernamentales y empresariales sobre la gestión de los riesgos, la ciberseguridad y la ciberdefensa para fortalecer los sistemas de protección de la información y garantizar la continuidad del negocio.

- Argumentar y debatir la importancia de pensar la seguridad integral en los ámbitos públicos, privados y académicos, y dar a conocer al público los avances en investigación y las disertaciones actuales sobre la seguridad informática y el crimen trasnacional.

Introducción

El IV Congreso Internacional de la Seguridad Integral es un evento académico planeado entre la Maestría en Dirección y Gestión de la Seguridad Integral de la Escuela de Postgrados de la Fuerza Aérea Colombiana en conjunto con la Comunidad Internacional en Gestión de Riesgos y Seguridad, teniendo como directriz los avances en la seguridad digital. Este evento es el resultado de un convenio interinstitucional es cual favorece la construcción de la línea de investigación de la maestría en Ciberseguridad y Ciberdefensa, y las discusiones con la academia nacional e internacional de la seguridad integral.

Dentro de las ponencias presentadas se encuentra una variedad temática que permite el debate amplio entre la Fuerza Pública, la academia y el sector privado. Siguiendo las necesidades y las coyunturas de la globalización, la expansión masiva de las tecnologías de la información y de la comunicación hacen necesario el refuerzo de la vigilancia y de la defensa de las actividades civiles y gubernamentales en el ciberespacio. El cambio en los medios de interacción social pone de manifiesto que los gobiernos requieren de nuevas estructuras y alianzas para operar dentro del marco legal vigente. Este ejercicio académico será de utilidad para los practicantes de la seguridad integral en todos sus niveles de formación y posiciones dentro de las organizaciones.

En primer lugar, el director del Departamento contra la Delincuencia Organizada Transnacional de la Organización de los Estados Americanos Gastón Schulmeister realizó una exposición sobre el impacto de la delincuencia organizada transnacional en el continente americano, en la que se recuenta el cambio en las dinámicas del crimen transnacional y los esfuerzos interestatales para hacerle frente. En segundo lugar, el ingeniero Ariel Pedrozo pone en cuestión lo ético en la actividad del hacker: si al entrar en un equipo ajeno para estudiar las vulnerabilidades del sistema de seguridad y optimizar la defensa de la información se puede considerar como un accionar ético o se debe respetar la privacidad de los usuarios ante todo.

En tercer lugar, ingeniero Camilo Arzuza expone cómo se puede implementar un método de cifrado efectivo dentro del sistema operativo Linux. En cuarto lugar, la investigadora Andrea Ramírez explora el impacto de la afiliación de las empresas al Operador Económico Autorizado en la seguridad de las cadenas de suministro internacionales. En quinto lugar, el investigador Gabriel Jiménez estudia comparativamente los métodos de seguridad y defensa de diferentes gobiernos de la región latinoamericana correspondientes al ciberespacio.

Palabras de Apertura

CR. Ervin Gaitán Serrano

Director de la Escuela de Postgrados de la Fuerza Aérea Colombiana

La semana de la educación evoca la integración de capacidades, y conmemora también la diversidad conceptual en torno a una sola intención: La avidez del conocimiento, que para esta especial ocasión nos reúne en temáticas de actualidad a discutirse, en el marco del IV congreso de seguridad integral, denominado: Geopolítica de la seguridad integral, la gestión del riesgo y el papel vital de la ciber seguridad. El segundo simposio de estudios militares aeronáuticos, con su enfoque en las amenazas hibridas y los retos de la fuerza aérea en los fenómenos del siglo XXI. El cuarto seminario internacional de seguridad operacional, con su énfasis en la seguridad operacional en la instrucción de vuelo. Y el conversatorio de egresados, respaldando, además, el fortalecimiento de las capacidades de la fuerza como líder en el ámbito aéreo espacial y ciber espacial, en la propuesta de los satélites y la ciencia aeroespacial.

Este programa de enfoque multidominio, nos sumerge en las nuevas realidades para propiciar una mayor capacidad de entendimiento y crecimiento en el seno de nuestras academias, buscando un nuevo resultado de reconocimiento, también, de las nuevas complejidades del mundo, en el inagotable ambiente aeronáutico y en la seguridad como eje trasversal, en el cada vez más complejo mundo ciber y la proyección ambiciosa hacia el espacio. La oportunidad que nos brinda ese escenario de reflexión y de aprendizaje se alimenta desde las diferentes perspectivas y nacionalidades, ofrecidas por el reconocimiento y las experiencias operacionales de nuestros participantes, a ellos extiendo mis más sinceros agradecimientos por acompañarnos en este noble propósito de multiplicación del conocimiento para el sector aeronáutico de seguridad espacial de la región. Debo reconocerlo con más énfasis, teniendo en cuenta la compleja situación que no sólo la pandemia sino sus efectos a representado para generar cambios y desarrollar nuevas capacidades de adaptación, resiliencia y determinación para enfrentar nuevos desafíos. Con esta interacción académica, pretendemos además facilitar diálogos de la comunidad militar nacional e internacional, fomentar los vínculos para fortalecer la investigación y la innovación, promover procesos operacionales, incentivando a su vez una actitud crítica frente a los problemas de seguridad y defensa de nuestra región, así como las diversas formas de abordarlos para la construcción de su solución.

Es ampliamente conocido que la calidad de las instituciones se asocia ineludiblemente a la formación del recurso humano en el fortalecimiento del quehacer, la innovación y la investigación para producir conocimiento valido, sostenible y socialmente pertinente. Esta semana de la educación es para oportunidad para reafirmar los lazos y resaltar el invaluable apoyo de instituciones como: COLADCA, la Inspección General de la Fuerza Aérea Colombiana y el Comando de Apoyo de la Fuerza. Así juntos por una visión compartida desde la academia apuntamos al desarrollo integral de nuestra nación y nuestra región. Este evento es el escenario propicio para reconocer con orgullo la disciplina y el trabajo de todos los docentes, alumnos e

investigadores; quienes han engrandecido con su ardua labor las mentes, los corazones de quienes han pasado por esta escuela. Tengo la certeza de que estos días servirán para reflexionar colectivamente y renovar el compromiso para continuar profundizando en el estudio de fenómenos sociales, políticos, económicos y militares actuales a través de las diferentes disciplinas y profesiones siempre con el interés de crecer en comunidad, trabajar y cooperar conjunta e institucionalmente. Los invito finalmente a ser parte activa de todas y cada una de las actividades programadas para que juntos sigamos fortaleciendo los lazos y las capacidades del sector aeronáutico, espacial y ciber espacial que nos convoca en nuestra semana de la educación.

El impacto de la delincuencia organizada trasnacional a la seguridad de las Américas

The impact of transnational organized crime on the Americas' security

Gastón Schulmeister[1]

La presentación tiene como objetivo reflexionar acerca de los desafíos y retos ante el crimen organizado en las Américas, y compartir la agenda de actividades y acciones que desde el Departamento contra la Delincuencia Organizada Transnacional (DDOT), de la Organización de Estado Americanos (OEA), se realizan para su combate.

El concepto de Delincuencia Organizada Trasnacional hace honor al aplicado desde la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional —conocida también como Convención de Palermo (2000)—, a partir del cual nuestro Departamento aúna esfuerzos a nivel hemisférico.

En este contexto, uno de los mandatos principales del Departamento es: ayudar y asistir técnicamente a los Estados miembros de la OEA para una mejor implementación de la Convención de Palermo en la lucha contra la delincuencia organizada trasnacional y sus protocolos adicionales, que versan sobre trata de personas, tráfico ilícito de migrantes y tráfico ilícito de armas.[2]

Teniendo en cuenta el contexto de la pandemia y algunas actualizaciones que se han hecho en el Departamento y en particular asociados a los asuntos de defensa, la presentación se divide en los seis (6) puntos a desarrollar: 1. Combate a la delincuencia organizada trasnacional (DOT) en pandemia; 2. Programas OEA DDOT; 3. Capacitaciones OEA DDOT; 4. Acciones vinculadas con la defensa; 5. Nuevos mandatos OEA DDOT; 6. Foros políticos y técnicos.

1. Combate a la delincuencia organizada trasnacional (DOT) en pandemia:

En el contexto emergente de la pandemia del COVID-19 y las respuestas generadas desde la OEA, desde el Departamento DDOT se planteó el interrogante de cómo podría impactar el accionar de la delincuencia organizada trasnacional en la región y cómo afrontar los desafíos latentes y las nuevas modalidades para afrontar el crimen organizado, ante nuevos riesgos en tiempos de pandemia.

Es bajo este contexto de incertidumbre y de parálisis de circulación de personas en la región, que preliminarmente se planteaba que había una reducción del delito en ciertas manifestaciones.

---

[1] Director del Departamento contra la Delincuencia Organizada Transnacional de la Organización de los Estados Americanos (OEA). Fue el Director Nacional de Cooperación Internacional en el Ministerio de Seguridad de la República Argentina. Politólogo de la Universidad de Buenos Aires. Magíster en Estudios Internacionales de la Universidad Torcuato Di Tella. Correo: gschumeister@oas.org

[2] Para más información sobre el Departamento contra la Delincuencia Organizada Transnacional de la OEA, puede consultarse su página web oficial: https://www.oas.org/es/sms/ddot

Sin embargo, no se tardó mucho tiempo para advertirse que el crimen organizado no se había tomado ninguna "cuarentena" y aún en una situación tan crítica como la pandemia no detendría su accionar en la región, haciendo que —entre otras cosas— la logística de las actividades criminales se trasladara de las calles a la virtualidad. No estamos hablando de fenómenos nuevos, sino más bien de la repotenciación de delitos en la órbita del ciberespacio, o de productos falsificados asociados con necesidades del sector de la salud.

En este contexto donde el sector seguridad y defensa se ha visto resentido por las nuevas tareas y deberes que ha tenido que adoptar para mantener el orden durante la pandemia; y expuesto a una repotenciación del tráfico ilegal de medicamentos, la falsificación de productos farmacéuticos y la aparición en el mercado negro de presuntas soluciones frente al virus —inexistentes hasta el momento—, que procuran explotar la crisis y las necesidades de nuestras sociedades sin ningún escrúpulo. Tampoco tardaron en aparecer manifestaciones por parte de los grupos criminales en abierto desafío a los Estados, asumiendo roles de "asistencia social", provisionando por ejemplo a la población de productos alimenticios y sanitarios, con la pretensión de ganar simpatías entre las sociedades y ejercer el control de los territorios.

Estos son algunos de las manifestaciones primarias que ha observado el Departamento y que han llevado a preguntar sobre el futuro de los desafíos que dejaría la pandemia. En tal sentido, se ha advertido que los fenómenos identificados pueden ser apenas semejables a la punta de un "nuevo iceberg criminal", dejando aun por resolver manifestaciones latentes en juego.[3] Al respecto, desde el Departamento se ha advertido sobre las posibilidades de explotación de la crisis financiera y económica por parte del crimen organizado, sobre todo entre sectores económicos vulnerables y expuestos a la parálisis causada por la pandemia, como ser el turístico o del entretenimiento.

En la presentación se expusieron algunos fenómenos que se dieron durante el año 2021 y que por parte de la OEA se fueron dando a conocer un año atrás, advirtiendo fenómenos que han sido confirmados y repotenciados posteriormente.

2. Programas OEA DDOT:

En el marco de la pandemia se han seguido coordinando los diferentes programas que tiene el DDOT y ha sido de gran importancia porque el Departamento ha logrado organizarse y adaptarse operativamente a las nuevas condiciones impuestas por la pandemia —a través de las nuevas tecnologías y la virtualidad, fortaleciendo asimismo las capacitaciones y la asesoría técnica a sus Estados miembros.

Ejemplos de ello han sido la continuidad de sus programas contra el lavado de activos en la región —con países como Surinam por ejemplo, donde se desarrollará su Evaluación Nacional de Riesgos en materia de lavado de activos, en conjunto con el gobierno y el Banco Interamericano de Desarrollo (BID).

[3] "La punta de un nuevo iceberg criminal", nota de opinión por Gaston Schulmeister, en Infobae, Argentina. https://www.infobae.com/america/opinion/2020/05/09/la-punta-de-un-nuevo-iceberg-criminal/

Asimismo, se cuenta con un programa en asistencia de técnicas especiales de investigación —léase Entrega Vigilada; Agente Encubierto; y Vigilancia Electrónica, contempladas en la Convención de Palermo.

También la emergencia de nuevos programas, como lo es el de lucha contra la minería ilegal a nivel regional, previsto para distintos países de América Latina y el Caribe, y el programa de fortalecimiento de capacidades en recuperación de activos por lavado de activos y corrupción en Colombia, dan asimismo testimonio de la ampliación del porfolio de acciones por parte del Departamento aun durante la pandemia.

Bajo el contexto del programa contra la minería ilegal, se destaca que, junto a la Fiscalía General de la Nación se ha logrado desarrollar un trabajo para Colombia en materia de minería ilegal desde la perspectiva de la inteligencia financiera. Es decir, se busca fortalecer y desarrollar las capacidades de las agencias encargadas de todas las etapas que comprometen la lucha contra las finanzas de la minería ilegal.

3. Capacitaciones OEA DDOT:

En cuanto a las capacitaciones, existe una variedad de actividades y capacitaciones que se han ido realizando desde el Departamento, a partir de las necesidades que surgen de los estados miembros de la OEA en materia de crimen organizado, trata de personas, evaluación de riesgos; entre otros.[4]

4. Acciones vinculadas con la defensa:

Se busca compartir y trabajar codo a codo con las instituciones que tienen como tema la defensa de los Estados y los asuntos militares. En particular, junto a la Junta Interamericana de Defensa (JID) se coordinan esfuerzos y se promueve el diálogo en asuntos relacionados con la defensa y la seguridad.

Solamente por nombrar algunas de las actividades que se realizan con la JID y desde la Secretaría de Seguridad Multidimensional de la OEA, a la cual pertenece el DDOT, durante el año 2021 se ha desarrollado un evento sobre ‘El papel cambiante de las Fuerzas Armadas y sus posibilidades para mitigar y enfrentar las nuevas amenazas’. En dicho evento se abordó el desafío que implican estas denominadas “nuevas amenazas” en sus diversas modalidades, con un crimen organizado que demuestra una capacidad logística significativa. Ante estos nuevos desafíos, se propicia el apoyo entre las Fuerzas Policiales y de seguridad y la promoción de las mejores respuestas, respetando el ordenamiento jurídico de cada Estado.[5]

[4] Para dar seguimiento a las distintas actividades que el Departamento realiza, se puede consultar su cuenta de Twitter oficial: @OEA_DDOT.

[5] Para más información sobre el evento de la Junta Interamericana de Defensa (JID), ver https://www.jid.org/jid-realizo-el-seminario-el-papel-cambiante-de-las-fuerzas-armadas-y-sus-posibilidades-para-mitigar-y-enfrentar-las-nuevas-amenazas/

Además de la JID, con el Colegio Interamericano de Defensa (CID) el Departamento tiene un diálogo permanente, colaboramos y asistimos con técnicos y especialistas para distintas actividades académicas como por ejemplo el Curso sobre Crimen Organizado, que incluso ha derivado en publicaciones relacionadas, y la Capacitación Estudio de Campo OCONUS.[6]

De la misma forma, en eventos como el que nos convoca el día de hoy, estamos siempre dispuestos en apoyar a los Estados miembros de la OEA, para acompañarlos en sus instituciones y Fuerzas Armadas. A modo de referencia inmediata, se resalta asimismo la participación del DDOT en el VIII Foro de Relaciones Internacionales, Seguridad y Defensa, organizado por la Escuela Militar de Cadetes José María Córdova del Ejercito Nacional de Colombia.

5. Nuevos mandatos OEA DDOT:

Volviendo a los nuevos desafíos planteados por el accionar del crimen organizado en tiempos de pandemia, se resalta que los Estados miembros de la OEA han respondido ante los nuevos fenómenos repotenciados, promoviéndose asistencia técnica por parte del Departamento en materia de lucha contra el contrabando de productos y sustancias ilegales, que incluyen medicamentos falsos, especies de flora y fauna y delitos contra el patrimonio cultural.

En este sentido, se resalta que la Organización, a través de los mandatos se ha ido adaptando y actualizando de forma dinámica a las nuevas amenazas, para la generación de acciones y programas institucionales en respuesta.

Con todo esto se quiere destacar la importancia que tiene la promoción y operativización de la cooperación internacional de los Estados junto a organizaciones internacionales como la OEA en el hemisferio occidental —vis a vis con a distintas contrapartes institucionales como son la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Organización International de Policía Criminal (INTERPOL), el Grupo de Acción Financiera Internacional (GAFI), el Grupo de Acción financiera de Latinoamérica (GAFILAT), el Grupo de Acción Financiera del Caribe (GAFIC), el Grupo Egmont de Unidades de Inteligencia Financiera, o la Comunidad de policías de Américas (AMERIPOL), entre otras— para combatir las problemáticas pertenecientes a las economías ilícitas de manera efectiva.

6. Foros políticos y técnicos:

La OEA con distintos foros y mecanismos para promover respuestas de los Estados en las Américas ante el accionar del crimen organizado.

Entre ellos se destacan la Reunión de Autoridades Nacionales en materia de Delincuencia Organizada Transnacional (RANDOT);[7] el Grupo de Expertos para el Control de Lavados de

[6] Publicación del Colegio Interamericano de Defensa (CID) sobre el Transnational organized crime workshop, organizado entre los días 5 y 6 de noviembre de 2020: https://publications.iadc.edu/wp-content/uploads/sites/6/ebooks/Libro-Crimen-Organizado-2020-version-marzo-17.pdf

[7] Para más información sobre la RANDOT: https://www.oas.org/es/sms/ddot/prog-Reunion-de-Autoridades-materia-Delincuencia-Organizada-Transnacional-RANDOT.asp

Activos (GELAVEX);[8] la Convención Interamericana contra la Fabricación y el Tráfico Ilícitos de Armas de Fuego, Municiones, Explosivos y Otros Materiales Relacionados (CIFTA);[9] y la Reunión de Autoridades Nacionales de Trata de Personas de la OEA.[10]

Estos foros buscan que los Estados miembros puedan emitir y promover acciones en cuanto a las temáticas y fenómenos implicados de la seguridad regional. Se busca que desde una perspectiva multidimensional se reconozcan las fortalezas y desafíos institucionales latentes de los distintos Estados miembros para combatir el accionar dinámico del crimen organizado.

En el contexto de foros promovidos, la presentación compartió una actividad realizada el 1ro de octubre de 2021 por el Foro para el Progreso de América del Sur (PROSUR) junto al apoyo de la OEA, sobre 'Seguridad Regional y Amenazas Híbridas', convocada bajo el liderazgo de Colombia. Presidido por la Vicepresidente y Canciller de Colombia, el evento contó también con la participación del Secretario General de la OEA y varios cancilleres de la región, junto al apoyo de la University for Peace de las Naciones Unidas y la Universidad Nacional de Colombia.[11]

En tanto el asunto de las amenazas híbridas es de gran atención para nuestra región, vale recordar al respecto como cierre las palabras el Secretario General de la OEA, Luis Almagro:

> "El combate a estas amenazas debe hacerse desde una perspectiva multidimensional, analizando las vulnerabilidades propias y encontrando las fortalezas en nuestras instituciones que nos permitan combatirlas de forma eficiente, protegiendo los activos críticos y anticipando la materialización de los riesgos, en función de cada circunstancia y caso particular".[12]

[8] Para más información sobre el GELAVEX, ver https://www.oas.org/es/sms/ddot/prog-expertos-para-el-control-del-lavado-de-activos-gelavex.asp

[9] CIFTA es la principal herramienta de la región para abordar el tema de tráfico y proliferación ilícita de armas de fuego desde una perspectiva coordinada y transnacional. Para más información: https://www.oas.org/es/sms/dps/prog-cifta.asp

[10] Para el caso de la Reunión de Autoridades Nacionales de Trata de Personas, como con CIFTA, ambos mecanismos se coordinan desde el DDOT, en conjunto con el Departamento de Seguridad Pública de la OEA. Para más información: https://www.oas.org/es/sms/dps/prog-trata-de-personas.asp

[11] Para más información, ver Memorias del Foro PROSUR – OEA sobre Seguridad y Amenazas Hibridas. https://foroprosur.org/wp-content/uploads/2021/10/MEMORIAS-FORO-PROSUR-OEA-SOBRE-SEGURIDAD-VF-.pdf

[12] Discursos del Secretario General de la Organización de los Estados Americanos (OEA), Luis Almagro: https://www.oas.org/es/acerca/discurso_secretario_general.asp?sCodigo=21-0051

¿Es ético el hacking?

Is hacking ethical?

Ariel Pedrozo[13]

Para comenzar tenemos que definir qué es hacking: es la búsqueda y la explotación de vulnerabilidades de seguridad en sistemas o redes. ¿Eso que significa? Que el profesional de la seguridad debe tener el conocimiento necesario para poder encontrar diversas vulnerabilidades en los sistemas, en las redes, en las bases de datos de cualquier tipo de sistema operativo que esté utilizando la empresa o el gobierno en este caso. De ahí partimos a lo que es la ética. La ética es una disciplina de la filosofía que estudia el comportamiento humano y su relación con las nociones del bien y del mal, los preceptos morales, el deber, la felicidad y el bienestar común. Juntando todo eso, tenemos lo que es el hacking ético. ¿Eso que significa? Que el profesional de la seguridad, que tiene una ética y una moral, tiene que utilizar los conocimientos necesarios para poder encontrar vulnerabilidades, solucionar esas vulnerabilidades e informar las vulnerabilidades que encuentra dentro de un sistema.

Hay distintos tipos de hackers. En este caso tenemos lo del sombrero blanco, los de sombrero gris y los sombreros negros. Partamos de lo que es un hacker de sombrero negro. Es la clase de hacker que está dedicada a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos y determinados productos de software que muchas empresas están adquiriendo. Son también conocidos como atacantes de sistemas expertos en romper la seguridad, pero específicamente buscando un beneficio propio.

Luego tenemos los hackers de sombrero blanco, que son los famosos hackers éticos, que es una clase de hacker dedicada a la corrección de vulnerabilidades de software. Hacen definiciones, metodologías, medidas de seguridad y defensas de sistemas por medio de distintas herramientas. Son aquellas personas que se dedican a la seguridad de las aplicaciones de los sistemas operativos y la protección de datos sensibles, ya que ningún la mayoría sabe que los pilares de la seguridad informática son la confidencialidad, la disponibilidad y la no vulneración de datos. Y entonces el hacker de sombrero blanco es el que se dedica a realizar la seguridad de todas esas áreas y de todas esas aristas.

Luego tenemos el hacker de sombrero gris, que es una clase de hackers que está dedicada tanto a la obtención como la explotación de vulnerabilidades. O sea, es una mezcla de las dos personas de que significa que tanto puede defender como puede atacar. Frecuentemente está catalogada esta persona como si fuera una persona de grandes habilidades y conocimientos que desempeña un punto en el medio de las dos de las dos personas.

[13] Ingeniero de Sistemas de la Universidad de la Integración de las Américas (UNIDA). Especialista en Seguridad de Redes Públicas de la Universidad Blas Pascal de Córdoba. Magíster en Tecnologías de la Información de UNIDA. Correo: ariel.pedrozo@lnx.com.py

Bueno, ellos hacen los tests de seguridad, los Pentesting. Realmente hay tres tipos de pentesting que se hacen, los White Box, Black Box, y Grey Box. El White Box es el más completo. Esto significa que cualquier pentester o auditor de sistema conoce todos los datos que tiene dentro del sistema real. Entonces ya tiene una idea de todo lo que es la estructura y cómo va a ser un tipo de ataque paso a paso, de acuerdo con el conocimiento que la empresa o el Gobierno le entregue a esta persona. El Black Box es el ataque más real que utiliza el pentester en este caso, que es la persona que directamente ya no tiene conocimiento de nada. Hace un ataque sin conocimiento y tiene que utilizar todas las fases del hacking para poder realizar un ataque de forma precisa y automática. Luego se tiene el ataque gris, que más o menos es tener la diversidad, el 50 por ciento se conoce y el otro 50 por ciento no. Entonces realizan toda una investigación de lo que ya conoce con lo que no conoce para poder realizar un ataque a la empresa o lo que fuese.

Para eso existen las fases del hacking y aquí tenemos dos tipos de fases o círculos de hacking que uno realiza. Se tiene el hacking ético y lo que sigue los pasos que sigue el cracker. En este caso, el paso del hacker ético tiene cinco fases, igual que la del cracker, solamente que se diferencian dos. El primer paso que utiliza un hacker ético, igual que un cracker, es el reconocimiento de lo que se tiene o a lo que se va a atacar. Por ejemplo, una infraestructura crítica que tiene ciertos servidores web con ciertos aplicativos que están publicados. Entonces se hace un reconocimiento de lo que realmente se tiene para realizar un ataque. La segunda fase es prácticamente la misma que utiliza el escaneo, el mismo cracker o hacker ético utiliza el escaneo para saber la cantidad de puertos. Si el servicio que está publicado en Internet tiene alguna vulnerabilidad en la cual uno puede aprovechar para poder justamente pasar a la tercera fase que es la fase de obtención de acceso. La obtención de acceso prácticamente es ejecutar un exploit y dentro de ese exploit ganar el acceso a la plataforma, ya sea a nivel de sistema operativo o base de datos o aplicativo que se han publicado en la web. Y aquí es donde se hace la bifurcación. El hacker ético en el cuarto paso empieza a escribir el informe de todo lo que encontró durante el reconocimiento. El escaneo y la obtención de acceso para la empresa la cual lo contrató. Del lado del cracker, él no genera ningún informe si no mantiene el acceso para que nadie pueda saber que él ingresó a esa plataforma y de ahí pueda hacer algún salto lateral. ¿Eso qué significa? Que puede utilizar esa misma plataforma para poder saltar y hacer otro tipo de hackeos a otros lugares. En el quinto paso el hacker ético presenta el informe para ver las soluciones posibles. Del lado del cracker, realiza el borrado de las huellas que él dejó durante el ataque que hizo, él las borra para que no se puedan detectar, o sea, no pueden detectar la presencia que él tuvo en un ataque previo.

Esas son las bases del hacking normal. Ahora hablemos un poquito de lo que es el hacking avanzado, que es prácticamente no utilizar herramientas que ya traen pentester. Por ejemplo, utiliza el sistema operativo Kali Linux o utiliza un Parrot donde tiene varias herramientas y utiliza su propia dirección IP para realizar algún ataque o alguna intrusión. En el hacking avanzado se utiliza, por ejemplo, Google. Google Hacking Database que es la plataforma que, aunque la mayoría de la gente cree que funciona para hacer búsquedas, también se pueden hacer búsquedas malintencionadas. Por ejemplo, tenemos tres o cuatro búsquedas que la gente en su casa puede tranquilamente copiar y probar, donde en el primero busca los autores, servicios y administradores de lo que sea FrontPage. En el segundo, busca tipos de archivo SQL, que mucha

gente publica eso sin darse cuenta. Google tiene uno de los crawler más potentes del mundo que es una araña o un spider web que entra en todas las direcciones IP. Todos los dominios que encuentra y empieza a hacer una indexación en su propia base de datos para poder buscar eso y con ciertos parámetros, que es el que se le colocan dentro del Google Hacking Database se pueden encontrar esos parámetros, como son los archivos SQL, archivos TXT donde mucha gente pone usuarios, contraseñas, tienen archivos docs, excel, incluso fotos privadas. El último parámetro busca password/contraseñas/login dentro de un tipo de archivo TXT a todo lo que fuese los dominios .com de Colombia en este caso solamente se le cambia el parámetro si es con .co o .edu o .gov, y el solamente busca durante esos sitios esos parámetros.

Muchos de los hackers que están a otro nivel utilizan la comunicación vía TOR porque gracias a la red ellos pueden realizar conexiones, por más que sea un poco más lenta, pero pueden realizar conexiones cifradas donde cuando se llega a enterar la víctima, no ven una dirección IP que es la del propio hacker, si no ven una dirección IP de cualquier otro país. Entonces la comunicación normal de cualquier pentester o hacker ético que hace es utilizar desde internet su usuario, hace una conexión habitual al servidor para hacer algún tipo de testeo. En cambio, el hacker malicioso utiliza la red TOR que entra en un bucle cifrado para llegar al servidor. ¿Esto qué significa? Accede a la red Tor a través de un proxy TOR, hace una serie de caminos cifrados hasta el servidor, al cual va a vulnerar. ¿Cómo funciona? La red TOR funciona a través de una criptografía asimétrica donde el Onion proxy, que en este caso que es la máquina atacante, utiliza un servicio de directorios dentro de la red TOR, que utiliza tres tipos de claves que van encapsulando uno a uno hasta llegar al destino. El primer Onion Router es el primero que encapsula el total. Por eso se ve el servicio al directorio, que es el principal. Luego esa misma clave es encriptada por la clave verde. El siguiente router vuelve a encriptar y el paquete que sale de destino sale sin el cifrado. Entonces, durante todo ese recorrido que hace, tiene toda una solución que es prácticamente irrastreable, porque yo desde Paraguay, por ejemplo, puedo hacer un ataque a través de la red TOR a Argentina o Colombia, pero si llegan a encontrar la dirección IP, es de Suecia, Noruega, Holanda o de cualquier otro país menos la mía. Dentro de la red TOR también existen los HoneyPot, gente especializada para capturar otro tipo de gente dentro de la red TOR.

¿Quiénes son las víctimas? Lastimosamente somos todos. Todos somos víctimas de cualquier tipo de ataque, de cualquier tipo de vulneración de datos y la mayoría de esos ataques que se nos hacen a las empresas, a las entidades gubernamentales, entidades financieras es por inconciencia nuestra. Con esto que quiero decir que el hacking ético, tanto como ético no lo es porque sí o sí, por más que uno esté contratado por alguna empresa, algún gobierno se está vulnerando alguna información que sea confidencial. Ya sé que se puede ver desde el punto de vista de la seguridad integral de decir nosotros tenemos problemas y queremos paliar eso. Bueno, el hacking ético en sí puede paliar eso, pero ahí es donde entra la ética y la moral. Es decir, si yo estoy haciendo esto con consentimiento, pero qué pasa si a mí me contrata para realizar un ataque y una solución de seguridad y a la par otra empresa de la competencia me paga más para sacar esa información, mientras que yo estoy haciendo la seguridad de esta empresa, ¿dónde está la ética? ¿Dónde está la moral? Entonces, decir que el hacking es ético depende de la persona.

Implementación de sistema de cifrado ELGAMAL en sistemas embebidos con Linux

Implementation of the ELGAMAL encrypted system in embedded systems with Linux

Camilo Ernesto Arzuza Bonett[14]

En el sistema de cifrado ELGAMAL implementado, se combina tanto hardware como software dentro de un sistema embebido, por un razón: en el Internet de las Cosas (IoT) se usan sistemas Linux en microprocesadores ARM, pero todavía hay que considerar cómo usar sistemas criptográficos como ELGAMAL en un *System on Chip* (SoC) que use un núcleo ARM. No obstante, antes de comenzar con los detalles sobre la implementación del criptosistema, se expresará las razones matemáticas que dieron lugar a su origen.

La Criptografía de Curva Elíptica es un método aplicado, aunque sus conceptos son de matemáticas puras. Las curvas elípticas son polinomios de tercer orden que se encuentran dentro de un grupo finito cíclico y se integran con varios tipos de sistemas criptográficos con Infraestructura de Llave Pública (PKI). Estas curvas provienen de una figura tridimensional como un cono geométricamente hablando, que cuando es cortado por unos planos coordenados, se vuelve una figura de dos dimensiones. La expresión canónica de la curva es:

$$y^2 = (x - a)(x - b)(x - c) : a, b, c \in R \quad (1)$$

La anterior ecuación es un polinomio de tercer orden, en el cual el gráfico está situado en el espacio de R^3 y que con el dominio de y^2 se expresan los planos ordenados en R^2. Sin embargo, las constantes que corresponden a la factorización de la expresión canónica de la curva pertenecen solo al conjunto R. Y también caben mencionar principios de la seguridad de la información que se pueden aplicar en sistemas embebidos; los pilares básicos de la gobernanza de Tecnologías de la Información (TI) en relación a la Seguridad de la Información, vienen de la norma 27001:

- Confidencialidad es que sólo las partes involucradas pueden ver los datos.
- Integridad es la garantía dentro de las variables controlables para que los datos se mantengan intactos durante su tránsito.
- Disponibilidad es que los datos estén al alcance de las partes que los solicitan.

[14] Ingeniero de Sistemas y Telecomunicaciones de la Universidad Sergio Arboleda. Miembro del Capítulo de Colombia de la Sociedad de Sistema Electrónicos y Aeroespaciales (IEEE-AESS). Correo: camilo.ab@tutanota.com

En cuanto al concepto de Criptografía de Curva Elíptica depende de las transformaciones de funciones matemáticas para que se aplique en el hardware y en el software. Para que tenga una fórmula matemática una aplicación en el ámbito de la criptografía, se necesita solucionar y factorizar los polinomios de las curvas. Las soluciones de los polinomios cuando se factorizan son las raíces; en una curva elíptica, como polinomio de tercer orden, y se tienen tres soluciones:

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc \quad (2)$$

El intercambio de llaves forma parte del concepto de PKI, conocido por el nombre Diffie-Hellman, y creado a finales de la década de 1980. La curva elíptica permite que el intercambio de llaves por medio de la PKI sea una forma diferente y que se mejoren los estándares de privacidad. También se utiliza el arquetipo de Alice y Bob que es la base para expresar las operaciones que ocurren en la seguridad de la información y en criptografía.

El proceso básico para el intercambio de llaves,parte de que la curva elíptica es cortada por una recta en dos puntos P y Q: este es el punto que está proyectado al punto infinito y este último, es el punto que está proyectado al punto del origen O(0,0) del plano cartesiano. El tercer punto de intersección da lugar a los valores simétricos R y -R, que son los que se van a utilizar para la generación de la llave pública.

Por lo tanto el dominio de dicha función es la transformación algebraica, de la intersección entre la curva elíptica y la recta, que va a dar lugar a una cantidad determinada de puntos. Por eso, cuando se cifran los mensajes, se puede tomar cualquiera de esos puntos y no es necesario que cada vez, sea el mensaje de igual o de diferente tamaño, use un mismo punto porque se vuelve un símil a una clave estática al estilo de WEP en el estándar IEEE 802.11, que trajo muchos problemas de seguridad en las primeras implementaciones del Wi-Fi.

¿Qué hacen Alice y Bob? Se ponen de acuerdo con una sola curva elíptica. Alice escoge un punto Q y un punto G, y a partir de eso genera una llave pública con los puntos -A y A. Esa llave la envía a Bob, de tal forma que él también pueda generar su llave con los puntos -B y B. Entonces, el valor de A tiene múltiple escalar del punto G de Alice y B que tiene como omega el punto escalar que multiplica el punto G de Bob. Eso sirve para que ambos generen la llave pública y realicen el intercambio de llaves:

$$A = \gamma G \quad (3)$$

$$B = \omega G \quad (4)$$

$$C = M^e (mod N) \quad (5)$$

$$C^{\left(\frac{1}{e}\right)} mod[(\gamma-1)(G-1)] \cdot modN \equiv M \quad (6)$$

De la ecuación (5), M es el mensaje que se va a cifrar y a la *e* puede ser Euler o un número primo en particular, de lo cual depende la robustez del criptosistema, y multiplicado por el módulo de N, el producto entre las dos llaves públicas que se generan. Para poder descifrar el mensaje con

intercambio de llaves Diffie-Hellman se expresa en la última ecuación, cifrado y descifrado general utilizando PKI con criptografía de curva elíptica.

Otro tipo de curvas elípticas pertenecen a las ecuaciones de Weierstrass; estas tienen la siguiente forma:

$y^2 = x^3 + Ax + B$ (7)

Es un polinomio de tercer orden, en el que A y B son números reales constantes y aunque estos números sirven para la factorización, para que una curva elíptica exista debe pertenecer a un grupo finito. La definición canónica de la Curva Elíptica de Weierstrass es:

$E(F) = |\infty| \cup [(x, y) \in F \times F \vee y^2 = x^3 + Ax + B]$ (8)

La lemniscata definida como el valor absoluto de infinito, es el punto proyectado al infinito y se toma con los valores (x,y), que corresponden al campo finito y también está expresada dentro de la curva elíptica. F es un campo finito dentro de la 2-celda, eso quiere decir que está definida dentro del grupo canónico R2 y también aprovisiona al grupo infinito. No se permiten raíces repetidas en estos polinomios porque afectaría la robustez de la implementación de criptografía de curva elíptica. En términos matemáticos puros se puede analizar, pero para esta aplicación no es conveniente. Entonces, se toman los coeficientes:

$4A^3 + 27B^2 \neq 0$ (9)

El resultado de (9), se toma como discriminante para hallar las raíces de la curva, expresado de la siguiente forma:

$\big((r_1 - r_2)(r_1 - r_3)(r_2 - r_3)\big)^2 = -(A4^3 + 27B^2)$ (10)

Desde (10), se denota el modelo generalizado para expresar todas las constantes en términos de un polinomio ya despejado en todos sus grados:

$y^2 + axy + by = x^3 + cx^2 + dx + e.$ (11)

El otro tipo es la Curva de Montgomery; estas existen gracias a un método de factorización más simple que hallar las raíces manualmente desde la Curva de Weierstrass. El método se llama *pseudomultiplicación,* que es tomar la función del polinomio y dentro del polinomio multiplicarlo por una magnitud escalada.

La magnitud anteriormente mencionada, pertenece a los números reales y a partir de ahí se toman las soluciones. El campo finito generado, es un subconjunto que ha sido construido a partir

de operaciones entre conjuntos canónicos y los elementos que los conforman; es necesario que dicho campo finito corresponda a la construcción de números primos específicos, que forman la curva elíptica épsilon.

La operación de multiplicar el polinomio por una magnitud escalar y dar resultado se conoce como *endomorfismo.* La expresión general de las Curvas de Montgomery es:

$$\epsilon_{|A,B|} = By^2 = x(x^2 + Ax + 1) \quad (12)$$

El campo finito que se va a utilizar son números primos impares y tampoco puede haber raíces repetidos en la Curva de Montgomery. Entonces:

$$B \neq 0, A^2 \neq 4 \quad (13)$$

El plano proyectivo que producen los cortes para dar a las curvas tiene una operación para convertir de las coordenadas del plano a las coordenadas de la curva:

$$x = \frac{X}{Z}, y = \frac{Y}{Z} \quad (14)$$

Al mismo tiempo, se tienen otros componentes como el invariante en el eje unitario *j:*

$$j\epsilon_{|A,B|} = \frac{\left(256\left(A^2-3\right)^3\right)}{\left(A^2-4\right)} \quad (15)$$

Los parámetros de retorcimiento son cambios en la longitud de arco. Por lo tanto, se toman como una aproximación donde sea posible parametrizar *y* con la constante B, para cambiar ligeramente la curvatura con objetivos de aplicación en criptografía.

Las parametrizaciones son maneras de tomar una ecuación sea en R3, R2 o una línea; en el caso de R3 es una lámina doblada y se transforme en un plano; en R2 una línea en espacio retorcido y se transforme en una recta y así sucesivamente.

Entonces, la parametrización es una técnica para convertir las curvas en planos para poder medirlas. La Curva Retorcida de Edwards es una versión más simplificadas de las curvas elípticas porque ayuda con los factores de retorcimiento a su parametrización y medición. A continuación, la formula correspondiente:

$$\epsilon^{Ed}: au^2 + v^2 = 1 + bu^2 + v^2, donde \begin{cases} a = \frac{(A+2)}{B}, \\ b = \frac{(A-2)}{B} \end{cases} \quad (16)$$

Los grupos cíclicos están definidos a partir de los campos finitos y por tanto son un subgrupo de ellos. Todos operan bajo el grupo abeliano de las matemáticas que involucran todas la operaciones del cálculo. Todas las operaciones entre conjuntos canónicos aplican para las operaciones del grupo abeliano.

A través del grupo cíclico es posible seleccionar de manera redundante las operaciones entre conjuntos canónicos. En este caso, se hacen operaciones entre números enteros que tengan un factor de un número primo, este puede variar; lo ideal es que para aplicaciones de criptografía ese número primo sea impar y grande. También el orden *x* debe ser lo más alto posible para poder asegurar que el grupo sea cíclico de los elementos del grupo que se vaya a escoger:

$$F_s^x \simeq \left(\frac{Z}{(pZ)}\right)^x (17)$$

Dentro del campo finito ya definido, el valor de *q* depende del número primo *s* elevado a la *r*, donde este es el orden del grupo finito *q,* que es diferente del grupo cíclico *s: q = s*^{r}.

Esto es para resolver el problema de logaritmos discretos, ya que son muy importantes para aplicaciones de criptografía porque trata de la solución del número primo n, es decir, hallar el exponente a partir de una base generadora, y otro número primo que es igual a un término escalar alfa. Entre más grandes sean estos números es mejor porque se asegura la robustez de cualquier sistema criptográfico.

El valor escalar se construye a partir de una base generadora semilla *g* y el exponente *n* que se necesita como solución para traslaparlo y utilizarlo como un número primo impar que sirva para el sistema que se va a aplicar; *s* es un número primo impar que se va a implementar como otra semilla. Entonces:

$$\alpha \equiv g^n, mods (18)$$

También se elige un factor base, el cual es un subconjunto del campo cíclico que se haya escogido para la aplicación criptográfica. También se hallan los valores solución para la base generadora:

$$g^{k^i} \equiv \pm \prod_{b \in B} b^{r_{b,i}} mods, 0 \leq i \lesssim |B| (19)$$

Se hallan las soluciones de los exponentes de dicha base:

$$k_i \equiv (\pm 1)L + \sum_{b \in B} r_{b,i} L(b) mods - 1 (20)$$

También se necesita demostrar la identidad que compone la relación entre la base generadora y el escalar inicial, su subconjunto del grupo cíclico. A partir de eso, se da la identidad de *n* como solución; la solución utiliza la función *L,* en términos de todos los escalares alfa que se hallan, y a partir de ahí se maneja otra serie geométrica que involucra otros escalares y estos tienen esa solución específica como exponente para poder trabajar en el criptosistema:

$$n \equiv L(\alpha) \equiv \sum_{b \in B} C_b \, L(b) - jmods - 1 \quad (21)$$

El método de cifrado ELGAMAL toma las bases generadoras y será un producto particular que formaría otro número primo. El número por factorizar debe ser primo en consecuencia y debe ser el máximo común divisor de ese número escalar junto con el número primo anteriormente seleccionado. A partir de ahí, y junto con la base generadora, se produce la llave pública porque con el número primo del máximo común divisor es que se genera la llave privada:

$$MCD(\alpha, s) = 1 \quad (22)$$

$$h = g^{\alpha} \quad (23)$$

A partir de *h,* del número cíclico seleccionado, y de la base generadora está la llave pública, que en este caso en el arquetipo de ciberseguridad la genera Bob. Alice también genera su llave pública, pero en vez de utilizar el término *h,* se utiliza el término *k:*

$$MCD(k, s) = 1 \quad (24)$$

Luego, entre ellos se hace un intercambio de llaves y se obtiene un producto:

$$w = h^k = g^{\alpha k} \quad (25)$$

Ese producto es el portador del mensaje cifrado ELGAMAL. La idea es que ese producto exponente sea un número primo tan grande, que dificulte en una gran medida el descifrado del mensaje por ataques de fuerza bruta o por ataques de hombre en el medio. Para descifrar el mensaje, se aplica la siguiente fórmula:

$$M_C = \left(g^k, M \cdot w\right) \quad (26)$$

El hardware utilizado ha sido la BeagleBone AI, y aunque este tipo de equipo no tiene como propósito este tipo de aplicaciones, tiene una buena composición para las aplicaciones criptográficas debido a que son de alta intensidad computacional. También se utiliza el cable de Ethernet para conectarse a internet, ya que se necesita para acciones administrativas del sistema

operativo que está corriendo, y además, se utiliza el puerto serial para tener acceso al Shell desde un computador portátil convencional con el sistema Linux operando.

No se utilizará la interfaz inalámbrica por razones de seguridad operativa todavía, debido a que apenas se están haciendo los ajustes y la fase experimental para la implementación de este tipo de criptosistemas. Hay un módulo FTDI, el cual permite convertir las señales del puerto serial de la tarjeta a una interfaz USB que permita mostrar caracteres de todo tipo en el computador para poder visualizar el sistema operativo.

Dentro del computador, y del sistema embebido se maneja la utilidad serial Minicom: esta es una aplicación por la línea de comandos, al estilo de Telnet, que utiliza sistemas Linux y tipo BSD. En este caso, se hizo el ajuste del puerto serial, de tal forma que apunte al dispositivo que fue detectado como FTDI y conectado por el puerto USB: *dev/ttyUSB0*. La velocidad de transmisión es de 115200 baudios, 8 bits de paridad y 1 de parada. Solo se hace control del flujo de software, pero no de hardware para evitar que un valor arbitrario o interferencias físicas de la comunicación, le afecte de manera negativa.

Desde ahí, una vez la utilidad serial esté lista, se puede observar cómo arranca el Sistema Operacional Arch Linux. En el cargador de arranque se identifica el fabricante y el modelo de la tarjeta, junto con la RAM y los espacios de almacenamiento, detecta dos porque tiene una memoria Flash G embebida y una memoria MicroSD. Se ha decidido arrancar desde la memoria MicroSD porque es la que tiene el sistema operativo Arch Linux.

Cuando arranca el kernel aparece el número 0.000000, el primer tic, una unidad mínima de tiempo atómica, determinada por la operación del reloj del sistema en chip que tiene el computador, en tarjeta o el sistema embebido en cuestión. El Linux que se utiliza es a tiempo real por motivos de utilidad porque en sistemas embebidos para reducir el riesgo de fallas a nivel de software y hardware.

Cabe agregar que el intercambio de llaves Diffie-Hellman también se da como operación administrativa en Arch Linux y la implementación de curva elíptica también. Es necesario ajustar el sistema operativo donde estaba el sistema embebido y la implementación del criptosistema. Para poder empezar la instalación de paquetes y de sistemas para la implementación es necesaria la generación de llaves pública y privada para dentro del sistema Arch Linux. Para eso se necesita utilizar el comando *pacman-key,* que es el administrador de paquetes y a partir de ahí que de los niveles de confianza y que las genere. Luego, se otorga todas las opciones de mantenimiento para lograr que el sistema esté en orden; se toma el repositorio donde está la información de la curva elíptica a través de *Git,* ya preinstalado.

Asimismo, se demuestra que la aplicación Safety sirve para observar vulnerabilidades en las dependencias del intérprete *python3.* Estas indican si hay vulnerabilidades específicamente en el paquete *pip,* un gestor de *python3* que permite instalar otros paquetes de software de *Python.* La versión de *pip 20.3* es antigua porque con el boletín de vulnerabilidad de 2021, si se conecta a través de un proxy, el zócalo de SSL lo va a autorizar y algún actor externo puede suplantar el ataque de hombre al medio y acceder remotamente al sistema. Por eso, es importante tomar notas de vulnerabilidades, bajo el marco común de CVE, y el esquema de puntuación CVSS,

para actuar sobre ellas antes de utilizar un ambiente de producción para la implementación pretendida.

La instalación de la implementación *ecc-elgamal* se hace mediante *pip3 install* dentro del mismo directorio. Esto permite instalar el paquete de *data classes* para ejecutar los *scripts* en *Python.* También se han hecho las pruebas de cobertura de código, su ventaja es que van en las pruebas unitarias de código y debe ser estándar para aplicar porque es una métrica de calidad. Dichas pruebas de cobertura indican si una pieza de implementación está lista para un ambiente de producción y eso se observa en operaciones de desarrollo. Es importante que la cobertura del código sea mayor al 85%, uno de los requisitos mínimos de la calidad del código. Para la seguridad de la aplicación en términos del código, Bandit ayuda con las vulnerabilidades analizando y validando cada una de las líneas de código.

Se utiliza un código proveniente del repositorio de *GitHub* y se modifica, generando el par de llaves pública y privada de la curva 25519, que es una Curva de Montgomery segura; el cifrado el ELGAMAL de esa misma curva, se cifra generando la llave pública con los puntos descritos de la curva elíptica, se descifra y después se imprimen en consola todas esas variables. Entonces, se agregan los permisos de ejecución y se ejecuta. Es importante resaltar que la llave privada o la pública no se deben mostrar a terceros dado que compromete al criptosistema y rompe los tres pilares de la seguridad de la información.

En las implementaciones de las clases se encuentran las aplicaciones de las Curvas de Weierstrass, de Montgomery y de Edwards. En las piezas de código donde se observa el modelo de las curvas y desde ahí se hacen las operaciones aditivas de los puntos para la generación de las llaves pública y privada, y para hacer el proceso arquetípico de Alice y Bob para la implementación del criptosistema.

En cuanto a los análisis de resultados, en Safety se halla una vulnerabilidad en las dependencias del intérprete de *Python.* Esta se resuelve por medio de la acción administrativa del sistema de actualizar la utilidad de una versión mayor a la 21.1. Esta vulnerabilidad reportada en el boletín CVE-2021-28363, indica cuál es la dependencia vulnerada, que es para conexiones que se utilizan en proxy con http y https. No involucra a los certificados SSL cuando hay una conexión directa a un punto de acceso. Esto hay que tomarlo como una gestión de riesgos más proactivo que reactivo, no cuando se esté en un ambiente de producción sino en uno controlado.

La ejecución de Bandit no detectó ningún problema o vulnerabilidad en la implementación. En el caso de Coverage, se considera una cobertura de código de 100% cuando las pruebas unitarias que fueron utilizadas para determinar el comportamiento de la aplicación, pero es mejor volver a realizar las pruebas para confirmar el resultado porque también hay que determinar si las pruebas unitarias efectivamente tratan todas las funciones y los métodos, en el caso de la programación orientada a objetos. En cuanto a la implementación, el código cumple con los elementos básicos del Sistema Criptográfico: efectivamente cifra, descifra, genera el par de llaves pública y privada, etc.

Se concluye que es recomendable utilizar un núcleo Linux a tiempo real porque se facilita la reducción de fallas en software en un sistema operativo completo; un núcleo genérico puede hacer que las tareas se traslapen con facilidad y pueda afectar este tipo de criptosistemas, igual

que a cualquier sistema embebido que requiera de una aplicación crítica, se debe operar a tiempo real en todo caso.

No es posible utilizar sistema de cifrado “en caliente” para periféricos como conversores análogos digitales o interfaces seriales que transfieran y reciban datos porque se tienen latencias de cinco segundos, mientras se resuelve el criptosistema para cifrar el mensaje. Deberían utilizarse para sistemas industriales que tengan un periodo de muestreo grande, que no requieran mediciones constantes en un período muy corto de tiempo. Por último, el uso de utilidades a nivel de seguridad de las aplicaciones de software debe estar incluido durante todos los ciclos de desarrollo.

Impulsores y barreras en la adopción del Operador Económico Autorizado por la seguridad de la cadena de suministros internacionales de empresas colombianas

Promoters and barriers in the adoption of the Authorized Economic Operator for the international supply chain security of Colombian companies

Andrea Ramírez[15]

En los últimos veinte años la configuración del comercio internacional ha cambiado con rapidez. Cambios que, sin duda alguna, han sido promovidos por una mayor especialización vertical, la búsqueda de ventajas competitivas y un aumento de cadenas de suministro cada vez más complejas y exigentes, más agiles y seguras. Esta dinámica no solo ha multiplicado el número de operaciones y de actores involucrados, sino también ha aumentado los desplazamientos entre fronteras, produciendo mayores implicaciones en materia de seguridad. Ello, proporcionalmente, también ha intensificado la probabilidad de vulnerar los sistemas de seguridad por medio de actividades ilícitas. Tal como quedó demostrado tras los ataques terroristas ocurridos en Estados Unidos en septiembre del 2001.

En consecuencia, distintos organismos –como la Organización Mundial de Aduanas– han generado un punto de referencia, el cual se materializó en 2005 mediante el marco normativo de seguridad y facilitación del comercio global SAFE (por sus siglas en inglés Secure and Facilitate Global Trade), cuyo principal objetivo es el de velar por la seguridad y la eficiencia de la cadena de suministro de bienes a nivel internacional, en búsqueda de certezas y de previsibilidades dentro de un marco de gestión integrada de riesgos. Más de 84 países de la OMA han implementado el marco de manera voluntaria y gradual, por medio de programas como la alianza comercial aduanera contra el terrorismo C-TPAT en Estados Unidos, o el Operador Económico Autorizado - en países de la Unión Europea, en países asiáticos como Corea del Sur, Japón, Hong Kong y en varios países de América como Canadá, México, Colombia, Perú, República Dominicana, Brasil, Argentina– entre otros.

El Operador Económico Autorizado (OEA), se ha consolidado no solo como una plataforma basada en la prevención del terrorismo y formas de delincuencia trasnacional, sino como un facilitador del comercio a nivel internacional. Busca principalmente agilizar y simplificar las formalidades y de forma indirecta, dar confianza a los terceros asociados al negocio, sobre la legitimidad de las operaciones aduaneras y una gestión de riesgos para la seguridad integral de la cadena logística. Algunos de los beneficios puntuales en Colombia, por ejemplo, han sido la disminución de los reconocimientos e inspecciones físicas, la reducción del monto de garantías globales, la actuación directa de exportadores como declarantes y la posibilidad de tener

[15] Profesional en Negocios Internacionales, Especialista en Gerencia de Proyectos en Inteligencia de Negocios del Politécnico Grancolombiano. Docente de Negocios Internacionales del Politécnico Grancolombiano. Correo: acramirez@poligran.onmicrosoft.com

procedimientos simplificados ante la Aduana, además de ser reconocidos como operadores seguros y confiables.

En Colombia, si bien la implementación del programa OEA inició en 2011, las primeras empresas se certificaron a partir de 2016. Inicialmente, fue habilitado solo para exportadores y, posteriormente, para importadores, agentes de aduanas y operadores portuarios. Desde entonces el número de empresas certificadas ha aumentado paulatinamente, a mayo de 2022 existían quinientos cuarenta y dos (542) empresas.

La solicitud no es obligatoria ni tiene costo ante la DIAN, además pueden aplicar empresas de distintos tamaños. Sin embargo, en el transcurso de diez años, la implementación del programa OEA en el panorama nacional ha sido bajo si lo comparamos con otros países que en un tiempo similar cuentan con un mayor número de empresas con dicha certificación. Al respecto, conviene preguntarse: ¿cuáles son los obstáculos que afrontan las empresas colombianas en su cadena de suministro durante el proceso de certificación OEA, lo cual ha hecho que tengan un nivel bajo de empresas certificadas? y ¿cuáles son los impulsores que han favorecido la consecución de esta? Por lo anterior se analizaron los procesos de certificación OEA en empresas colombianas bajo la metodología de estudio de caso múltiple. Se identificaron, cuáles han sido las principales barreras, así como los impulsores en la implementación.

Las unidades de análisis fueron Diez organizaciones que se encontraban en diferentes etapas del proceso de la implementación de la certificación OEA y los informantes se han desempeñado como líderes del proceso al interior de cada una de estas organizaciones, además han proporcionado los datos relacionados con la experiencia que han tenido. La muestra es de tipo no probabilístico y ha sido el producto de una selección intencional, la cual se acopla a la pertinencia del estudio según criterio del experto. Es decir, que las empresas-estudio han sido seleccionadas conforme se ha percibido que pueden llegar a asemejar casos “prototípicos” de lo que experimentan las empresas durante el proceso de implementación del OEA.

Las variables de observación se basaron en los requisitos dispuestos en la autoevaluación del OEA en la Circular 170 de la DIAN. Que incluyen: Análisis y administración del riesgo; Asociados de negocio; Seguridad del contenedor y demás unidades de carga; Controles de acceso físico; Seguridad del personal; Seguridad de los procesos; Seguridad física; Seguridad en tecnología de la información; Entrenamiento en seguridad y conciencia de amenazas; y Seguridad sanitaria y fitosanitaria. Lo anterior permite comparar el porcentaje de avance que tiene cada objeto de estudio, en su proceso de solicitud de la certificación.

Gestión del riesgo para la seguridad de la cadena de suministro

Cuando se habla de riesgo existen distintas definiciones generadas por los autores en las múltiples áreas del conocimiento. Generalmente, dicho concepto es tratado como la incertidumbre sobre la probabilidad de ocurrencia de pérdidas. A nivel empresarial se puede utilizar la que propone la ISO 31000 que define “riesgo” como el “Efecto de la incertidumbre sobre los objetivos”. Un efecto se puede entender como una desviación de lo esperado; en otras

palabras, el riesgo frecuentemente se relaciona con los eventos potenciales y las consecuencias que pueden variar entre un efecto positivo, negativo o mixto.

En términos de riesgo al interior de la cadena de suministro, este puede variar dependiendo de los distintos flujos de materiales, información o dinero. Según Spekman & Davis (2004) existen tres dimensiones del riesgo en cadena de suministro. La primera, donde el riesgo es relacionado con el suministro de bienes, es decir, impedimentos en el proceso de compra o abastecimiento. La segunda, está asociada con rupturas en el flujo de información. Y, finalmente, la tercera dimensión concerniente al flujo de dinero está relacionada con fluctuaciones de precio, coberturas, pago puntual de las facturas, entre otras. De estas dimensiones se vislumbran riesgos como el asociado con la seguridad de los sistemas de información, también el generado por el grado de interdependencia entre aliados, la forma en la que la reputación y la imagen de la organización pueden ser afectadas por las acciones de otros actores en la cadena de suministro.

Yossi Sheffi en su libro El poder de la resiliencia, cómo las mejores empresas gestionan lo inesperado --publicado en 2015-- clasifica en cinco perspectivas el riesgo que puede afectar la operación de las empresas y en últimas su cadena de suministro. Estas son desastres naturales, accidentes, violaciones de seguridad e incumplimiento, creatividad destructiva, crisis globales e interrupciones intencionales. De este último, se desprenden otras fuentes de riesgo que pueden ser las personas involucradas en la operación que, de manera intencional o no, pueden hacer que se materialice un riesgo, por ejemplo, al afectar un proceso crítico que genere fallas o disrupciones en la cadena. Además, estos podrían envolver cualquier combinación de proveedores, trabajadores, consumidores, competidores, el entorno construido, gobiernos y entes no gubernamentales. En concordancia con lo anterior, los tipos de falla que propone se pueden materializar en el suministro, en la demanda, en el transporte, en las instalaciones o en la red de comunicaciones y en la carga. Por esto, la atención de la gestión del riesgo en la cadena de suministro debe concentrarse en analizar los posibles modos de falla luego de que se vea impactada por un evento disruptivo.

Sistemas de gestión de la Seguridad en la Cadena de Suministro (SCS)

La seguridad de la cadena de suministro, se considera la piedra angular para garantizar las operaciones ininterrumpidas y el flujo de mercancías. Las empresas han adoptado diferentes enfoques para abordar los problemas relacionados con esto. Uno de ellos son las normas ISO28000 que incluye la especificación para los sistemas de gestión de seguridad para la cadena de suministro. Estas buscan estandarizar su proceso interno y mejorar la SCS, otras están participando en la asociación gobierno-empresas para aumentar sus prácticas de seguridad, como es el caso de Programas como el operador económico Autorizado.

Si bien estas opciones no son excluyentes, la implementación de una u otra va a depender de los objetivos de las empresas. La norma propone proteger la mercancía, el punto de

fabricación hasta el punto de venta, incluyendo temas críticos como el financiero, la fabricación, la gestión de la información y la logística, el almacenamiento, el transporte, entre otros. Según esta norma se entiende el concepto de seguridad como resistencia a actos intencionales, sin autorización, destinados a causar perjuicio o daño a/o mediante, la cadena de suministro. Los sistemas de seguridad en SCS incluyen la metodología para identificar, evaluar, documentar y mantener actualizado el sistema de información, así como comunicar a los stakeholders para que cada uno sea consciente de estos. La seguridad es corregida periódicamente para garantizar que sigan siendo pertinentes con la política de gestión.

El Operador Económico Autorizado en la gestión de riesgos de cadena de suministro

Los objetivos del OEA se orientan básicamente en asegurar la cadena logística del comercio internacional mediante la implementación de medidas mínimas de seguridad contra actividades ilícitas y conductas delictivas, basadas en estándares internacionales (ALADI, 2019). Por lo anterior, la seguridad de la cadena de suministro es clave en la solicitud e implementación del OEA en las empresas. La gestión de riesgos que se haga a lo largo de los eslabones determinará qué tan segura y confiable es la empresa, y esto la ayudará a obtener o no la certificación necesaria para la continuidad de su negocio.

Obtener la calidad del OEA, por otra parte, muestra que la empresa tiene distintos lineamientos relacionados con la seguridad de la cadena de suministro y que, además, cuenta con un historial satisfactorio en el cumplimiento de obligaciones aduaneras y fiscales. El reconocimiento representa, en otras palabras, “un fuerte respaldo a las actividades de comercio exterior inspeccionadas por la legislación aduanera, la Superintendencia de Puertos y Transporte, la Dirección General Marítima y la Aeronáutica Civil, entre otros. En este sentido, cobra relevancia el administrar riesgos relacionados con contrabando, contaminación de la carga, el transporte de sustancias precursoras, entre otros riesgos relacionados con actividades ilícitas. La empresa, al prevenir dichos riesgos por medio de políticas y procedimientos, está cuidando su imagen y está disminuyendo la probabilidad de interrupción de su actividad económica. Además, esto conlleva a mejorar la predicción y precisión del movimiento de mercancías de un territorio a otro y la disminución del hurto de la carga, mejorando así la seguridad en general, entre otros beneficios. Lo anterior se constituyen como impulsores para la obtención de la certificación que los acredite con el programa OEA.

Con el fin de alcanzar el objetivo que busca aumentar la seguridad en la cadena de suministro, se deben adoptar medidas que la aseguren frente a amenazas relacionadas con el terrorismo, el crimen organizado multinacional, el narcotráfico y otros delitos conexos.

Resultados y Discusión

Los principales impulsores que las empresas prefieren experimentar a la hora de acceder al proceso de solicitud de certificación voluntaria del OEA son: a) los beneficios que el programa

del OEA propone, agilidad en procesos aduaneros, reducción de trámites, menores inspecciones, entre otros; b) por requisitos o preferencia del cliente, que dan prioridad negociaciones con empresas que estén certificadas; c) las mejoras que acarrea en Seguridad en la Cadena de Suministro, traducida en menor posibilidad de interrupción del negocio y mayor eficiencia de esta. Por otra parte, las principales barreras que refieren las empresas son: a) la inversión significativa que implica las implementaciones y la justificación en el presupuesto; b) la obtención y cumplimiento de los requisitos de cada capítulo, especialmente el de asociado de negocio; c) el cambio organizacional a nivel cultural que implica una conciencia de administración de riesgos.

Toda mejora que representa la implementación del OEA se ve reflejada en las ventajas que el programa propone y se traduce en cambios en los procesos logísticos, oportunidades de mejora para los integrantes de la cadena de suministro, la posibilidad de simplificar, disminuir y homologar procesos entre los actores de esta, mejorar en la regulación aduanera, mayor implementación de tecnologías de la información, reducción de trámites, agilidad en procesos aduaneros, reconocimiento mutuo entre aduanas, entre otros. Por otra parte, un impulsor clave en seguridad de la cadena logística que inicia con una mayor conciencia del riesgo en la cadena de suministro y la favorabilidad que proporciona al gestionar dichos riesgos. De tal manera, es posible evitar las interrupciones a lo largo del negocio. En contraste, una barrera es la dificultad de generar una cultura de administración del riesgo no solo al interior de las organizaciones, sino a lo largo de la cadena de suministro

Es importante contar con proveedores seguros que impidan al máximo una interrupción del negocio, que tengan experiencia y capacidad para responder a la demanda, en caso de tener que cambiar algún proveedor. Es decir, que siempre exista uno previamente evaluado. Conocer mejor a mis proveedores y saber que estoy rodeado no solo de los mejores, sino de los más seguros, para que en caso de que ocurra algo ellos puedan ser parte de un plan de emergencia. No todos los proveedores son conscientes de que deben contar con una gestión de riesgos y seguridad en CSI. Las empresas suelen tener demoras en la recepción de documentos para inscripción como proveedores, como es el caso de la manifestación suscrita: “muchos proveedores no entregan la manifestación suscrita, o se demoran en hacerlo y eso retrasa el cumplimiento del requisito” (Vasco, 2021).

Un reto que parece constante es el de completar el capítulo de asociados de negocio, debido a que el área comercial y el área de compras normalmente buscan que se realice el negocio lo antes posible, y para ellas pedir la documentación a clientes o proveedores puede desembocar en un aumento del tiempo o, incluso, en la pérdida del negocio. Es importante que las empresas realicen la debida diligencia desde el principio, que tengan incorporadas políticas que faciliten el procedimiento en la vinculación. También refiere que en este numeral es trascendental la implementación del SAGRILAFT (Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo).

Cuando las empresas lo implementan dentro de su proceso de conocimiento de asociados de negocio, favorece mucho la seguridad de estos, porque apoya las labores de consulta y verificación de listas restrictivas, entre otros aspectos. Los asociados de negocio, así como los actores de cada eslabón de la cadena de suministro, pueden desempeñar roles recurrentes a largo plazo o cambiar con frecuencia. Así que entre mejor se tenga, más fácil será identificar los

riesgos asociados en la cadena. Y es que, para cumplir este requisito, muchas veces las empresas deben realizar inversiones significativas, según indican esto al principio puede llegar a constituirse en una barrera, ya que no siempre forma parte del presupuesto que se plantea para iniciar la solicitud. Indiscutiblemente hay un costo para unirse al programa. Pero cuando se logra obtener el reconocimiento, se puede obtener los beneficios. El análisis de costo-beneficio es complejo, nunca será una ciencia perfecta.

Una de las razones del lento crecimiento del número de empresas certificadas como el OEA, se atribuye a la falta de evidencia anecdótica sobre los beneficios de la certificación para empresas de diferentes tamaños. En otros países que en la actualidad poseen el programa del OEA y que cuentan con un gran número de empresas que lo implementan, perciben de manera más cercana la inversión de unirse al programa, con los beneficios que el programa y con la promoción que hace de este. No obstante, el análisis de costo-beneficio nunca será una ciencia perfecta, pero varios países le han dejado esto a que un mayor volumen de comercio y el tiempo lo puedan resolver.

Por otra parte, se vislumbra la importancia de que las organizaciones se concentren más en que sus colaboradores y asociados de negocio cuenten con una mayor conciencia de seguridad integral, especialmente seguridad cibernética, así como educación, capacitación y uso de simuladores para crear un firewall humano más fuerte, a fin de proteger sus activos digitales y tener una continuidad del negocio. En este orden de ideas, la seguridad tecnológica y de la información va más allá de implementaciones del software y hardware, ya que aun cuando las empresas invierten en el tema puede que no sea suficiente, ya que siempre debe estar acompañada de otros elementos, tales como: el seguimiento y la mejora continua. Además, un plan de continuidad de negocio que permita sobrepasar los eventos que se presenten sin mayores interrupciones de la operación.

Conclusiones

Finalmente, un reto altamente mencionado es el liderazgo que debe existir en la empresa para poder adelantar el proyecto, y es porque el OEA no es competencia exclusiva de las áreas de comercio exterior, a pesar de que se entienden los beneficios en la operación aduanera. Se requiere participación de varias áreas y esta sinergia no es tan sencilla.

El estudio realizado logró identificar impulsores y barreras a lo largo de la implementación del programa del OEA en empresas colombianas para el mejoramiento de la seguridad de la cadena de suministro. Así mismo, el método usado para resolver la pregunta de investigación fue el adecuado porque tuvo en cuenta experiencias de empresas que han participado del proceso, dentro de los cuales se identificaron casos exitosos y no exitosos.

Es necesario reconocer que sus resultados no son extrapolables a todas las empresas, sino a aquellas que cuentan con características similares a las expuestas a lo largo del documento. Aun así, ofrece una primera aproximación para futuros estudios. A partir de los resultados obtenidos se desprenden temas como los costos-beneficios de la implementación en el programa, así como la implementación de buenas prácticas no solo para la obtención de la certificación, sino para la

conservación de esta. Igualmente, para una futura revisión de cómo la consecución del OEA aumenta los negocios internacionales de Colombia, entre otros temas donde es importante continuar investigando.

En suma, la implementación del programa del OEA en empresas colombianas fortalece el compromiso con la seguridad en la cadena de suministro, que puede conllevar a obtener procesos más eficientes, reflejados en menores costos, tiempos e interrupciones en el negocio. Esto se convierte en una cadena de impulsores. En contraste, un reto grande, es lograr que funcione al interior de las organizaciones, para lo cual contar con un liderazgo que promueva una cultura de administración de riesgos es fundamental. Así mismo son componentes indispensables los recursos humanos, físicos y económicos; además la sinergia entre partes interesadas que es la base. Se integran el conocimiento y la experiencia para alcanzar los objetivos no solo a corto plazo, sino mediano y largo. Lograr una cultura organizacional basada en riesgos es un reto grande, puesto que implementar nuevas actividades a las que no se estaba acostumbrado es difícil, y más si no es la alta dirección la que moviliza quiénes son el mayor impulsor al interior de las empresas. Por otro lado, en seguridad el componente económico puede ser una barrera relevante, no obstante, al comparar el costo-beneficio se puede superar. De aquí la importancia de arrancar el proyecto costeado.

Finalmente, el mercado internacional cada vez demanda más a las empresas para que se diferencien y sean competitivas. Si con el programa del OEA es como pertenecer a un club se puede generar gran parte de esta diferenciación, además porque se va a dar preferencia a querer negociar con empresas que estén en el mismo medio, sobre la misma altura y condiciones. Todo ello coloca a la empresa en una mejor posición para poder negociar. El reconocimiento no es único por parte de las demás empresas, sino por parte de la aduana y también por parte de la sociedad que ve con mejores ojos ese tipo de organizaciones comprometidas con la confianza y la seguridad.

Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance delictivo del cibercrimen en Colombia y la región

Cybersecurity: a look into the anticipatory methods and strategies for the delinquent advances of cybercrime in Colombia and the Latin American region

Gabriel Jiménez Almeira[16]

Por medio de un enfoque cualitativo y basado en una investigación documentada, la ponencia tiene como objetivo esclarecer los conceptos como ciberespacio, ciberdelitos y cibercrimen para la comprensión del accionar del gobierno nacional, de la estructura del Estado y de las políticas públicas de prevención del cibercrimen. Para tratar los temas relacionados con el ciberespacio y la ciberseguridad se entiende la evolución de los conflictos, la mutación de los actores y de las formas de lucha, teniendo en cuenta el fenómeno de la globalización y más específicamente de los procesos de globalización desviada.

La evolución de los conflictos lleva a que los medios digitales, con el avance de las tecnologías de la información, sean los nuevos escenarios donde se desarrolla el crimen organizado. El paso de los delitos al ciberespacio tiene repercusiones en el abordaje de la seguridad pública y de la seguridad integral. Cuando se habla del ciberespacio se deben abordar dos conceptos en relación con la seguridad del Estado: ciberseguridad y ciberdefensa. La ciberseguridad es preventiva y del ámbito nacional; cómo el Estado previene los riesgos que pueden suceder en el ciberespacio. La ciberdefensa es reactiva, los métodos y las acciones que emplea el Estado para contrarrestar los delitos que se pueden presentar en el ciberespacio.

Skopik[17] afirma que los grupos armados utilizan 'ataques duales', hay un riesgo en doble vía cuando se habla de la ciberseguridad y de la ciberdefensa: puede que las acciones se concierten mediante el ciberespacio, pero la materialización sucede en el espacio físico. Entonces estos ataques duales van a posibilitar un accionar multidimensional de la criminalidad, generando procesos de inestabilidad dentro de las instituciones estatales y sociales.

En el caso de los Estados europeos es evidente una sinergia en las políticas y en las acciones referentes a la protección de la infraestructura crítica y a la prevención de los ataques cibernéticos. En el ámbito regional latinoamericano, y especialmente en América del Sur, se muestran avances paulatinos en las agendas de ciberseguridad. Uno de los países que ha podido desarrollar fuertes estrategias de prevención es Brasil que a través de una agenda descentralizada e integrando el sector aeroespacial con el nuclear ha posicionado el asunto de la ciberseguridad en un nivel superior para la seguridad nacional. Este desarrollo estratégico que

---

[16] Internacionalista de la Universidad del Rosario. Magister en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra (ESDEG). Joven Investigador del Departamento de Estrategia de la ESDEG. Columnista de la revista digital Kien&Ke.com. Asesor de la Consejería Presidencial para la Juventud, Colombia Joven. Correo: jimenezg@esdegue.edu.co

[17] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60,* 154-176.

ha empleado Brasil ha sido a través de diferentes ministerios públicos coordinando trasversalmente acciones preventivas y de la gestión del riesgo. Asimismo, el Ministerio de Defensa concentra las estrategias de ciberdefensa a través de las Fuerzas Militares, incluso fomentando la cooperación regional para combatir el ciberdelito cometido por grupos de crimen organizado trasnacional.

En el caso mexicano, hay una gran diferencia en el abordaje de la ciberseguridad debido a su posicionamiento geopolítico al compartir fronteras con Estados Unidos. En este sentido, sus políticas se centran en la identificación del actor, haciendo una diferenciación clara entre los intereses políticos y los económicos. Sobre todo, se hace énfasis en el interés económico debido al fuerte tráfico en la frontera porosa con Estados Unidos, teniendo en cuenta el enfoque de infraestructura de la prevención dada por acciones del actor. Entonces, si el actor es estatal o no, la acción reactiva depende de la identificación de sus intereses para poder desmantelar la acción.

En la República Argentina, se tiene una visión realista y alineada con las acciones preventivas del Estado, esperando que las acciones en el ciberespacio provengan de otro Estado, más que de un grupo criminal. Entonces, la ciberseguridad está fuertemente relacionada con la cooperación interestatal y la organización del Estado generando lazos interinstitucionales. Cuando la amenaza no proviene de otro Estado, se baja su nivel a asuntos de seguridad ciudadana, en lo relativo a la protección de los datos en los movimientos financieros y comerciales.

En Chile, la ciberseguridad también se encuentra dentro de una estructura descentralizada que tiene una visión de desarrollo estratégico, que es la necesidad de generar prospectiva del riesgo en el ciberespacio a través de la creación de políticas a largo plazo y de instituciones que sirvan para la defensa. Con el desarrollo económico reciente del Estado chileno, se han centrado en la protección de su estructura financiera. Entonces, esta estructura les permite identificar a tiempo a los actores y mitigar las amenazas en el ciberespacio.

Para el caso de Perú, el Estado ha empezado recientemente a trabajar en la construcción de un aparato centralizado. Si bien existe una cooperación entre el sector público y el privado para la protección de la estructura institucional cibernética, esta se canaliza mediante un organismo estatal encargado de la ciberseguridad y de la ciberdefensa. Por último, en Ecuador la estructura de la ciberseguridad se caracteriza por ser descentralizada con unos sectores aeroespacial y nuclear con nivel superior, por encima del narcotráfico y del accionar de grupos criminales porque afectan la infraestructura y la operatividad del Estado, y del sector financiero-bancario ecuatoriano. Por tanto, se generan asociaciones público-privadas para la prevención.

En el panorama colombiano en cuanto al ciberespacio y al cibercrimen se define en cinco conceptos: el primero es la mula informática o cibernética, léase un usuario que, dentro de su actividad en el ciberespacio, directa o indirectamente coopera con estructuras criminales para generar mecanismos desestabilizantes; el segundo es el ‘money donkey’, el encargado de la limpieza del dinero ilegal y de su ocultamiento en paraísos fiscales; el tercero es el ciberactivismo con fines ilegales; el cuarto es el ciber reclutamiento; por último, con la cobertura de internet regional es más difícil que el ciberdelito pueda tener efectos por fuera de las ciudades.

Así mismo, el Estado colombiano está buscando cada vez más estrategias de mitigación en el que no se vulneren los derechos humanos de los ciudadanos, como la Ley 752 de 1999 de comercio electrónico, pasando por las diferentes leyes y desarrollos, en especial los que entran

en materia del ciberespacio. El CONPES 3701 de 2011 que se encarga de la creación del Equipo de Respuesta a Emergencias Computacionales (ColCERT), el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético de las Fuerzas Militares (CCCOC). El Estado se da cuenta de las mutaciones en las acciones de grupos criminales y que estaba siendo atacado desde el ciberespacio, específicamente a las páginas institucionales y los servidores donde reposa la información estratégica. En consecuencia, se genera la recomendación en el CONPES de construir estos dos centros descentralizados con un financiamiento de 4.600 millones de pesos.

El CONPES 3854 de 2016 se basa el enfoque de gestión de riesgos en seguridad digital por recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE) con un financiamiento de 85.070 millones de pesos. El actual CONPES 3995 de 2020 busca con más esmero fortalecer el plan en gestión de riesgos de seguridad digital y respuestas de incidentes al sector a través del Departamento Administrativo de la Presidencia DAPRE, configurando modelos y nuevas estrategias, contando con un presupuesto de 4.600 millones de pesos. Además busca fortalecer y trabajar con distintos ministerios en la creación de una serie de guías metodológicas en lo respectivo a la cibernética y los fortalecimientos en materia de gestión de riesgos. Finalmente, el Ministerio de Tecnologías de Información y Comunicaciones (MINTIC) será el encargado de expedir los lineamientos y guías que faciliten a las entidades públicas a la adopción de la ciberseguridad. Es importante entender que la descentralización aglomera las instituciones que pueden articularse para actuar para la seguridad digital con enfoque de gestión de riesgos.

Luego se realiza una descripción del mapa de actores que han estado en el proceso y desarrollo de la estrategia y de los actuales proyectos de prevención del cibercrimen: ColCERT, CCP, CCCOC, Equipo de Respuesta a Incidentes de Seguridad (CSIRT), Dirección de Gobierno Digital, Comité de Ciberdefensa y las Unidades Cibernéticas de las tres fuerzas militares. También es fundamental integrar al sector privado de la seguridad dado que tiene mecanismos que pueden favorecer las acciones en el ciberespacio.

En cuanto a los métodos de ciberseguridad y ciberdefensa en Colombia se deben considerar tres sectores: el Sector de Defensa y Seguridad se agrupa en la Policía Nacional como las Fuerzas Militares en la acción de procesamiento de datos, interconexión directa a las comunicaciones con capacidad de investigación y la prevención de ataques (Ransomware, Malware, Phishing, Skimming y Reporte de Incidentes); el Sector de Tecnologías de Información y Comunicación a través del CSIRT Gobierno como nueva acción del MINTIC para la generación de alertas y advertencias, análisis de vulneraciones web, monitoreo de eventos de seguridad y de portales gubernamentales, así como gestión de incidentes y análisis de malware; y el Sector Privado tiene capacidades importantes para la prevención como los circuitos cerrados de televisión, el acceso a la identificación dactilar, la reserva de información en servidores especializados y la seguridad electrónica.

Finalmente, Colombia se encamina hacia la construcción y el fortalecimiento de cuatro aspectos:

1. El sector educativo con enfoque de prevención para que en la formación de los niños y jóvenes se incluyan los mecanismos de prevención y las vulnerabilidades de la ciberseguridad.
2. El sector académico con enfoque de ciencia y tecnología, en tanto es importante generar procesos de investigación para producir métodos, software y hardware propios de anticipación al cibercrimen y así proponer procesos regionales de cooperación en cuanto el abordaje de la ciberseguridad y la ciberdefensa.

3. El sector institucional requiere de más esfuerzos en la legislación en lo referente a la ciberseguridad, en la actualización de la Ley de Inteligencia y Contrainteligencia, en la promulgación de una Ley de Seguridad Nacional donde se incluya la ciberseguridad y la ciberdefensa, colocando estas temáticas en la agenda pública y en debate con los diferentes actores institucionales, según la evolución de los conflictos.
4. El sector defensa y seguridad requiere de fortalecimiento para continuar con la protección de infraestructura crítica y la prevención de ciber ataques a las empresas públicas y privadas, garantizando las condiciones para el desarrollo económico y social.

Conclusión

El IV Congreso Internacional de la Seguridad Integral ha finalizado exitosamente debido a una gran participación internacional e interorganizacional; el interés demostrado por los asistentes y participantes en cualquiera de sus modalidades recuerda una vez más la importancia de abrir espacios de discusión sobre las necesidades de la seguridad contemporánea, en especial de la ciberseguridad. Uno de los corolarios a considerar es la necesidad de extender la cooperación multinivel entre diferentes instituciones del Estado, la empresa y la academia, así como entre las diversas autoridades gubernamentales, sus fuerzas policiales, militares y de inteligencia. A través de la formación de estos lazos cooperativos multinivel será posible fortalecer los esfuerzos de seguridad integral en tanto se reúnen capacidades operativas, experiencias y objetivos comunes. La plataforma que ofrecen las organizaciones internacionales para dialogar y construir requerirá de repensar las nociones tradicionales del Estado, de la defensa y de la seguridad, adaptándose a las contingencias de los riesgos y las amenazas actuales.

El ciberespacio es un aspecto esencial de la seguridad contemporánea en tanto la virtualidad cambia el sentido de la espacialidad y de la información. Esto no solamente se debe al cambio en el canal de comunicación entre seres humanos, sino a la condición de posibilidad de nuevas interacciones entre humanos y máquinas, instituciones, leyes y gobiernos. Otro corolario que queda del evento es la conciliación entre la seguridad y la privacidad. Al poner en cuestión el carácter ético de la vigilancia y del hacking, es necesario indagar sobre métodos y técnicas que ayuden a encontrar un balance entre la seguridad de la información y su privacidad, en cada una de las interacciones del ciberespacio, como el cifrado y la encriptación.

El último corolario es que la seguridad integral es inevitable y necesaria como concepto aplicado a todos los procesos políticos y económicos contemporáneos. Tanto las instituciones públicas como las organizaciones privadas deben planificar una agenda de seguridad para el manejo de la información, del personal, de la cadena de suministro, de la infraestructura física y de activos vitales. Esto se hace necesario porque se enfrentan a escenarios inciertos y a amenazas cambiantes, a un futuro dinámico y complejo que se encuentra enlazado a una red de actores de diversa naturaleza. En este sentido, la seguridad integral como esfuerzo organizacional por suplir a la seguridad pública con la ciberseguridad y la seguridad industrial es una respuesta al medio globalizado de la información fluida y constante entre actores multinivel.