CCCP
CENTRO DE COORDINACIÓN DE CAPACITACIÓN POLICIAL MERCOSUR

MERCOSUR

REVISTA MERCOPOL

Capacitación y Cooperación Policial del Mercosur
Capacitação e Cooperação Policial do Mercosul

Edición Paraguay - Año XI - Nº 11 Nov. 2018
ISSN 2236-9236

CIBERCRIMEN Y CIBERSEGURIDAD

- CRIPTOACTIVOS
- GOING DARK: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NA ATRIBUIÇÃO DA AUTORIA DELITIVA
- LA IMPORTANCIA DEL ANÁLISIS FORENSE DIGITAL, EN LA PERSECUCIÓN PENAL DE LOS DELITOS INFORMÁTICOS
- LOS DELITOS INFORMÁTICOS EN PARAGUAY

Editorial

Abg. Juan Ernesto Villamayor
Ministro del Interior

Es para mí un honor y un privilegio poder presentar, en nombre del Gobierno de la República del Paraguay, la Edición N° 11 de la Revista MERCOPOL, de Capacitación y Cooperación Policial del MERCOSUR, cuyo tema central es "Cibercrimen y Ciberseguridad".

Esta obra, es producto del equipo humano que conforma la Reunión de Ministros del Interior y Seguridad de este poderoso bloque regional, al que día a día dedicamos nuestros esfuerzos, con la ilusión y en pos de consolidar una visión y un actuar regional común, que impacten y fortalezcan uno de los bienes públicos más importantes para toda sociedad, que es la seguridad.

No podemos olvidar que la creciente gravitación de los procesos económicos, sociales y culturales de carácter mundial, sobre los procesos de carácter nacional, imponen desafíos comunes a nuestra región, sobre todo, los drásticos cambios generados por la revolución de la informática y las comunicaciones, que han contribuido, sin duda, en la mejora sustancial de la calidad de vida del ser humano, también han brindado nuevas herramientas y oportunidades a los criminales, para que, desde lugares remotos puedan cometer actos delictivos contra la integridad de las personas, su honor, su patrimonio, así como el daño a infraestructuras criticas de organizaciones, instituciones, empresas y particulares.

Esto nos obliga, a los responsables nacionales de seguridad, a reforzar el actuar conjunto y a un solo cuerpo a nivel regional, en la lucha contra la delincuencia, en especial en sus formas transnacionales, para ello nuestras fuerzas operativas de seguridad deben ser dotadas de capacidades e infraestructura acordes a los requerimientos actuales.

A la luz de estos desafíos, el nuevo Gobierno de la República del Paraguay ha fijado como uno de los principales objetivos para su desarrollo integral y sustentable, el fortalecimiento institucional de las fuerzas del orden público, en busca de una convivencia pacífica y segura y dentro del marco de un Estado de derecho respetuoso de las leyes.

Para ello, la estrategia principal es la de dotar de mayor capacitación al personal del orden público, de tal manera a generar conciencia y fortalecer los lazos de servicio entre los uniformados y la ciudadanía en general. Esta capacitación se genera desde las bases formativas de la Policía Nacional, dotándola de una malla curricular actualizada con nuevas técnicas, tecnologías y procedimientos que se ajustan a los requerimientos del siglo XXI.

La modernización de los recursos tecnológicos, el adiestramiento adecuado para luchar contra actividades delictivas que hace años no existían, o que se perfeccionaron y masificaron amparadas en el avance tecnológico, requerirá indefectiblemente del esfuerzo mancomunado de nuestros países, la cooperación y colaboración internacional tanto en materia de formación como de ejecución de políticas de seguridad. La integración tecnológica de las fuerzas del orden público permitirá hacer frente de manera eficiente al flagelo del cibercrimen y la delincuencia organizada transnacional; para ello, el Paraguay apuesta a la inversión en sus recursos humanos y la adecuada utilización de las tecnologías de vanguardia.

Espero que, esta publicación, pueda contribuir a entender mejor los desafíos que implica que los avances tecnológicos en el área de la informática y las comunicaciones sean utilizados con fines delictivos.

Finalmente reitero mi satisfacción por el espacio de difusión, y destacar a la vez la importancia del aporte de la Revista MERCOPOL que con su dinámica contribuye con los organismos de seguridad de la región.

Contenido

CIBER CRIMEN Y CIBER SEGURIDAD

FORMACIÓN Y CAPACITACIÓN POLICIAL

NOTAS DE INTERES

REVISTA MERCOPOL

Edición Paraguay - Año XI Nro. 11 - Noviembre de 2018
Capacitación y Cooperación Policial del Mercosur
Capacitação e Cooperação Policial do Mercosul

EDITOR RESPONSABLE
Lucio Ibañez Arce
lucio.ibanez@mdi.gov.py

COMISIÓN Y CONSEJO EDITORIAL
Evelyn Dacil Garrote
(Argentina)
Armando Slompo Filho
(Brasil)
Lucio Ibañez Arce
(Paraguay)
Maria Belén Camejo
(Uruguay)

PUBLICACIÓN ANUAL
Formato Digital

EDICIÓN GRAFICA
Departamento de Publicaciones
de la Policía Nacional
Amado Dionicio Ortellado Agüero
Crio. Pral. MCP. - Jefe
Enrique M. Barrios
Suboficial Superior PS

CCCP
CENTRO DE COORDINACIÓN
DE CAPACITACIÓN POLICIAL
MERCOSUR

CRIPTOACTIVOS

Su utilización por parte de la criminalidad económca para fuga de capitales y blanqueo de otros activos

AUTOR: Ing. Pablo Augusto Lázaro *

RESUMEN: En los últimos tiempos los criptoactivos (comúnmente llamados criptomonedas) se han convertido en un paraíso para todo criminal que quiera sacar divisas de un país sin control alguno, o realizar operaciones compatibles con el lavado de activos producto de la criminalidad. En el presente artículo desarrollaremos: ¿Qué son los criptoactivos? ¿Cuáles son los más populares? ¿Cómo se generan? Historia del Bitcoin. Ejemplos de causas criminales en las que se utilizaron criptoactivos como método de financiación o fuga de capitales. Herramientas utilizadas por los criminales y por los investigadores. Medidas de prueba que pueden sugerirse a jueces y fiscales con el fin de realizar investigaciones más eficientes.

Palabras Claves: Criptomonedas, Criptoactivos, Lavado de activos, Fuga de divisas, Bitcoin

Definición y Convenciones

Es muy común escuchar la palabra "criptomonedas" para referirse a los distintos y crecientes medios de intercambio digitales. Lo primero que debemos aclarar es que el G20, reunido en la ciudad de Buenos Aires en su reunión plenaria de Ministros de Hacienda en el mes de Marzo de 2018 definió a este fenómeno como "criptoactivos" y plantean dejar de utilizar la palabra "criptomonedas" ya que estos, según definiciones de los economistas, no son una moneda como se la conoce tradicionalmente: no tienen, como veremos, el respaldo de un banco central ni entidad financiera alguna. Por lo tanto, lo consideran un activo financiero más parecido y equiparable a lo que sería poseer una obra de arte, objetos de valor, etc. Si bien mi especialidad no es la economía, tomo esta definición habida cuenta que especialistas en esta materia han validado el concepto, pero además, como iremos viendo a lo largo del presente trabajo, los criptoactivos tienen otras peculiaridades específicas, como por ejemplo que una persona cualquiera puede crearlas o descubrirlas. Por este motivo tomo el ejemplo de la obra de arte, o específicamente un cuadro: en donde de la nada, a partir de un proceso se puede generar la obra de arte que luego, cotizada entre pares y público interesado va adquiriendo un valor de mercado y puede intercambiarse por otros bienes y servicios.

Del comunicado emitido por el G20 en la citada reunión, destacamos especialmente que las propiedades y riesgos que le atribuyen a los criptoactivos son los siguientes:

"...Carecen de los atributos necesarios para considerarse una moneda soberana ...".

"... Podrían tener implicancias en la estabilidad financiera de los países [...] recomendamos su monitoreo...".

"... Reclamamos la revisión de los estándares propuestos por el GAFI hacia ellos...".

El Grupo de Acción Financiera (GAFI), a juicio de los miembros del comité de hacienda y finanzas del G20 plantea controles e indicadores bastantes laxos respecto de la lucha que deberían dar los Estados respecto del combate a la criminalidad económica y el blanqueo de activos a través de este medio.

* *Director de Investigaciones del Ciberdelito de la Dirección Nacional de Investigaciones*
Ministerio de Seguridad de la Nación Argentina
pablo.lazaro@minseg.gob.ar

¿Qué son los criptoactivos? Un poco de historia.

En la actualidad existen cientos de criptoactivos; por citar solo algunos de ellos podemos hablar de Bitcoin, Litecoin, Monero, Ethereum, Ripple, Dogecoin y otros tantos. Incluso el presidente de Venezuela, Nicolás Maduro, ha lanzado hace poco tiempo su propio criptoactivo: el "Petro".

Partimos de la base que un criptoactivo es un "medio digital" de intercambio de valores, que se da a través del ciberespacio. Entendiendo como ciberespacio a la interconexión de equipos electrónicos y seres humanos a través de un canal, generalmente internet, que se considera una dimensión específica de conflictos. Para los teóricos de la Defensa, el ciberespacio, se considera la "quinta dimensión de conflicto", siguiendo a las tradicionales tierra, mar, aire y geoespacial, esta dimensión tiene sus peculiaridades y problemáticas específicas: no existen fronteras, los eventos se dan casi instantáneamente en cualquier punto del planeta y es muy complicado "atribuir" eventos ocurridos en este entorno a una persona física o a una "nación-estado", ya que por más que a simple vista veamos que el supuesto origen de una conexión sea desde un país determinado esto puede ser producto de varios engaños o puentes entre distintas conexiones y resultar siendo falso.

En este entorno funcionan los criptoactivos. La historia de cada uno de ellos es fascinante e invito al lector a investigar sobre el funcionamiento de todos, pero por cuestiones de respeto a los límites de trabajo dentro de esta publicación, hablaremos solamente de uno de ellos, el más antiguo y popularizado de todos: el Bitcoin. Teniendo en claro cómo funciona este criptoactivo en particular nos haremos de una clara idea de cómo funciona el resto, ya que han ido cambiando los métodos más o menos eficientes, el limite de emisión total, algunas herramientas asociadas (como el caso de Ethereum que posee su propio lenguaje de programación asociado llamado "Smart Contracts" para que la comunidad pueda crear herramientas asociadas), pero el corazón de todos ellos sigue siendo el mismo, el planteado por Bitcoin: el blockchain.

Debemos darle un poco de contexto mundial al nacimiento y auge del Bitcoin, ya que es de singular importancia: el 15 de Septiembre de 2008 el gigante financiero Lehman Brothers presenta su declaración de quiebra formal, iniciando un efecto dominó en las finanzas internacionales que culmina el *25 de Octubre de 2008*, casi un mes después, día en que se produce una masiva caída de los índices bursátiles del mundo comenzando lo que hoy se conoce como la "Gran crisis financiera del 2008". El *31 de Octubre de 2008*, apenas unos días después, cuando todo el sistema financiero y bancario se encontraba en duda por parte de la opinión pública, un tal "*Satoshi Nakamoto*" publica en un foro destinado a criptólogos en internet un artículo llamado "*Bitcoin: a peer to peer electronic cash system*" (Bitcoin: un sistema de dinero electrónico entre pares).

Figura 1: Línea de tiempo - aparición bitcoin.

En este escrito, Satoshi Nakamoto, plantea "*he trabajado en un nuevo sistema electrónico de dinero que es totalmente de igual a igual, sin tercero fiduciario*". Es decir, sin un organismo intermedio (Banco, financiera, etc) que haga de actuario de buena fe en las transacciones realizadas entre dos personas para asegurar la existencia de fondos, la existencia de las cuentas de origen y destino, etc. Lo que plantea Nakamoto es que toda la comunidad sea la dueña y depositaria de la buena fe en todas las transacciones; para esto, propone un sistema basado en una modalidad denominada "par a par" (peer to peer en inglés, comúnmente denominado por el acrónimo p2p) que hasta esa fecha se utilizaba como método para intercambio de archivos en redes en sistemas como el Kazaa o Emule, donde se plantea la inexistencia de servidores de datos centrales, y se los reemplaza por múltiples nodos y tantos servidores como clientes existan conectados a la red. Esto produjo un cambio de paradigma, ya que al no haber un servidor central es muy difícil "apagar el sistema" por completo una vez lanzado. Pero además de esto, le agrega una peculiaridad, lo que se conoce como el sistema "blockchain" (cadena de bloques) con el fin de dar fe de todas y cada una de las transacciones realizadas históricamente en el sistema bitcoin.

Para mejor ejemplificación veamos la figura número 2: en un extremo tenemos el antiguo sistema cliente/servidor tradicional, en el extremo derecho vemos el sistema "p2p". También podemos utilizar esta misma figura para

ejemplificar el sistema planteado para las transacciones económicas por Satoshi Nakamoto: en el gráfico izquierdo el tradicional sistema basado en un "banco central" por donde pasan todas las transacciones entre los distintos clientes, y en el lado derecho, el sistema planteado para Bitcoin, en donde cada uno de los usuarios da fe de los movimientos del resto.

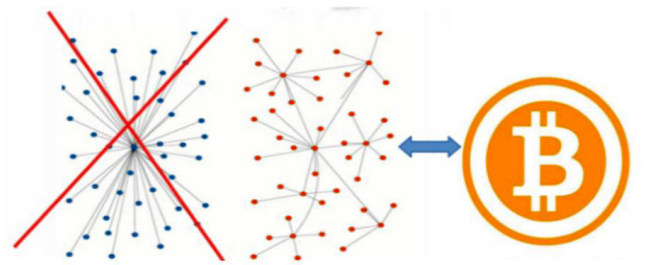


Figura 2: diferencia entre cliente/servidor y p2p.

Satoshi Nakamoto, en la presentación que hace de su proyecto establece algunos principios rectores para el armado del algoritmo que haga posible el uso de este criptoactivo, que se convertirán luego en las reglas de funcionamiento de todo el sistema:

- Los pagos realizados son irreversibles: las transacciones ya confirmadas por la comunidad no pueden borrarse ni ser canceladas. La historia es IMBORRABLE. Si alguien transfirió "por error" (o robo) dinero de un lugar a otro, la única manera de recuperarlo es con un nuevo giro a la inversa: no se puede borrar lo realizado.
- Sin censura: Nadie puede prohibir ni censurar transacciones.
- Código abierto: todo el sistema, todo el desarrollo es Open Source y está disponible para cualquiera que desee descargarlo y ver como funciona o, incluso, realizar su propio criptoactivo. De esta manera han proliferado otros tantos.
- Anónimo: no se requiere una identificación nominal de la persona que realiza operaciones en Bitcoin.
- Divisible: prácticamente hasta el infinito, la forma más común es conocida como un Satoshi, equivalente a 0,0000000001 Bitcoins (10 decimales).
- Límite de emisión monetaria: el sistema prevé que la cantidad de Bitcoins circulantes jamás podrá superar los 21 millones de unidades. Este punto obedece a cuestiones de teoría económica: al establecer un límite podrá luego fluctuar el precio de las unidades existentes.

Establecidos estos parámetros en el documento publicado, y con la ayuda de cientos de programadores a lo largo y ancho del planeta, en el año 2009 nace Bitcoin; y en este punto sucede algo muy interesante: Satoshi Nakamoto desaparece, se reserva para si mismo 1 millón de BTC (Bitcoins), libera los dominios de internet que había registrado a su nombre (bitcoin.com y otros) y nunca más se supo de él.

Existen diversas teorías sobre quién o quienes podrían ser realmente Satoshi Nakamoto, pero la realidad es que a la fecha no se encuentra demostrado, ni se sabe tampoco si este es un nombre real o un alias de un grupo de gente. En su propio perfil de redes sociales con el que interactuaba con la comunidad, manifestó ser un hombre de 57 años residente en Japón: pero esto fue rápidamente descartado debido a varios giros idiomáticos de la documentación presentada por él y algunos indicios encontrados en el software que fue presentando que lo emparentan más a gente relacionada con la bolsa de Nueva York, EEUU. Investigaciones posteriores sugirieron que podría ser gente de otros países tan disímiles como Inglaterra, Finlandia, un matemático Japonés que vivió en EEUU. La investigación mas avanzada sobre la posible identidad de Satoshi Nakamoto llegó hasta Australia, donde un emprendedor llamado Craig Wright confirmó ante varios medios ser realmente Satoshi Nakamoto, incluso aportó llaves criptográficas con las que presuntamente "Satoshi" había enviado una serie de mensajes originales en los foros e inclusive las primeras transacciones de bitcoins. Distintas demostraciones posteriores que fueron publicadas en el foro Reddit.com han arrojado un halo de misterio y el mismo Wright, un año después desmintió ser Satoshi Nakamoto pero sí, uno de los primeros en apoyar el proyecto Bitcoin y por lo tanto, colaborador. A la fecha, sigue siendo un misterio.

¿Cómo se "crea" un Bitcoin?

Primero debemos aclarar que no se "crea", sino que se "descubre": un bitcoin es el resultado producto de una compleja operación matemática. Es un gran "reto" matemático donde aquel que descubre el siguiente resultado obtiene el premio: el siguiente bitcoin. Tomemos como ejemplo, a modo de ilustración, el número "pi" que nos enseñan desde la escuela primaria como "3,1416"; este número es irracional e infinito, es decir, no existe un límite a la cantidad de decimales que pueden encontrarse y a medida que encontra-

mos el siguiente decimal se hace más complejo de encontrar el siguiente: ¿por qué? porque normalmente en este tipo de cálculos requiere elaborar operaciones sobre todos los resultados anteriores, con lo cual a medida que tiende a infinito será más y más laborioso realizar el cálculo. Con el poder de cálculo que actualmente tiene la humanidad, recién hemos podido encontrar el decimal nro 10 billones de algo que parece sumamente simple y que se utiliza desde el principio de los tiempos trigonométricos.

Tomando este ejemplo, apliquémoslo a Bitcoin, encontrar el siguiente Bitcoin es cada vez más complicado porque a medida que se van encontrando requiere realizar operaciones sobre todos los resultados anteriores. Todos aquellos que se dan a la tarea de descubrir Bitcoins se los conoce como "Mineros". "Minar bitcoins" es el hecho de buscar el resultado de estas operaciones matemáticas donde el reto matemático siempre es igual en su proceso pero las variables son diferentes y solo puede resolverse probando números al azar sin parar hasta dar con el resultado que se busca en ese momento, basado además en todos los anteriores. El primero que lo consiga se lleva la recompensa. Esto genera competencia y búsqueda de eficiencia mejorando las computadoras para este objetivo. Es por esto que en el año 2009 había varias computadoras personales realizando minería de bitcoins, porque el cálculo necesario para encontrar el siguiente era más o menos sencillo, y nos encontramos al día de la fecha en el que encontrar el siguiente es casi imposible en un tiempo prudencial para un equipo hogareño y se dedican grandes centros de datos exclusivamente a los fines de buscar el próximo bitcoin. Actualmente, luego de 10 años, nos encontramos con 16 millones de BTC encontrados, y recordemos que el límite máximo que podrá encontrase es de 21 millones, con lo cual se estima que aproximadamente en tres años más se habrán encontrado los restantes, y podrá trabajarse infinitamente sobre el valor que tendrán las divisiones de bitcoins (sus decimales) para las transferencias.

La manera de almacenar Bitcoins, ya sea porque se descubre uno en el proceso de minado, o bien porque quiero recibir/enviar bitcoins con otros miembros usuarios de la comunidad se realiza a través de las denominadas "billeteras bitcoin" (bitcoin wallet). Estas reemplazan la identidad de la persona poseedora de los bitcoins. Vale decir: quien posea la billetera, es el dueño de los Bitcoins que ella posee. Al hablar de billeteras imaginemos una base de datos (contenedor) dónde cada uno de los bitcoins que ella posee son tablas o registros dependiendo de la óptica, que estén contenidos dentro de la base de datos, protegida con una contraseña: única barrera existente entre el usuario que tiene acceso a la billetera y los bitcoins: si se pierde esta clave no hay forma de recuperar los bitcoins y por lo tanto, el dinero.

La billetera, esa "base de datos contenedora de bitcoins", puede ser generada en una computadora personal, "en la nube" a través de sitios especializados que almacenan billeteras a las que se accede con usuario y clave como si fuese un sistema de webmail ó utilizar hardware específico para billeteras como por ejemplo el denominado Trezor, que es un dipositivo del tamaño de un pendrive, que se coloca/remueve de una computadora a la hora de utilizarlo y luego se puede transportar a cualquier lado (ver figura 3)

Figura 3: Trezor – Billetera BTC por Hardware

Cada uno de estos métodos presenta sus contras: el caso de tenerlo en la computadora personal conlleva el riesgo que de perder o ante el robo del equipo se pierda para siempre; el caso del sitio en línea puede ser hackeado o cerrar de un día para el otro (como en casos ya renombrados en internet), y el trezor, es un dispositivo que puede perderse, ser robado, etc. Porque esta es una de las principales "contras" de usar bitcoin: si uno pierde acceso a su billetera virtual, pierde, literalmente, los bitcoins para siempre. Otros criptoactivos, como Ethereal, tienen lenguajes de programación propios como se dijo más arriba: uno podría crear un evento con este lenguaje de programación que si no hubiere actividad en la billetera durante tanto tiempo, que automáticamente se transfiera a otra. Esto no sucede con bitcoin, solo algunos portales (uno de los tres métodos vistos) ofrecen la posibilidad de hacer esto de forma automática pero se le está dando al dueño del portal acceso a la billetera y, por lo tanto, a los bitcoins.

¿Cómo funciona Blockchain?

Como dijimos en otro apartado de este escrito, blockchain es el corazón de bitcoin. La cadena de bloques o «block chain» es una contabilidad pública compartida en la que se basa toda la red Bitcoin. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos Bitcoin pueden calcular su saldo y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se está haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se guardan y distribuyen entre todos los mineros, que dan certeza de que las transacciones son válidas. Si habláramos en términos contables Blockchain sería el "Libro Mayor" de una empresa, donde se guardan todas las entradas y salidas a las distintas cuentas y subcuentas.

Todo bitcoin se puede rastrear desde su descrubrimiento hasta su actual ubicación en una billetera: es totalmente rastreable, lo cual no significa que el humano o empresa detrás de una billetera lo sea. Recordemos que el único medio de identificación para acceder a los bitcoins es tener la clave de acceso a la billetera, y a ella puedo acceder desde cualquier lugar del mundo, con un alias, con TOR o VPN (es decir, no mostrar mi IP de internet real, etc).

¿Cómo establecemos su valor? Como con cualquier activo: la diferencia entre lo que un tenedor esta dispuesto a recibir para venderlo y lo que un comprador esta dispuesto a pagar. Existen sitios especializados como Bitso, BitcoinExchange, etc. donde uno puede ver el valor histórico de este activo a lo largo del tiempo y las distintas fluctuaciones que fue sufriendo por diferentes factores, por ejemplo, cuando China prohibió la compra de bitcoins a través de tarjeta de crédito ó cuando hubo un robo muy grande en un popular sitio de intercambio de bitcoins: los valores se desplomaron (por citar solo un ejemplo).

Uso de los criptoactivos para la criminalidad organizada

Hasta aquí hemos visto el funcionamiento de los criptoactivos, tomando como ejemplo el más popular de ellos: Bitcoin. Sus usos para "el bien" están mas que demostrados y largamente explicados en sitios pro-criptomonedas. En este espacio, y en este medio, mi idea es alertar a los distintos investigadores sobre los usos que está tomando "para el mal", para el lavado de activos, la fuga de capitales y la criminalidad organizada en general, ya que por las condiciones predichas se hace muy difícil de rastrear a los dueños y tenedores de estos activos.

Para la fuga de capitales: comprar criptomonedas es tan sencillo como tener dinero y cambiarlo, en línea o personalmente. Por ejemplo, volviendo al caso de bitcoins, invito al lector a ingresar al sitio www.localbitcoins.com, en el que podrá elegir dónde comprar bitcoins, no solo a través de internet, sino en un lugar físico para cambiar billetes por bitcoin. En el ejemplo de la figura 4 vemos el resultado de haber puesto "compra de bitcoins, en buenos aires, en efectivo". Surgen sitios realmente llamativos como encontrarse a determinada hora en una estación de subte, o un bar, otros invitan a una oficina previo arreglo a través de whatsapp, etc. No es en si mismo nada ielgal, pero convengamos que llama la atención:

En estos ejemplos uno puede ir con billetes físicos, cambiarlos por bitcoins y tener el dinero convertido a criptoactivos sin más. Algo que parece trivial pero vale la pena recordar con esta frase tajante: una vez comprados los bitcoins, el dinero ya no se encuentra en el país. Si estos bitcoins nos son declarados al fisco, la fuga de capitales se ha consumado.

Para el lavo de activos: uno de los principales componentes en cualquier proceso de lavado de activos es el "Mezclador de dinero" (Money Mixer en inglés), en esto cito a mi colega el Director de Investigaciones sobre Lavado de Activos, el Dr. Martin Laborde, con quien venimos investigando este fenómeno de lavado a través de criptoactivos; es el hecho de volver muy dificultosa la reconstrucción de la ruta del dinero lavado: entradas/salidas al país, compra de servicios y bienes, sociedades que adquieren sociedades, y un largo etc. que se encuentran tipificados en el manual de controles que propone el GAFI. En el mundo de los criptoactivos también contamos con "Money Mixers". Por citar un solo ejemplo, existe el servicio llamado "Helix", donde uno

ingresa su billetera virtual con el dinero a "lavar", esta pagina lo distribuye en cientos de millones de pequeñas transacciones (Satoshis, 10 decimales de un bitcoin) y lo devuelve de otras billeteras "limpias" (por supuesto con una módica suma de descuento a modo de comisión en el medio) haciendo prácticamente inviable de ser revisado por un humano, es decir, recordemos que todas las transacciones son consultables de principio a fin a través del blockchain, pero cuando hablamos de cientos de miles de transacciones de blanqueo por cada uno de los bitcoins que existen en una billetera solo puede reconstruirse en un tiempo aceptable a través de software especializado.

Se usan como método de financiación de otros delitos: miremos el ejemplo de la figura 6, un caso que fue publicado en la cuenta de twitter de la Ministra de Seguridad de la Argentina, Dra. Patricia Bullrich, sobre un pedófilo que fue arrestado.

En la imagen capturada podemos ver que esta persona poseía lo que se conoce como una "Granja de minado", un grupo de placas de video de enorme poder de cálculo cuyo único fin es estar todo el día buscando nuevos criptoactivos, es decir, "Minando monedas" como vimos más arriba.

Algunas recomendaciones para investigadores:

1) Como dijimos: una vez que se compra una criptomoneda, el dinero ya no está en el país. Esto es importante fijarlo, es la clave del delito de fuga de capitales: existen cada vez más casos de envíos de dinero al exterior de carteles narcotraficantes a través de criptoactivos. Por nombrar solamente un caso argentino, el operativo "Bobinas blancas", un grupo que enviaba toneladas de cocaína al exterior de Argentina y cambiaba aproxidamente 1 millon de dólares al mes en bitcoins que, se sospecha, se convertían nuevamente a dólares en México.
2) El hecho de tener criptomonedas en una causa, por si solo, no es para nada ilegal. Tenerlos, en el caso de Argentina, en breve será equivalente a tener un cuadro o cualquier obra de arte: mientras este declarado ante el fisco es legal, y si no lo está, puede tratarse de un fraude fiscal. Las criptomonedas y su tenencia, merecen ser investigadas y solicitar medidas de prueba adicionales si existe sospecha de otras actividades conexas que pueden utilizar esto como medio de fuga de capitales o blanqueo de activos.
3) Agregar como "buena práctica" en los allanamientos: así como se buscan celulares, cámaras, y demás objetos que puedan ser de interés para la causa, la búsqueda de billeteras de criptoactivos. Esto es importante para dejar asentado en las actas, dado que puede ser luego la manera de explicar cómo es que se movían capitales entre distintos países.
4) Capacitar al personal: aparecen y desaparecen cientos de criptoactivos al año. Es importante tener personal especializado.
5) Adquieran sus propios criptoactivos: en procesos como el de "Agente revelador" o "Compras controladas", será cada vez más común la necesidad de contar con estos medios. Por ejemplo: venta de estupefacientes o armas a través de la dark web, el método de compra es a través de criptoactivos.

Por último, como recomendación general, seguir las noticias de esta temática en sitios especializados, como las recomendaciones del GAFI, o sitios tecnológicos específicos de criptoactivos: las modalidades mutan todo el tiempo y si bien, es muy difícil estar un paso adelante la única posibilidad real para realizar estas investigaciones es estar capacitados.

Bibliografía:

1) https://g20.org/sites/default/files/media/comunicado_-_marzo_2018.pdf g20.org – Reunión de Ministros de Hacienda en Buenos Aires, Marzo 2018.

2) https://www.lanacion.com.ar/2110645-petro-criptomoneda-nicolas-maduro-venezuela-crisis "Nicolás Maduro lanza la criptomoneda bolivariana: cuánto cuesta hoy el Petro" – La Nación, Argentina, Febrero 2018.

3) http://www.ieee.es/Galerias/fichero/docs_marco/2016/DIEEEM19-2016_Quinta_Dimensioxn_Fuster.pdf "La quinta dimensión digital" – IEEE, José Maria Fuster, Noviembre 2016

4) https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf Bitcoin.com – "Bitcoin: un sistema de dinero en efectivo electrónico peer¬to-peer", Satoshi Nakamoto, Octubre 2008.

5) https://clipset.20minutos.es/craig-wright-satoshi-nakamoto-bitcoin/20 Minutos – Craight Wright confirma ser el creador de Bitcoin. Agosto 2016

6) http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf Las recomendaciones del GAFI

7) https://www.infobae.com/sociedad/policiales/2017/09/03/cocaina-en-canada-quien-es-el-operador-de-bitcoins-argentino-procesado-por-lavar-dinero-de-narcos-mexicanos/Infobae.com "Quién es el operador de bitcoins argentino procesado por lavar dinero de narcos mexicanos".

GOING DARK: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NA ATRIBUIÇÃO DA AUTORIA DELITIVA

AUTORES: Alesandro Gonçalves Barreto[1]
José Anchieta Nery Neto[2]

RESUMO: A atribuição de autoria delitivano ambiente cibernético não vêm sendo tarefa fácil para os integrantes da polícia judiciária, especialmente em razão das tecnologias utilizadas por empresas de telemática ou de aplicações de internet em geral. Nesse contexto, procuraremos abordar as dificuldades na individualização da autoria e apontamento de materialidade delitiva, especialmente quando se busca o conteúdo de conversas criptografadas de criminosos, ou demais dados informáticos, armazenadas na nuvem ou em dispositivo informático protegido por senha.

Palavras-chaves: Criptografia. Investigação. Going Dark.

Introdução

O incremento das tecnologias, especialmente a interconectividade e a digitalização das relações sociais, tem trazido vários benefícios ao nosso dia.Todavia, essas ferramentas, em sua grande maioria, vêm sendo utilizadas como potencializadoras de ações praticadas por organizações criminosas e terroristas. Seja atingindo um maior número de vítimas, seja utilizando o anonimato para a prática dos seus atos, a Internet vem sendo terreno fértil e garantiade impunidade dos criminosos.

Nos dias de hoje, a busca de evidências no ambiente cibernético gera muitas dificuldades para os integrantes da polícia judiciária. Atribuir autoria delitiva não é tarefa fácil em um cenário em que temos empresas provedoras de Internetsituadas em país A,domínios registrados em país B, e servidores de armazenamento de conteúdo localizados em país C.

Como todo fenômeno social, a atividade criminosa se adapta e se reinventa a partir das mudanças vividas pela sociedade. A vida moderna interconectada, a dependência dos dispositivos móveis para atividades pessoais e profissionais, a disponibilidade de recursos financeiros a um clique, tudo isso tem potencializado também o cometimento de práticas criminosas. Por conseguinte, deve o aparelho de repressão estatal adquirir capacidade técnica de responder à altura deste novo desafio.

O celebrado autor Mark Goodman (2015, p.188,189), na obra *Future Crimes*,bem descreve o cenário apontado acima:

[1] *Delegado de Polícia Civil do Estado do Piauí e co-autor dos livros Inteligência Digital, Manual de InvestigaçãoCibernética e Investigação Digital em Fontes Abertas, da Editora Brasport, Vingança Digital, Mallet Editora. delbarreto@gmail.com.*

[2] *Delegado de Polícia Civil do Estado do Piauí ecolaborador eventual da Secretaria Nacional de Segurança Pública.anchieta.nery@pc.pi.gov.br*

> Os fora da lei são particularmente adeptos ao uso e da exploração de tecnologias criadas por outros para os próprios fins, sempre em busca de novas oportunidades. Assim que os smartphones com acesso à internet entraram na moda, os grupos de crime organizado na cidade do México começaram a usá-los para fins de pesquisa. O que eles estavam pesquisando? Quem sequestrar é claro. Os executivos que chegavam ao Aeroporto Internacional da Cidade do México representavam uma miscelânea de potenciais vítimas de sequestro. Equipes do crime organizado implantadas no aeroporto haviam se posicionado na área de chegada, ao lado da esteira de bagagem, onde as filas de motoristas elegantemente vestidos esperavam os executivos que haviam contratado seus serviços. As gangues criminosas no aeroporto utilizavam as informações nos cartazes dos motoristas para pesquisar sobre os executivos na Internet por meio de seus smartphones e descobrir seus cargos na empresa e o patrimônio líquido. Vários executivos foram sequestrados ou mortos com o uso da técnica de pesquisa via smartphone.

Nesse diapasão, os órgãos de investigação criminal visam maneiras de individualizar autoria e materialidade delitiva, especialmente por meio dabusca de evidências junto aos provedores de conexão e aplicações de Internet. Todavia, a tarefa não tem sido exitosa, especialmente tratando-se de serviços de mensageria com criptografia fim a fim, dispositivos móveis bloqueados pelos usuários ou conteúdo armazenado em nuvem.

Muito embora as autorizações judiciais sejam expedidas para a obtenção dessas informações imprescindíveis à persecução criminal, os órgãos de investigação encontram dificuldade no cumprimento dessas decisões por parte das aplicações de Internet. Esse cenário é comumente denominado de *Going Dark.*

1. Going dark

O FBI – *Federal Bureau of Investigation* – utiliza a expressão "*going dark"* para descrever a ausência de capacidade técnica no cumprimento dasautorizações judiciais de interceptação e acessoao conteúdo das comunicações ou de dados armazenados em dispositivos protegidos por senha, em razão das tecnologias empregadas pelos provedores de conexão e aplicações de Internet.

A discussão sobre o tema ganhou força após o FBI conseguir uma ordem judicial para obter dados contidos no Iphone 5c de Syed Farook, em decorrência de um ataque terrorista com 14 mortos e 22 feridos, ocorrido em 02 de dezembrode 2015,na cidade de San Bernardino-CA. A ordem judicial determinava à Apple Inc. a criação de uma nova versão do sistema operacional a fim de que o dispositivo não fosse bloqueado após diversas tentativas para obtenção da senha de acesso. A empresa, todavia, se negou a cumprir a determinação judicial alegando ter responsabilidades na proteção de dados e da privacidade dos usuários.

A problemática, todavia, não persiste apenas em solo americano. Os ataques terroristas dos últimos anos fizeram o Parlamento da Alemanha regulamentar a interceptação de aplicativos como WhatsApp e Skype. Segundo o diploma aprovado, as polícias podem utilizar procedimentos de penetração para buscar o conteúdo das comunicações de criminosos[1].

Outro exemplo dessas dificuldades encontradas na obtenção das evidências aconteceu na Rússia, cenário em que a negativa de acesso ao conteúdo de comunicação de investigados resultou no bloqueio do aplicativo Telegram[2].

No Brasil, com base em possíveis dificuldades técnicas, as decisões judiciais para obtenção de dados de criminosos enfrentam, desde algum tempo, óbice ao seu cumprimento. No ano de 2007, ocorreuo bloqueio da plataforma de compartilhamento de vídeos Youtube em razão da não remoção de um vídeo com imagens íntimas de uma apresentadora com seu namorado na Espanha. No Estado de Santa Catarina,um juiz do Tribunal Regional Eleitoral determinou a suspensão dos serviços do Facebook no Brasil pelo prazo de 24 horas. Por conseguinte, tivemos decisões judiciais bloqueando o aplicativo de mensageria WhatsApp em território brasileiropor descumprimento de ordens judiciais de acesso a dados de usuários sob investigação policial:Piauí (fev.2105), Sergipe (abr.2015), São Paulo (dez.2015) e Rio de Janeiro (jul.2016).

Assim, destacamos que o problema identificado pelo termo *Going Dark* engloba primordialmente dois pontos críticos, atualmente verdadeiras barreiras, para a persecução penal:

1) O sistema de controle de acesso de dispositivos informáticos (senha numérica, digital papilos-

cópica, *FaceID*), quando a polícia já apreendeu o equipamento relacionado a fato criminoso em apuração;

2) A alegação, por parte de provedores de aplicação de internet, que o uso de criptografia impossibilita a implementação de decisões judiciais relacionadas ao afastamento do sigilo de dados telemáticos.

2. Desafios da polícia judiciária na atribuição de autoria

A utilização de tecnologia pelos criminosos tem dificultado sobremaneira a investigação policial. Buscavam-se, outrora, testemunhas e outros dados no ambiente físico para elucidar um fato. Nos dias que correm, representamos por elementos informativos imprescindíveis para individualizar a autoria e materialidade delitiva, dentre os quais: registros de conexão e de acesso a aplicação de Internet, dados em nuvem e armazenados em dispositivos informáticos bloqueados e dados em movimento (conteúdo de comunicações de *e-mail*, redes sociais e aplicativos de mensageria).

Alguns avanços tecnológicos trazem embaraços na busca por esse dado de interesse da investigação. Especialmente quando se trata de conteúdo comunicacional encriptado ou quando se trata de dispositivo com algum tipo de bloqueio ou chave para acesso.

A transmissão de mensagens de forma codificada é prática utilizada desde a Antiguidade, por povos como os hebreus e os romanos, mas foi nos últimos anos que a criptografia alcançou escala mundial de utilização, conforme lecionamKurose e Ross (2013, página):

> Embora a criptografia tenha uma longa história que remonta, no mínimo, a Júlio César, técnicas modernas, incluindo muitas das usadas na *Internet*, são baseadas em progressos feitos nos últimos 30 anos. O livro de Kahn, The codebreakers [Kahn, 1967], e o livro de Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography [Singh, 1999], nos oferecem um panorama fascinante dessa longa história.

A criptografia é crucial na proteção das comunicações noâmbito militar, na salvaguarda das transações financeiras e na segurança e proteção de dados de pessoas e/ou corporações. Afinal a criptografia garante, dentre outras propriedades, a confidencialidade, a integridade da mensagem e a autenticação do ponto final (confirmação de identidade do destinatário). Não obstante, sua utilização em larga escala por uma infinidade de aplicações possibilitou também aoscriminosos realizar transações e comunicar-se de forma segura, furtando-se à aplicação da lei, com o uso de serviços ofertados a clientes em geral,sem necessidade de nenhum investimentoextra nessa "proteção".

A partir do momento em que uma autoridade policial requisita um dado ou almeja dar cumprimento a uma ordem judicial com o intuito de receber conteúdo relacionado à prática de crimes, recebe negativas de que a empresa não poderá dar cumprimento em razão de criptografia ponto a ponto ou de proteção incondicional dos dados de todos os usuários. As recusas são reiteradas no fornecimento de qualquer dado útil à investigação.

A atividade investigativa, quando busca elementos individualizadores de uma conduta criminosa no ambiente cibernético é, por vezes, cognominada como "estado vigilante" que, a todo custo, exige a obtenção de conteúdo do universo de usuários da Internet.

Sem embargo, quando há uma representação pela quebra de sigilo telemático ou interceptação telemática, os dados buscados são atinentes apenas a um grupo determinado de investigados e não de todo o universo de usuários. Ademais, as representações pela interceptação e pela quebra de sigilo telemáticocarecem do devido processo legal, com o exame dos indícios suficientes de autoria e materialidade criminosa, o respeito aos direitos fundamentais relacionados ao devido processo legal, à privacidade e aos demais ditames constitucionais e legais. Por fim, subsiste ainda um juízo sobre a necessidade-adequação da medida que, de forma alguma,pode ter seu uso banalizado, conforme preconiza o art. 2º da Lei nº 9.296/1996[3].

Ao pontuar sobre essa excepcionalidade na busca de elementos informativos, no discurso de abertura do FBI International Conference on Cyber Security (2018), o diretor da agência americanaassinalou:

> Nós não estamos interessados nos milhões de dispositivos utilizados pelos cidadãos diariamente. Nós estamos interessados apenas naqueles dispositivos que têm sido utilizados para planejar ou executar crimes ou atividades terroristas. Alguns têm questionado que ter acesso ao conteúdo das comunicações não é necessário – que temos uma enormidade de outras informações disponíveis fora dos nossos smartphones e dispositivos. Informação

> como a transacional para chamadas e mensagens de texto -*metadata*. Embora haja umacerta quantidade elementos que podemos colher a partir deles (metadados) a fim de processar terroristas e criminosos - prevenindo ataques e salvando vidas através da prisão e da persecução criminal - palavras podem ser evidências, enquanto mera associação entre sujeitos não será (WRAY, 2018).[4]

Por outro lado, as aplicações de Internet fazem uma coleta massiva de dados pessoais e de navegação dos usuários sob o pretexto de ofertar um melhor serviço.Todavia, operam com fins extremamente comerciais, especialmente para impulsionar propaganda ou direcionar conteúdo. A regra é coletar e repassar dados com propósitos econômicos sem controle. Noutra banda, para o fornecimento de informações de investigados, negam com argumentaçãode "estado vigilante".

Escusas para o cumprimento de ordens judiciais para fornecimento de conteúdo persistem há muitos anos no Brasil. Muito embora a Lei nº 9.296, de 24 de julho de 1996, haja regulamentado o inc. XII da parte final do art. 5º da Constituição Federal, autorizando a realização de interceptação telefônica para fazer prova em investigação policial ou instrução criminal, as operadoras de telefonia eram, de quando emvez, recalcitrantes no cumprimento de ordens emanadas pelo poder judiciário. A despeito da legislação em apreço garantir à autoridade policial o poder de requisitar serviços e técnicos especializados às concessionárias de serviço público, foram necessários diversos embates para superar os "problemas técnicos" então alegados.

Acrescente-se que já em seu artigo primeiro, parágrafo único, a Lei de Interceptações Telefônicas (Lei nº 9.296/1996) afirma que o ali disposto aplica-se "à interceptação do fluxo de comunicações em sistemas de informática e telemática". Nessa perspectiva, a utilização do diploma legalretro citado, juntamente com os novos dispositivos elencados no Marco Civil da Internet, deve ser o caminho para a operacionalização da interceptação do fluxo de comunicações telemáticas e na obtenção de dados armazenados em nuvem ou em dispositivos informáticos locais bloqueados.

O Marco Civil da Internet, Lei nº 12.965/2014, foi promulgado para estabelecer princípios e garantias do uso da Internet no Brasil. Nessa missão, traz as responsabilidades de provedores e aplicações de internet, tanto para com os usuários dos serviços, quanto para com os órgãos de persecução penal. É dever destas empresas: a guarda e disponibilização de dados de conexão (art. 10); a disponibilização do conteúdo de comunicações privadas, mediante ordem judicial(art. 10, §2º); o respeito à legislação brasileira quando a coleta, tratamento ou armazenamento de dados ocorra no Brasil, mesmo sendo a empresa estrangeira (art. 11).

Além das obrigações impostas aos *players* globais da Internet, para atingir seu fim, o Marco Civil prevê a aplicação de sanções em caso de descumprimento das determinações legais (art. 12): advertência, multa, suspensão temporária e até proibição do exercício das atividades. A lei não determina um escalonamento ou necessidade de progressão na aplicação das penalidades, mas, de certo, a autoridade deve pautar-se pelos princípios da razoabilidade e proporcionalidade na implementação da medida.

Em que pese a existência de arcabouço legislativo suficiente para imprimir às aplicações de internet a obrigação de atendimento a ordens judiciais que determinam interceptação do fluxo de comunicações ou o acesso a dados armazenados, como demonstrado, ainda persistem dificuldades destas ordens judiciais. Assim, devehaver necessária participação do Poder Judiciário e do Ministério Público na discussão sobre o tema, que reflete diretamente na independência do judiciário e uma das vertentes do princípio da inafastabilidade de jurisdição.

O princípio da inafastabilidade de jurisdição inicialmente determina que nenhuma lesão ou ameaça de lesão a direito será afastada da apreciação do Poder Judiciário. Mas só isto não é suficiente.Assim, a doutrina aponta como uma segunda vertente a garantia de que essa tutela jurisdicional cumpra a função social do sistema jurídico, garanta a satisfação da tutela pretendida. Por todos, apresentamos o ensinamento do professor Dinamarco (2013, p. 203-204):

> O inc. XXXV do art. 5º da Constituição, antes interpretado como portador somente da garantia da ação, tem o significado político de pôr sob controle os órgãos da jurisdição todas as crises jurídicas capazes e gerar estados de insatisfações às pessoas (...) **o princípio da inafastabilidade do controle jurisdicional manda que as pretensões sejam aceitas em juízo, sejam processadas e julgadas, que a tutela seja oferecida por ato do juiz àquele que tiver direito a ela – e, sobretudo, que ela seja efetiva como resultado prático do processo** (grifo nosso).

Conclusão

O crescimento econômico das empresas, em paralelo aos avanços tecnológicos, deve ser atrelado ao aumento de suas responsabilidades, tanto legais quanto sociais. Causa-nos espanto como algumas aplicações de internet lidam com o fornecimento de informações de organizações criminosas ou de células terroristas para os órgãos investigativos, ou mesmo para o Poder Judiciário, como é o caso do Telegram ao afirmar que "[...] Até hoje, nós divulgamos 0 (zero) bytes de dados de usuários para terceiros, incluindo governos[5]".

Noutra banda, o CEO da Blackberry, John Chen, demonstrou discernimento nacooperação com as investigações policiais em andamentoe dissensão da ideia de utilização da criptografia para proteção de criminosos ao afiançar que:

> Na verdade, uma das empresas de tecnologia mais poderosas do mundo recusou recentemente um pedido de acesso legal em uma investigação de um traficante de drogas conhecido, porque isso "mancharia substancialmente a marca" da empresa. Estamos de fato em um lugar escuro quando as empresas colocam sua reputação acima do bem maior. Na BlackBerry, entendemos, sem dúvida mais do que qualquer outra grande empresa de tecnologia, a importância de nosso compromisso com a privacidade para o sucesso dos produtos e o valor da marca: privacidade e segurança formam o ponto crucial de tudo o que fazemos. No entanto, nosso compromisso de privacidade não se estende aos criminosos (MOUNT, 2016)[6].

Não se trata, conquanto, de enfraquecer a criptografia à disposição dos usuários de novas tecnologias ou de criar *backdoors* para a obtenção de conteúdo necessário a uma investigação. Pelo contrário, o governo e a iniciativa privada devem fortalecer a criptografia visando, especialmente, a proteção e a privacidade dos dados. Não obstante, em casos excepcionais, como previsto em lei e sob autorização do Poder Judiciário, as empresas, quando demandadas, deverão auxiliar os órgãos de persecução criminal no bom desempenho de suas funções.

As decisões judiciais, amparadas na razoabilidade e proporcionalidade, quando da aparente colisão entre princípios constitucionais, harmonizam o momentâneo afastamento do sigilo e privacidade para garantir a segurança pública e defesa nacional, com aparo legal.Nesse cenário, o Estado deve buscar a efetividade das decisões judiciais, garantindo as características basilares de imperatividade e autoexecutoriedade atinentes aos atos jurídicos. Não cabe, portanto, às corporações privadas avaliarem, escolherem, se devem ou não cumprir a lei.

Em período de graves e sérios problemas relacionados à segurança pública brasileira, especialmente no avanço da criminalidade organizada atuante no tráfico de armas e drogas, ações contra o sistema prisional e aumento do número de homicídios no Brasil, a investigação policial, sem a cooperação das aplicações de Internet, estará caminhando para a escuridão.

Referências

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da *Internet***. Rio de Janeiro: Ed. Brasport, 2016.

_____. Aplicativo Simphony: criptografia responsável e boas práticas em tempos de going dark. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI281303,41046-Aplicativo+Simphony+criptografia+responsavel+e+boas+praticas+em>. Acesso em: 07jun. 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 15mai. 2018.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 15mai. 2018.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 15mai. 2018.

_____. Lei nº 9.296, de 24 de julho de 1996**. Regulamenta inciso XII, parte final, do art. 5º da Constituição Federal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l9296.htm>. Acesso em: 20mai. 2018.

_____. Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 15mai. 2018.

DINAMARCO, Cândido Rangel. **Instituições de direito processual civil**. Ed. Malheiros: São Paulo, 2013.

FEDERAL BUREAU OF INVESTIGATION. **Going Dark**. Disponível em:<https://www.fbi.gov/services/operational-technology/going-dark>.Acesso em: 15 mai. 2018.

GOODMAN, Marc. **Future Crimes:** tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. HSM Editora, São Paulo, 2015.

GLOBO. **Alemanha aprova lei para interceptar dados criptografados de WhatsApp e Skype**. Disponível em: <https://g1.globo.com/tecnologia/noticia/alemanha-aprova-lei-que-facilita-acesso-a-dados-criptografados-de-whatsapp-e-skype.ghtml>. Acesso em: 15mai. 2018.

KUROSE, James F. ROSS, Keith W. **Redes de computadores:** uma abordagem top-down. São Paulo-SP. Pearson Education do Brasil, 2013.

LOVELUCK, Benjamin. **Redes, liberdades e controle:** uma genealogia política da *Internet*.Petrópolis-RJ. Editora Vozes, 2018.

MOUNT, Ian. **Apple CEO Tim Cook's Feud With BlackBerry Has a Quiet End**. 29/set/2016. Disponível em: <http://fortune.com/2016/09/29/tim-cook-apple-blackberry/>. Acesso em: 15mai. 2018.

TELEGRAM. **Perguntas Frequentes**. Disponível em: <https://telegram.org/faq/br>. Acesso em: 15mai. 2018.

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA. **Ação Cautelar nº 86-37.2012.6.24.0013.** Recurso em Representação nº 203745, Acórdão de 17/03/2011, Relator(a) Min. MARCELO HENRIQUES RIBEIRO DE OLIVEIRA, Publicação: DJE - Diário da Justiça Eletrônico, Data 12/04/2011, Página 29.

UOL**. Rússia bloqueia app Telegram por não dar conteúdo de conversas**. Disponível em: <https://tecnologia.uol.com.br/noticias/afp/2018/04/13/tribunal-russo-ordena-bloqueio-do-aplicativo-telegram.htm>. Acesso em: 15mai. 2018.

WRAY, Christopher. **Raising Our Game:** Cyber Security in an Age of Digital Transformation Remarks prepared for delivery.Disponível em: <https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation>. Acesso em: 15 mai. 2018.

NOTAS

[i] *Alemanha aprova lei para interceptar dados criptografados de WhatsApp e Skype.*

[ii] *Rússia bloqueia app Telegram por não dar conteúdo de conversas.*

[iii] *Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:*

I -não houver indícios razoáveis da autoria ou participação em infração penal;

II -a prova puder ser feita por outros meios disponíveis;

III -o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

[iv] *Tradução pessoal. No original: "We're not interested in the millions of devices used by everyday citizens. We're only interested in those devices that have been used to plan or execute criminal or terrorist activities.Some have argued that having access to the content of communications isn't necessary—that we have a great deal of other information available outside of our smart phones and our devices; information including transactional information for calls and text messages, or metadata. While there's a certain amount we can glean from that, for purposes of prosecuting terrorists and criminals, words can be evidence, while mere association between subjects isn't evidence".*

[v] *TELEGRAM. Perguntas Frequentes. Questões gerais – Vocês processam solicitações de dados?*

[vi] *Tradução pessoal. No original: "In fact, one of the world's most powerful tech companies recently refused a lawful access request in an investigation of a known drug dealer because doing so would "substantially tarnish the brand" of the company. We are indeed in a dark place when companies put their reputations above the greater good. At BlackBerry, we understand, arguably more than any other large tech company, the importance of our privacy commitment to product success and brand value: privacy and security form the crux of everything we do. However, our privacy commitment does not extend to criminals".*

CIBERDELITOS RIESGOS Y AMENAZAS EN EL CIBERESPACIO

Autor: Felipe Andres Cáceres Villagra

RESUMEN: Día a día, son más las personas y entidades que se encuentran expuestas a ciberdelitos, debido a la masificación de las diferentes tecnologías y al uso masivo de internet, por lo que es necesario educar a la población mediante campañas preventivas de los potenciales riesgos que existen al divagar día a día en el mundo virtual, considerando que muchas veces se ponen en peligro sus datos comerciales o personales. Fugas de información, fraude y robo de datos, vulnerabilidad en la web o falta de un plan de continuidad de negocio son algunos de los riesgos de las empresas públicas y privadasa las que se ven expuestas en sus actividades diarias.

Por último, considerando el incipiente aumento exponencial en el uso de las tecnologías, se han desarrollado nuevos términos técnicos asociados a estos delitos emergentes, como lo son el "phishing", "pharming", "grooming", amenazas a través de redes sociales, etc., con lo cual han aumentado las denuncias asociadas, sin que existan estos términos en la legislación vigentede algunos países.

Palabras claves: phishing, pharming, grooming.

Es un hecho que, a lo largo de la historia de la evolución de la sociedad, ésta ha avanzado a pasos agigantados en lo relativo a las tecnologías creadas por el hombre. Es aquí cuando nacen los llamados "Delitos informáticos", donde el mal uso de estas tecnologías de la información, especialmente de los "Softwares", ha traído consigo consecuencias muy perjudiciales en nuestra Sociedad, evidenciando los diversos delitos relacionados con medios informáticos.

Atendido el carácter global del ciberespacio, los riesgos y amenazas provienen del interior de cada estado y del exterior, originándose tanto en causas naturales como en actividades delictuales. Por ejemplo, en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio, y con ello, los derechos de las personas.

A nivel global, existen abundantes antecedentes sobre ciberataques y actividades de espionaje en la red. La interceptación masiva de redes de telecomunicaciones, la inutilización del servicio de internet, el espionaje contra gobiernos y empresas, además de ataques contra infraestructuras críticas como servicios básicos, instituciones financieras y entidades gubernamentales, han marcado la pauta informativa a nivel global en esta materia.

A nivel regional, los países que registran el mayor número de ciberataques de "Phishing" en Latinoamérica son

Brasil, Argentina y Chile. Los accesos o robo de información desde computadores o dispositivos infectados predominaron en la región.

Asimismo, los ciberdelitoscometidos en Chile confirman el carácter transnacional de éstos, especialmente los relacionados con el uso fraudulento de tarjetas de crédito y débito, estafas informáticas, entre otros.

En atención a la naturaleza global del ciberespacio, los riesgos provienen de amenazas provenientes tanto del interior de un país como del exterior, poseen diversos orígenes, entre los que destacan:

- *Incidentes internos*: Fugas involuntarias de información, interrupción accidental de sistemas informáticos, u otros incidentes involuntarios que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
- *Desastres naturales o fuerza mayor*: Terremotos, inundaciones u otros desastres que puedan afectar al ciberespacio, debido a la destrucción de infraestructuras físicas esenciales para la disponibilidad de la información.
- *Actividades de espionaje y vigilancia llevadas a cabo por actores estatales*: Conductas que afectan la confidencialidad de la información, mediante su sustracción con fines políticos o estratégicos. En particular, destacan acciones utilizando herramientas sofisticadas conocidas como APT (amenazas avanzadas persistentes), que a su vez pueden valerse de vulnerabilidades informáticas no publicadas de las tecnologías en uso.
- *Ataques de denegación de servicio y denegación distribuida de servicios (DOS y DDOS):* Consisten en la sobrecarga intencional de servicios que se proveen en un sistema informático, que puede ser conducida desde un punto de la red o distribuirse para coordinar el ataque desde varios puntos, muchas veces mediante dispositivos infectados con programas maliciosos, con el fin de cumplir dicho propósito.
- *Cibercrimen*: actividades criminales cometidas contra componentes del ciberespacio (acceso no autorizado, sabotaje de información, robo de información, secuestro de información o "ransomware" o empleando herramientas del ciberespacio como medio de comisión "phishing", "pharming", fraudes virtuales, y otros relacionados).
- *Ataques a infraestructuras críticas mediante el ciberespacio:* la alteración en el funcionamiento de infraestructuras críticas (físicas o de la información) realizada por medios electrónicos. Por ejemplo: disrupción masiva de sistemas financieros, intervención de servicios básicos, daños físicos a infraestructuras físicas, y otros relacionados.

Todos estos riesgos y amenazas afectan la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información en el ciberespacio, y en el mediano plazo, puede afectar el desarrollo del país en el ciberespacio, privándonos de los beneficios asociados al gobierno digital, comercio electrónico, formas de organización social facilitadas por el ciberespacio, y amenazando la seguridad de las personas e instituciones en este ambiente.

DESAFÍOS RELATIVOS AL CIBERCRIMEN

Día a día, son más las personas y entidades que se encuentran expuestas a ciberdelitos, debido a la masificación de las diferentes tecnologías y el uso masivo de internet, por lo que es necesario educar a la población de los potenciales riesgos que existen al divagar día a día en el mundo virtual, y que muchas veces se ponen en peligro sus datos comerciales o personales. Así como las entidades públicas o privadas deben mantener los datos de sus usuarios a salvo, también es preocupación de cada uno hacerlo con su información personal y bancaria, en el quehacer diario en el mundo virtual o tecnológico.

Además, se debe crear conciencia de la importancia de mantener sistemas de seguridad actualizados y conocer los riesgos de la exposición a códigos maliciosos o cualquier forma que pueda representar una vulnerabilidad a la seguridad de nuestra información, que, en algunos casos, dichos ataques o intervenciones se masifican rápidamente pudiendo llegar a sistemas de información de alta importancia.

Por otra parte, para que exista una eficiente detección de los llamados ciberdelitos, esto debe ser, mediante la implementación de políticas robustas, modificación de ciertas leyes y el aumento en la gradualidad a las sanciones con respecto al delito cometido. También debe existir un mayor

conocimiento de estos, debiendo mantenerse actualizadas en la materia todas las diferentes entidades destinadas a realizar su prevención y detección en diferentes niveles. Dicha actualización debe ser realizada por diferentes organizamos nacionales e internacionales y ser considerada una política constante, la cual conlleve a una educación continua en estas materias, como también la asignación de los recursos e infraestructura para este propósito, es decir, la preocupación debe ser el accionar hoy para la detección y prevención de los delitos emergentes o delitos de ocurrencia futura.

REFERENCIAS BIBLIOGRÁFICAS

Noam Eppel.Security Absurdity: The complete, unquestionable and total failure of information security(La falla completa, incuestionable y total de la seguridad de la información). Toronto: Vivica Information Security Inc,2006.

TrendTic, "Chile es el tercer país de la región con más ataques por Ransomware". Revista TrendTic. http://www.trendtic.cl/2018/04/chile-es-el-tercer-pais-de-la-region-con-mas-ataques-por-ransomware/

Tarzano, Cesar. "Amenazas informáticas y seguridad de la información", Derecho Penal y Criminología. Colombia, p. 137- 146, 2007.

LOS DELITOS INFORMÁTICOS EN PARAGUAY

AUTORES: Comisario Principal MCP. Hugo Oscar Aguilera Penayo
Comisario MGAP Diosnel Alarcón González

RESUMEN: En la sociedad paraguaya actual, indudablemente la tecnología se ha introducido en diferentes aspectosde la vida cotidiana. Tanto a nivel personal, educativo, económico, laboral y cultural, se observa cierta dependencia de la tecnología para la comunicación entre personas, la simplificación deltrabajo, el acceso a la información, el desarrollo profesional y personal.

Palabras claves: clonación, pornografía, concienciación, sextorsión, armonización.

Es indiscutible el alcance que ha tenido hoy el uso de internet, en las personas de todas las edades como una herramienta en el día a día. Es por esto que se da lugar a diferentes riesgos en eluso de las mismas, debido al desconocimiento, o bien a la mala intención de los usuarios al momento desu utilización.

En este sentido surgen los delitos informáticos, donde personas malintencionadas buscan obtenerinformaciones indebidas o privadas de personas u organizaciones, perjudicar a terceros u obtenerbeneficios con esto.

Si bien no existe aún una medida exacta de la importancia de estas transgresiones, su incidencia se acentúacada vez más, afectando en mayor número en primer lugar a los menores de edad, en lo patrimonial, al Estado y en lo educacional.

Los tipos penales tradicionales resultan inadecuados para encuadrar las nuevas formasdelictivas, el tema plantea, además, complejos perfilespara el Derecho Internacional cuando el delito afecta a más de una jurisdicción Nacional.

La Policía Nacional del Paraguay para poner frente a los desafíos de prevención e investigación de los DELITOS INFORMÁTICOS, la Comandancia en el año 2010 ha creado la División Especializada Contra los Delitos Informáticos y en un corto tiempo esta Dependencia pasó a ser uno de los más importantes en materia de apoyo para las investigaciones en el uso de la tecnología.

El Departamento Especializado Contra la Investigación del Cibercrimen es la encargada de planificar estrategias contra el Cibercrimen y ejecutar los planes de trabajos anuales. Al frente de esta Dependencia Técnica se encuentra el Comisario MCP HUGO AGUILERA, cuenta con personales técnicos especializados en el área para la tarea de investigación, así mismo cuenta herramientas forenses y las técnicas de investigación utilizando OpenSourse.

ASPECTO LEGAL

Dentro del marco legal, el bien jurídico que protege las normas son los datos que deben permanecer íntegros, confiables y disponibles dentro de los dispositivos de almacenamiento y procesamiento, de ahí viene el concepto de los Delitos Informáticos, que *"son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas"*.

La Ley que regula y tipifica algunos aspectos de los delitos informáticos es la Ley 4439 que modifica y actualiza algunos artículos del Código Penal, fue sancionada en el Congreso Nacional el 8 de septiembre de 2011, promulgada por el Poder Ejecutivo el 3 de octubre de 2011

MARCO PENAL Ley 4439/11:

Art. 140.- Pornografía relativa a niños y adolescentes.

Habla del que produjere publicacionesque representen actos y abusos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales;

- organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o;
- distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.
- El que reprodujera publicaciones según el numeral 1 del inciso 1°, será castigado con pena privativa de libertad de hasta tres años o multa.
- La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:
- las publicaciones y espectáculos en el sentido de los incisos 1° y 2° se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados;
- el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
- el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
- el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o
- el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.
- El que obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3°, será castigado con pena privativa de libertad de hasta tres años o con multa.
- Se aplicará, en lo pertinente, también lo dispuesto en los Artículos 57 y 94."

Artículo 146 b.- Acceso indebido a datos.

El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa.

Como datos en sentido del inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible."

Artículo 146 c.- Interceptación de datos.

El que, sin autorización y utilizando medios técnicos:

- obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2°, no destinados para él;
- diera a otro una transferencia no pública de datos; o
- transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor."

"Artículo 146 d.- Preparación de acceso indebido e interceptación de datos.

El que prepare un hecho punible según el Artículo 146 b o el Artículo 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros:

1. las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2°; o
2. los programas de computación destinados a la realización de tal hecho,

Será castigado con pena privativa de libertad de hasta un año o multa.

2° Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°."

"Artículo 174 b.- Acceso indebido a sistemas informáticos.

1° El que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa.

2° Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático."

"Art. 175.- Sabotaje de sistemas informáticos.

1° El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante:

1. un hecho punible según el Artículo 174, inciso 1°; o
2. la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable.

Será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos será castigada también la tentativa."

"Artículo 175 b.- Instancia.

En los casos de los Artículos 174 y 175, la persecución penal dependerá de la instancia de la víctima; salvo que la protección del interés público requiera la persecución de oficio."

"Artículo 188.- Estafa mediante sistemas informáticos.

1° El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. una programación incorrecta;
2. el uso de datos falsos o incompletos;
3. el uso indebido de datos; u
4. la utilización de otra maniobra no autorizada; y con ello causara un perjuicio al patrimonio de otro,

Será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos, se aplicará también lo dispuesto en el Artículo 187, incisos 2° al 4°.

3° El que preparare un hecho punible señalado en el inciso 1°, mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

4° En los casos señalados en el inciso 3°, se aplicará lo dispuesto en el Artículo 266, incisos 2° y 3°."

"Artículo 248 b.- Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago.

1° El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error:

1. falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago; o
2. adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° Se castigará también la tentativa.

3° Cuando el autor actuara comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, la pena privativa de libertad podrá ser aumentada hasta diez años.

4° Tarjetas de crédito, en sentido del inciso 1°, son aquellas que han sido emitidas por una entidad de crédito o de servicios

financieros para su uso en dicho tipo de transacciones y que, por su configuración o codificación, son especialmente protegidas contra su falsificación.

5° Medios electrónicos de pago en el sentido del inciso 1°, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, permitiendo al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta

PRINCIPALES DELITOS INFORMATICOS INVESTIGADOS

En el año 2009, la modalidad más frecuente que se registró en Paraguay, fue la utilización de la clonación de tarjetas de Créditos o Débitos con cuentas Bancarias principalmente de Europa y Estados Unidos y en menor grado dentro de la región de América del Sur.

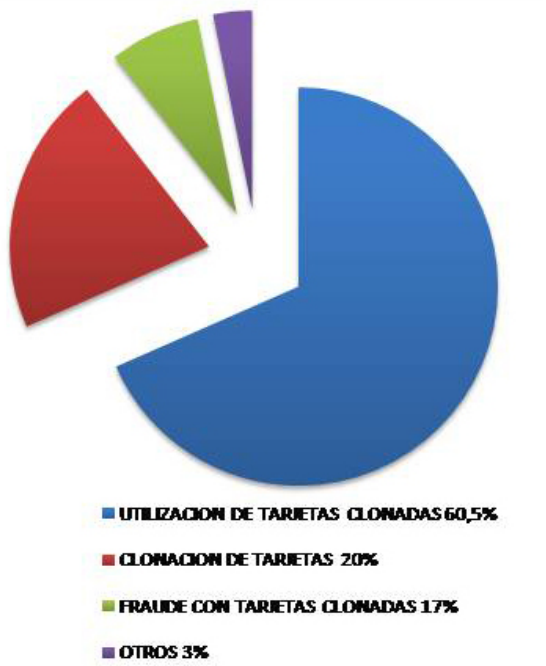
Para hacer frente a esta problemática el Departamento Especializado en la Investigación del Cibercrimen, ha establecido cooperaciones estratégicas con las procesadoras de tarjetas y las entidades Bancarias, para la obtención oportuna y efectiva de la información, permitiendo esta acción reducir en un 95% esta actividad delictual.

El plan estratégico y la coordinación efectiva permitió un operativo de gran envergadura por el Departamento de Cibercrimen, que logró la captura de uno de los delincuentes considerados como el "REY DE LOS HACKERs" **KOLAROV ALEKSEY PETROV.**

01 DE JULIO DE 2015 | HISTORIA DE UN PEZ GORDO QUE EMBAUCÓ AL HOMBRE MÁS RICO DEL MUNDO

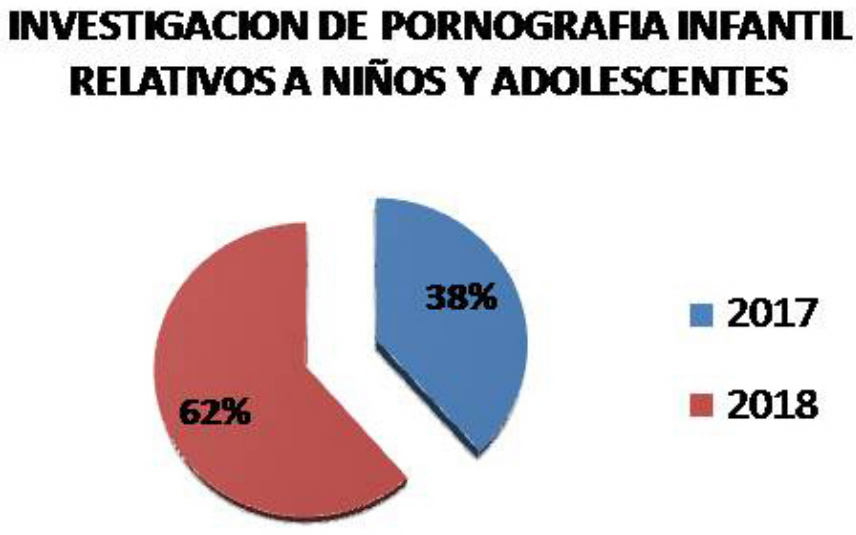
Fraude al magnate de EE.UU.

Publicaciones de la época, con referencia a la detención de los cuatro búlgaros en Paraguay, señalan que el jefe de la red, Kolarov Aleksey Petrov, es un objetivo del Servicio Secreto de los Estados Unidos y de casi todas las brigadas de fraudes bancarios de Europa, luego de haber clonado una tarjeta de crédito de nada menos que el magnate Bill Gates, presidente de Microsoft. En Bulgaria es conocido como e "rey de los hackers".



Fuente: Policia Nacional

A partir del año 2015 el Delito Informático más frecuente es la **"PORNOGRAFIA RELATIVA A NIÑOS Y ADOLESCENTES"**, que lleva un 80% de las investigaciones en el área del Departamento de Cibercrimen, la lucha contra este flagelo mundial se ha enfrentado estableciendo convenios estratégicos a nivel Internacional, como así también grupos de trabajos dentro de la Región de América a través de la Secretaría General de INTERPOL, para que dentro del cada cuerpo policial exista una fluida, oportuna y efectiva comunicación para coordinar las pesquisas e investigaciones contra esta problemática.



Fuente: Policia Nacional

En este 2018, han incrementado la Sextorsión, las Estafas y los Fraudes contra las entidades financieras, a través de Phishing, ataques dirigidos a través de códigos maliciosos utilizando Ransoware y en menor grado los sabotajes a entidades gubernamentales a través de los incidentes de denegaciones de servicios y defacement entre otros, que en mayor grado se generaron parches y no se ha profundizado la instigación pertinente.

- 19/06/2018 EXTRADICIÓN A EEUU, POR ESTAFAS MEDIANTE SITEMA INFORMÁTICOS. Se Trata de Ariel Boiteux, argentino, ingeniero informático de 35 años, quién será extraditado por ser requerido por la justicia de los Estados Unidos, por los cargos de conspiración para transmitir comunicación amenazante en el comercio interestatal y extranjero y otros hechos.
- Esto es gracias a la tarea de inteligencia y la coordinación y cooperación internacional del Departamento de Cibercrimen.

Red internacional de extorsión cibernética

La banda que hacía "trabajos" de brujería cibernética, modalidad conocida en Paraguay como "payé cheto", podría ser encarcelada, como mínimo, por cinco años, aunque la sentencia puede ser aún mayor dependiendo del concurso de penas. La fiscala Irma Llano imputó a cuatro argentinos y dos paraguayos.

Otras tareas importantes para la prevención de los delitos informáticos es el desarrollo de un plan de capacitación y concienciación, llevado a cobo a instituciones educativas en coordinación con el Ministerio del Interior y el Ministerio de Educación, que permite educar a los jóvenes del uso responsable de internet y los peligros que existen en la red.

Seminario sobre "Uso seguro de las redes sociales y delito informáticos", dirigido a Funcionarios del Congreso Nacion

DISERTANTE: Comisario MGAP Abog. DIOSNEL ALARCON, del Departamento Especializ en la Investigación del Cibercrimen

SEMINARIO INTERNACIONAL CIBERDEFENSA, celebrado en el Comando del Ejercito Paraguayo

DISERTANTE: Comisario MGAP Abog. DIOSNEL ALARCON, del Departamento Especializado en la Investigación del Cibercrimen

Por último, señalar que Paraguay firmes en su compromiso en la lucha frontal con la delincuencia trasnacional y en especial del CIBECRIMEN, ha suscrito y ratificado en Agosto del presente año el Convenio de Budapest, para fortalecer la prevención y hacerle frente a los delitos informáticos, mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación, y el aumento de la cooperación entre los Estados y su relación con el sector privado.

ESPALDA JUSTICIERA: DELITOS INFORMÁTICOS

AUTOR: Emerson Wendt

RESUMEN: Este artículo tiene como objetivo analizar los principales desafíos (impuestos) al Estado brasileño frente a los delitos informáticos, considerando la sociedad de consumo en que estamos insertos a su complexidad. Por lo tanto, el foco del desafío está en la comprensión de los nuevos riesgos de la era digital, y, viendo una sistematización de análisis, abordándose a los desafíos impuestos a el Estado brasileño en el enfrentamiento a los delitos informáticos por las dimensiones sociológica – especialmente a través de la (re)comprensión de los (nuevos) riesgos –, estructuralista, técnico y procedimental, además de la dogmática, cada una con su recorte específico. Al final de esta investigación, se concluye que es necesario fomentar búsquedas académicas que digan respecto a el fenómeno de los nuevos riesgos y de los procedimientos aptos a detectar, analizar y descifrar aplicaciones y códigos y/o acciones criminosas complejas en el ambiente informático/telemático.

Palabras-claves: Delitos Informáticos. Desafíos. Estado. Riesgo. Sociedad de Consumo.

Introducción

El objetivo de este trabajo es analizar los principales desafíos (impuestos) al Estado brasileño frente a los delitos informáticos, considerando la sociedad de consumo en que estamos insertados y su complejidad. Tema de difícil respuesta cierta/única y que necesita de constante análisis y debate, en fase de las intensas e inmediatos cambios de esa sociedad, cada vez más tecnológicamente activa y enfocada en medios alternativos, por así decir, de comunicación y de búsqueda de información, de datos, de conocimiento y de bienes a consumir.

Mismo si fuésemos thunderianos, recién desembarcados en el «Tercer Mundo» y de pose de un ojo místico insertado en una «Espada Justiciera» (*Sword of Omens*, en el original), jamás seríamos capaces de proyectar el alcance del que podrá ser el futuro, con excepción de prospecciones basadas en el contexto en que estamos y lo que podría venir, tan solamente[1]. La metáfora parece infantil tal cual lo es seriado *Thundercats*, pero el objetivo es que sea provocativa de reflexión, en el sentido de que no hay visión mágica de futuro y de solución milagrosa, si no de comprensión del momento social en curso y sus aspectos contemporáneos: económico, cultural y político.

En los años 1950/60, cuando se proyectó el embrión de lo que es hoy el Internet, jamás se pensó en lo que ella es hoy, basada en la movilidad, IoT (*Internet of Things* - Internet de las cosas), e interacción a través de redes sociales. Así, no se tiene la seguridad de hasta dónde iremos con los avances tecnológicos en esa área, que tuvo su intenso crecimiento en los últimos 25 años; en el Brasil, específicamente, en los últimos 20 años.

Sin embargo, se permite un análisis, un diagnóstico de las circunstancias actuales en el enfrentamiento a la criminalidad informática, sus aspectos factuales y culturales, dogmáticos y estructurales. O sea, algo centrado en sus aspectos contemporáneos, *v.g.* el aumento del comercio electrónico, y aptos a conducir/proporcionar respuestas.

Mandarino y Canongia, en Brasil (2010) ya alertaban sobre la nueva conformación de la Sociedad de la Información, con fenómenos que van desde una acentuada convergencia tecnológica, para un aumento impar de sistemas y redes de información, cada vez más interdependientes y interconectados, situación potencializada por el aumento creciente de acceso en el Internet (más de 120 millones

de personas en Brasil ya usan/usaron el Internet) y de las redes sociales (Facebook con 89 millones de usuarios en el Brasil) y por los avances de las tecnologías de información y comunicación (TICs). Por lo tanto, el foco del desafío está en la comprensión de los nuevos riesgos de la era digital, con el aumento de las amenazas y de las vulnerabilidades de seguridad cibernética.

Así, como recorte terminológico, usaremos *contemporáneo* o *contemporaneidad*, de Giorgio Agamben (2009) al revés de *posmodernidad* o *modernidad líquida* (BAUMAN, 2001, 2008, 2009). Para Agamben (2009, p. 58-59),

> Pertence realmente ao seu tempo, é verdadeiramente contemporâneo aquele que não coincide perfeitamente com aquele, nem se adéqua a suas pretensões e é, portanto, nesse sentido, inatual. Mas, justamente por isso, a partir desse afastamento e desse anacronismo, é mais capaz do que os outros de perceber e de apreender o seu tempo. [...].
>
> Essa "não-coincidência" não significa, naturalmente, que seja contemporâneo quem vive em outra era, um nostálgico que se senta mais cômodo na Atenas de Péricles, ou na Paris de Robespierre e do Marquês de Sade do que na cidade e no tempo em que lhe coube viver. Um homem inteligente pode odiar o seu tempo, mas sabe que irrevogavelmente lhe pertence, sabe que não pode fugir de seu tempo. [...].
>
> A contemporaneidade é, pois, uma relação singular com o próprio tempo, que adere a este e, ao mesmo tempo, toma distância dele. Mais exatamente, é "essa relação com o tempo que adere a este, por meio de uma defasagem e de um anacronismo". Os que coincidem de um modo excessivamente absoluto com a época, que concordam perfeitamente com ela, não são contemporâneos, porque, justamente por essa razão, não conseguem vê-la, não podem manter seu olhar fixo nela.

Esa contemporaneidad (que) llama la atención por diversidad de actores y diversidad de pensamientos y acciones desde un contexto de uso de las aplicaciones y, principalmente, medios sociales, hasta la cuestión de los intereses sociopolíticos y económicos, estos basados en el consumismo desenfrenado y, por qué no, irresponsable de dispositivos y aplicativos que, al par de la utilidad prometida, tiene más capacidad de extraer informaciones que le son útiles, de lo que cumplir la (f)utilidad deseada. O sea: estamos convivendo com riesgos cotidianamente!

No se tiene la prevención de presentar las respuestas; por el contrario, se propone nuevos cuestionamientos, sin embargo haciéndolo a partir de un contexto dialógico entre la sociedad (de riesgo y de consumo), la estructura que existe para el enfrentamiento de los delitos informáticos y el contexto dogmático penal (y lo que tiene relación con el proceso penal).

Así, visando una sistematización de análisis, abordarse a los desafíos impuestos al Estado brasileño en el enfrentamiento a los delitos informáticos por sus dimensiones sociológicas, especialmente a través de la (re) comprensión de los (nuevos) riesgos, estructuralista, técnico y procedimental, más allá de la dogmática, cada una con su recorte específico, dado el carácter de este trabajo.

Dimención sociológica de los desafios frente a los delitos informáticos

No existe una definición perfecta e indicada al respecto de los delitos informáticos, por lo tanto, se presupone apenas que, o un sistema informático es utilizado como medio, como mecanismo para la práctica de un crimen o contravención, o el sistema informático es algo de conductas típicas, ilícitas y culpables. En ambos casos las conductas son debidamente previstas en la ley[2].

En la verdad, la definición, en sí, no es tan importante como a lo que lleva el poder legislativo a decir que la conducta "x" va ser crimen/contravención y no la conducta "y". Están en juego, por lo tanto, vectores sociales, culturales, económicos, técnicos y políticos, todos formateando valores sobre circunstancias de riesgo.

En ese contexto, las observaciones sociológicas como el riesgo deben ser rescatadas como el principal desafío en esa dimensión sociológica. El primer sentido que se puede dar al riesgo es, «los peligros a evitarse», especialmente en el contexto de las navegaciones exploratorias de los Siglos XV y XVI. Dentro de estos peligros están la inseguridad, la elección, la aventura y las posibilidades de perdida y de ganancia.

Ese contexto de la «navegación» hoy puede ser empleada al sujeto navegar en el Internet, o mejor, en la Web, a *surface* de aquella (la faz visible del Internet, para diferenciarla de la web profunda, llamada de *deep web*.

Para Luhmann (2006) la característica más básica de riesgo es establecer decisiones humanas como raíz de maleficios que vengan a ocurrir en el futuro. El fenómeno de riesgo, al pautarse por la percepción de responsabilidad humana en relación al curso de determinados eventos y procesos, se relaciona íntima e implícitamente con la percepción de la "capacidade do sujeito agir perante o Universo" (MARQUES, 2013, p. 45).

En este contexto, se tiene la concepción substancialista de riesgo, donde este es tenido como algo relacional y contextualizado, o sea, una amenaza de un determinado tipo para un determinado actor (individuo, grupo de ellos, una sociedad o una especie). La otra concepción, de las ciencias sociales, tiene el riesgo como el modo históricamente determinado de identificación y selección de eventos problemáticos que pueden venir a realizarse en el futuro. Se retira, a partir de esa concepción social, el foco de las ocurrencias y de los objetos y los disloca para la propia fabricación, indicando una negociación intersubjetiva (*decisión*) a constituir el riesgo (MARQUES, 2013).

Segundo Machado (2005), los nuevos riesgos, de la era tecnológica, presumen decisiones industriales, específicamente decisiones que tienen su foco en ventajas y oportunidades económicas, basadas en criterios de utilidad (en especial, algo que puede ser consumido y generar lucro). En los estudios sociológicos del fenómeno del riesgo, el desvío tiene relación y depende del proceso de producción de normas, donde una sociología del riesgo indica como riesgos son construcciones en un juego interactivo (crear, recrear).

En las ciencias sociales, así, los riesgos se articulan con valores. Los potenciales daños objetivos y posibilidades de transgresores de las expectativas culturales suscitan reacciones de identificación del riesgo. Se procura legitimar esos valores, socialmente y culturalmente relevantes. Como las personas responden (percepción) al riesgo depende: (a) del contexto de los grupos o redes sociales específicas; (b) raza o género; (c) afectos y reacciones emocionales (ex., binomio gusto/no gusto), y; visión del mundo. Así, la percepción del riesgo es una realidad constituida social y culturalmente (MARQUES, 2013).

La noción de que el riesgo es socialmente construido es realizada en un proceso en que el «gana existencia» reconocida por las personas, depende de agentes y instituciones interactuando en torno de discursos que tornan determinadas amenazas legitimadas mientras tanto riesgos verdaderos (MARQUES, 2013, p. 51).

Posiciones sociales y sistemas simbólicos participan de la definición del riesgo: de lo que él es, como debe ser considerado y cuestionado. Por lo tanto, quien tiene más «poder», tiene mayor posibilidad de, simbólicamente, considerar un riesgo y así delimitarlo. Trayendo el contexto de la discusión académica para la realidad nacional, se tiene ejemplo de la aprobación la Ley 12.737/12, cuyo proyecto fue aprobado en apenas 11 días después de la divulgación de la exposición pública de las fotos envolviendo la actriz Carolina Dieckmann[3].

Así, por la concepción de una perspectiva relativista de construcción social de riesgo[4], a través de contextos sociales y culturales, estos no son cognoscibles fuera de sistemas simbólicos, o sea, no pueden ser tomados como completamente objetivos: riesgos dependen de discursos negociables (v.g., de abogados, de profesionales de TI etc.) y de padrones culturales (v.g., el «padrón» brasileño actual, tendiente a la criminalización).

En este proceso, hay el embate entre «laicos» y «expertos» o *experts* sobre la percepción del riesgo: ignorar, negar o desafiar tales riesgos como formulados por expertos es parte de la vida social. En ese paso, se habla de modulación de las percepciones de riesgo y, (a) como determinados riesgos pueden ser amplificados, a través de la intensificación o atenuación de riesgos, y, (b) se lleva en cuenta las instancias de sociabilidad: individuo, grupos sociales y culturales, medios, agencias gubernamentales, profesionales de relaciones públicas, que son estaciones de los procesos de amplificación de los riesgos (MARQUES, 2013).

Estas estaciones de amplificación pueden tener como función: (a) realizar especie de filtros, (b) realizar mediaciones, y, (c) «opinar» sobre la información corriente a respecto de amenazas específicas. De otra parte, son factores de influencia/partes del proceso de influencia de las estaciones de amplificación en la transmisión de la información: intensidad de atención dada a un determinado asunto (v.g., divulgación sobre nuevo *bug* del milenio); la disputa en torno de las informaciones (v.g., empresas antivirus divulgando relatórios de amenazas); el modo con que las informaciones son dramatizadas (v.g., crimen cibernético generó prejuicio de "x" billones); las connotaciones simbólicas dadas (v.g., conceptos de *hacker*, *cracker* etc.).

Por otro lado, también participan del proceso de amplificación los movimientos de respuesta social a las

informaciones transmitidas (están modulando el riesgo), permitiendo el análisis de nociones (MARQUES, 2013, p. 56):

(a) de «valor de señal»: el riesgo trae consigo no solamente una información a su respecto, mas también una *informatividad*. Relativamente a los eventos cercados de misterio y menos comprensión y percibidos como controlables o completamente generar, tiene que alcanzar un valor de señal al rumbo de los hechos. El valor de señal relaciona los riesgos, sus características, las posibilidades de estas generar incertidumbre y el significado de los riesgos teniendo en cuenta esta incertidumbre.

(b) de estigmatización: la noción sociológica de estigma se aplica también a las tecnologías, productos y lugares. Así, potencializan una respuesta de amplificación por parte de los agentes sociales. Esos elementos estigmatizados son tenidos y tomados como una identidad deteriorada en el plano social, o sea, algo mal, indeseado, que contiene una amenaza y, por lo tanto, marcado (v.g., Windows es inseguro y no necesariamente la forma de su uso). O sea: el riesgo y su impacto en la sociedad no tiene limitación en las medidas objetivas, dependiendo de la transmisión de las informaciones y de las respuestas públicas a esos flujos comunicacionales[5].

En otras palabras, un riesgo transmitido y/o perfeccionado de manera equivocada puede generar un contexto informacional tendiente a lo que es normal en relación al riesgo: eliminación. En el caso del derecho, haciendo una prospección futura, el desafío es comprender ese contexto y, principalmente, tratar de esa expectativa de manera correcta.

Todavía sobre la matización de la normalidad del riesgo, Giorgi (1998) medita que el ideal es *a avaliação racional das eventualidades futuras* y no basada en experiencias pasadas. Así, surgen alternativas: *una*, tratar el riesgo como condición existencial (en este caso, la inseguridad crese con la información: cuanto más se es informado, más claramente se percibe la contemporaneidad de todos los acontecimientos y más claro se tornan los límites para que se hagan el control de los propios acontecimientos, son muchos, y, cada vez más, todo acontece en el presente); *otra*, la inseguridad seria resultado del proceso de civilización y crecería simultáneamente con el riesgo resultante da disminución de control social.

La *tercera* alternativa es la hipótesis, citada por Giorgi (1998, p. 195), de la «segunda modernidade», de la «contramodernidade» o «sociedade de risco», que el autor citado considera patética. Esa sociedad comienza donde fallan los sistemas de normas sociales que habían prometido seguridad. «Estes sistemas falham pela sua incapacidade de controlar as ameaças que provêm das decisões», amenazas que son de naturaleza tecnológica. El procedimiento adoptado es siempre igual: se fijó un principio y se la realidad no se adapta, «se critica la realidad y activase el pánico»:

> Quando nos damos conta do que o modelo de racionalidade que nos foi construído e dava segurança não funciona, recorremos à moral, que, em relação aos princípios, funciona sempre. Mas nem mesmo a moral pode vir em socorro, porque, nas decisões individuais, ela não leva ao consenso, mas produz conflito sobre a avaliação dos riscos e sobre a sua aceitabilidade. Sem auxílio da moral, resta então o pânico (GIORGI, 1998, p. 196-197).

Para Giorgi (1998) con el riesgo se tornan evidentes los límites con que se deparan estos sistemas cuanto a la construcción de vínculos con el futuro, que se efectúa en el «medium» de la probabilidad/improbabilidad, teniendo este «medium» como referencia a incertidumbre, el no saber y la fatalidad.

El autor puntúa que el riesgo es modalidad de distribución de «bads» y no de «goods», pues se basa en la su portabilidad, en la aceptación y no en la certeza de las propias expectativas. En razón de eso, los riesgos no pueden ser transformados en derecho, aunque puedan ser monetarios. Sin embargo, el riesgo sobrecarga el derecho, pues se trata de estrategias de retraso del riesgo y no de estrategias que evitan el riesgo (GIORGI, 1998, p. 198). De otra parte, es necesaria una continua repolitización de los riesgos, aunque sea, para la política, arriesgada tanto la situación que se decide cuanto la que no se decide sobre los riesgos.

Por esa óptica, basada en la concepción (social) del riesgo, los desafíos del Estado brasileño en el enfrentamiento de los delitos informáticos serán de, usar estrategias del enfrentamiento a los riesgos de la era digital, definir correctamente su amplio espectro de necesidades, de defesa y/o de seguridad cibernética. De defesa, del punto de vista estratégico, enfrentando situaciones macro y que digan respecto con los riesgos de carácter global y/o regional en relación a las infraestructuras básicas y de sobrevivencia de la población brasileña; de la seguridad, del punto de vista de

la educación digital – y culturización de comportamientos adecuados frente a los riesgos en internet – y del enfrentamiento específico a la criminalidad cibernética en el contexto del territorio brasileño.

Dimención estructural, técnica y procedimental de los desafíos del enfrentamiento a los delitos informáticos en el Brasil.

Analizada la óptica del desafío bajo el enfoque sociológico, es necesario establecer una directriz para el aspecto estructural, técnico y procedimental. Aquí, por lo tanto, el análisis es desenfocado del rigor técnico de un estudio de situación o diagnóstico y, sí, volteados para determinados parámetros, que son vinculados a partir de desafíos correlativos.

El ámbito de los riesgos en los sistemas informáticos puede ser clasificado en ambientes de defensa cibernética y de seguridad cibernética, como referenciado en el tópico anterior. El enfrentamiento a los delitos informáticos, por definición constitucional, queda a cargo de los sectores de la seguridad cibernética.

Así, del punto de vista estructural, el enfrentamiento a los delitos cibernéticos en el Brasil es hecho por las policías judiciales, Federal y Civil. Aquella, de carácter nacional, principalmente relativamente a las fraudes electrónicas – que envuelven el patrimonio público, como, por ejemplo, los casos de hurtos calificados mediante fraude de los correntistas de la Caja Económica Federal – y los crímenes de «pedofilia» de carácter transnacional[6] Más allá de eso, es de la atribución de la Policía Federal la apuración de infracciones penales de repercusión interestatal o internacional que exijan represión uniforme. La referida actuación también posé previsión legal en el articulo1º, inciso III, de la Ley 10.446/02[7].

Ya las Policías Civiles, por último, cabe la atribución de la investigación crimínale de los demás delitos y, como visto, en algunas circunstancias en atribución concurrente con la Policía Federal. En ese caso, todos los demás delitos informáticos, sean ellos impuros (pueden ser cometidos por los medios tradicionales o por el sistema informático) o puros de informática (solamente pueden ser cometidos por el sistema informático)[8], son de atribución da la Policía Judicial de los Estados, cada una con su estructura y organización.

En el ámbito nacional da Policía Federal hay Servicio de Represión a Crímenes Cibernéticos – SRCC, vinculado a la Coordinación General de la Policía de hacienda – CGPFAZ, responsable por la central de monitorización para «acompañar sospechosos, identificar los ataques a las redes del gobierno y prevenir mayores daños» (G1 BRASIL, 2012). Como se trata de una única organización, los procedimientos y técnicas son fácilmente estandarizados y la gestión es, al menos, factible.

Por otro lado, cuanto a los Policías Judiciales Civiles estatales, tratándose de unidades autónomas en relación a las otras, bien como tener su conducción por gobiernos locales, las políticas de enfrentamiento a los delitos informáticos quedan inviabilizadas sin una centralización y actuación padrón, o, al menos, orientada. Situación semejante se da en relación a los trabajos de forense computacional, la pericia relacionada a los sistemas informáticos, cuja estructura está todavía a quién de las Policías Judiciales civiles de los Estados.

El desafío, así, del punto de vista estructural se diseña en una necesidad de análisis y orientación con parámetros capaces de ser aptos a establecer procedimientos uniformes en relación a los delitos informáticos en todo el Brasil, pues siquiera la mitad de los Estados tiene organizaciones propias para realizar investigaciones criminales relativamente a los delitos informáticos registrados[9]. Los ejemplos y actuación de la Policía Federal son importantes, pero al par de una parametrización, bienvenida, hay necesidad de reconocer las peculiaridades de cada Estado federado, o, en la peor de las hipótesis, de cada región del Brasil.

La creación, en gestión, de un Laboratorio de Combate a los Crímenes Cibernéticos – Ciber-LAB –, a cargo de la Secretaría Nacional de la Seguridad Publica, puede ser una solución eficaz, por lo menos en medio plazo, no sólo para la estructura de investigación, pero el soporte de ella en términos de pericia computacional. El Ciber-LAB puede prevé la utilización de tecnologías y técnicas de análisis de datos para la producción de informaciones con el objetivo de subsidiar acciones de inteligencia y investigaciones criminales, para reducción del índice de crímenes cibernéticos, siendo un Laboratorio con foco y formato específico a ser instalado en todas las especializadas del Brasil. La fundamentación de la creación del Ciber-LAB está en la Ley 12.735/12: «Art. 4º Los órganos de la policía judicial estructuraran, en los términos de reglamento, los sectores y equipos especializados en el combate a la acción delincuente en rede de computadores, dispositivo de comunicación o sistema informatizado».

Bajo el punto de vista técnico, aunque existan varias posibilidades de análisis dada la complejidad inherente[10],

en fase del contexto peculiar de este ensayo se prefiere otro recorte metodológico y centralizar el análisis sobre la comprensión en el, de los aspectos técnicos de las acciones criminales – amenazas y vulnerabilidades – realizadas por los agentes delincuentes en el ámbito de los sistemas de informática.

El primer desafío, en ese aspecto técnico, es encontrar profesionales de seguridad pública capaces de tener un conocimiento de comprensión e investigación de, por ejemplo, todas las técnicas criminales relatadas en estudios de empresas antivirus, como de la Trend Micro (MERCÊS, 2014) y McAfee Labs (COCHIN et al., 2014; CASTILHO et al., 2015).

Mercês (2014) relata que el Brasil ha sido conocido por los caballos de Troya bancarios y que muchas de esas amenazas fueron creadas en el Brasil o, también, por brasileños, visando clientes de bancos locales, o sea, sujetos activos de una relación de consumo. Así, ellos, los agentes criminales, usan varias técnicas para robar credenciales de las víctimas, dentro de ellas: (a) uso de *Bolware* (código malicioso para adulteración de boletos bancarios); (b) adulteración del Sistema del Nombre de Dominio (DNS); (c) uso de falsa ventana en el navegador; (d) uso de extensión maliciosa en el navegador; (e) uso de *proxy* malicioso, inclusive código *proxy* de autoconfiguración (PAC)[11].

También, el desafío puede abarcar la comprensión del que Mercês (2014) llama de «ações no submundo digital", como: credenciales de cuenta de aplicación empresarial; credenciales de tarjeta de crédito; verificadores de número de tarjeta de crédito; generadores de número de tarjeta de crédito; cifradores (partes del código malicioso son cifradas); seguidores de media social (visualizaciones/me gusta); verificadores de credencial de cuenta de servicio online (ej.: PagSeguro, sistema de medio de pago de la Uol en el Brasil); páginas de *phishing*; listas de números de teléfono; módem 3G para envío de *spam* via SMS mensajes) el software para enviar spam por SMS. Todavia segun el McAfee Labs (COCHIN; et al., 2014), los desafíos son ampliados a otros temas/acciones criminales corrientes, como el espionaje cibernético (gubernamental y/o corporativa), el *ransomware* (virus secuestrador), ataques contra dispositivos móviles y contra dispositivos IoT (*Internet of Things* – Internet de las Cosas), entre otros.

Finalmente, en el parámetro procedimental, el desafío es establecer una uniformidad responsable en el combate a los ilícitos penales informáticos. ¿Cómo así? Acciones conjuntas y estandarizadas en relación a los autores, con cambio de conocimiento sobre metodologías, organización estructural y humana para la práctica criminal, más allá de estudios sobre los códigos utilizados para la práctica del crimen (v.g., los citados por Mercês en su trabajo de 2014, p. 5).

Además, esa observación cuanto a la necesidad de producción de conocimiento en el ambiente cibernético ya fue objetivo de críticas anteriores, cuando de la elaboración de estudio sobre la Inteligencia Cibernética (WENDT, 2011). La producción y cambió de conocimientos entre organizaciones de inteligencia de defensa y seguridad es fundamental para resultados efectivos y capaces de generar comprensión de los actos y promover actos tendientes a la mayor seguridad digital.

Estandarizar la forma de acción puede hasta limitar determinados conocimientos, pero puede ser un punto de partida importante para un proceso de combate a los delitos informáticos que se inicia en Brasil. Ejemplo de ese trabajo es el estudio de orientación (manual) realizado por el Ministerio Público Federal en 2006. También, el trabajo propuesto habiendo sido actualizado en frente de la constante manutención de las aplicaciones en el Internet (WENDT; JORGE, 2013). Della Vecchia (2014) también trae a su contribución en términos de pericia digital, fundamental para el suceso de investigaciones criminales relativas a los citados delitos.

Fomentar investigaciones académicas que digan respecto a procedimientos aptos a detectar, analizar y descifrar aplicaciones y códigos y/o acciones criminales complejas en el ambiente informático/telemático es otro desafío impuesto. ¿Si será aceptado por la comunidad académica? Hay esperanza que si!

Así, se percebe que los aspectos relativos a esa dimensión estructural, técnica y procedimental de combate a los delitos informáticos solo dependen de un ojo mágico/espada justiciera y mucho menos de héroes solares como Lion-O, pero sí de organizaciones y diseminación de conocimientos y acciones de *multistakeholders* (múltiplos interesados y envueltos, entre personas y organizaciones).

Dimensión dogmática de los delitos informáticos: ¿necesitamos de más tipos penales?

La última dimensión de la propuesta de análisis de los desafíos relativos a la criminalidad informática tiene que ver con su aspecto dogmático. ¿Necesitamos de más tipos

penales relativos a las conductas que causan daños en uso/actividad de la informática? ¿O apenas necesitaremos revisar los tipos penales existentes y su redacción?

La respuesta no es fácil. Se opta, en este estudio, por la segunda opción y eso tiene una justificación socio política: la aprobación de la Ley 12.737/12, denominada «políticamente» de "Lei Carolina Dieckmann" (LCD), Después de la filtración en el Internet de las fotos íntimas de la actriz.

Varios ya fueron los casos de filtración de imágenes y videos envolviendo famosos, en el Brasil y en el mundo (EGO, 2011)[12], sin embargo el caso de la actriz Carolina Dieckmann tuvo una repercusión mayor, con reportajes producidas por los medios de comunicación. El hecho (envolviendo la actriz) vino a la superficie en el día 4 de mayo de 2012, volviéndose noticia en varios sitios brasileños (TERRA, 2012; OLHARDIRETO, 2012; ZMOGINSKI, 2012a). Todos los sitios destacaban la infiltración de 36 fotos de la actriz, total o parcialmente desnuda, «con partes íntimas expuestas» (TERRA, 2012, s/p.), «los senos fuera, más allá de algunos desnudos frontales» (UOL SP, 2012) y/o que ella fue «víctima de hurto de imágenes de su celular o computador personal» (ZMOGINSKI, 2012a, s/p.).

El sitio IG Gente (2012a) destacaba que «en el área criminal, el caso será encuadrado como hurto y tentativa de extorsión» y todavía «el computador de la actriz pasó por manutención hace poco tiempo y que el contenido pode haber sido copiado». Borges y Weneck (2012, s/p.) buscán reproducir el encuadramiento penal informado por la Policía Civil de Rio de Janeiro: «extorsão qualificada, difamação e furto».

La producción del programa Fantástico (2012) divulgó el acompañamiento, en los bastidores, de la investigación criminal que llevo a prisión de los involucrados y la búsqueda y retención, en el Estado de São Paulo, en la residencia de uno de los sospechosos, Más allá de diligencias en el Estado de Minas Gerais. El subtítulo del reportaje enfoca la «investigación policial que desmontó una *grupo de hackers*, especialistas en *invadir computadores*» (FANTÁSTICO, 2012), en evidente producción de estigmas.

El reportaje también dio enfoque de que en el «Brasil no hay ley específica para crímenes de informática», aunque también se refiera que, «no significa que quien comete crimen virtual quede sin punición. La Justicia se basa en el Código Penal, y en el caso de la actriz los involucrados serán indiciados por hurto, extorsión cualificada y difamación» (FANTÁSTICO, 2012).

Paralelamente la divulgación de la infiltración de las fotos de la celebridad, pocas noticias, como la del O Globo (MACHADO, 2012), buscaban esclarecer como él habría acontecido[13] y cual interpretación adecuada al mismo, aunque tenga atribuido la acción a un ataque de *phishing*[14], el cual si quiera resto tipificado por la redacción de la LCD. De la misma forma, ese análisis procura dar énfasis a datos que causen todavía más temor al lector. WSegundo dados do FBI, *só nos EUA acontecem 31 mil ataques de phishing por mês , ou seja, mais de mil por dia,* e 11 milhões de pessoas tiveram suas identidades digitais roubadas em 2011. No mundo, *187 milhões dessas identidades foram roubadas no ano passado,* segundo a Symantec, e um entre cada 239 e-mails continha malware (MACHADO, 2012, s/p., bastardilla nuestro).

El punto crucial, por así decir, de la actividad mediática vino a los telespectadores y lectores el lunes – 14/05/2012 – con la divulgación, en cadena nacional, de la entrevista de la actriz Carolina Dieckmann al programa de noticias Jornal Nacional. La toma de la noticia llama la atención por el término apelativo en el hablar de la actriz víctima y de los medios de comunicación: «sensación del cuchillo en el pecho» (JORNAL NACIONAL, 2012). La frase fue dicha después de la actriz haber sido cuestionada sobre ver o no «diferencia entre el crimen digital del cuál usted fue víctima y un crimen convencional». La entrevista batió record de audiencia, conforme el F5 (2012), alcanzando la marca de 36 puntos de media, lo que equivale a más de 2 millones de telespectadores[15], más allá de las visualizaciones en los sitios que propagaran la misma (entrevista).

Por otro lado, la entrevista con la actriz demuestra como los medios de comunicación y las personas, por el censo común[16], tratan la substracción de datos en el Internet, o sea, como *robo*.

> «*JN:* ¿Qual foi a sensação de ver essas fotos sendo roubadas e publicadas em sites de pornografia fora do Brasil?».
> «*Carolina Dieckmann:* Pior para mim foi ter sido roubada desse jeito. A pessoa ter tentado tirar dinheiro de mim com uma informação sobre a qual ela não tem direito. Não é dele, é minha» (JORNAL NACIONAL, 2012, bastardillas originales).

También, por esas noticias, se puede concluir que el

censo común desconoce cuál la acción adecuada prevista, ya contingencia da por el derecho para el caso en concreto o circunstancias semejantes.

«*JN:* ¿Que tipo de punição você acha que estas pessoas devem ter? ¿Que roubaram e divulgaram suas fotos?». «*Carolina Dieckmann*: Não sei» (JORNAL NACIONAL, 2012, bastardillas originales).

Esa énfasis mediática acabó por, el decir de Luhmann (2011), irritar el sistema político brasileño y producir más derecho. Los enfoques mediáticos de «invasão de privacidade» (TEIXEIRA, 2012), «roubo» (R7, 2012), la súper exposición de las fotos y visualizaciones por «milhões de pessoas» (PIPOCA MODERNA, 2012)[17], más allá de la publicación de las fotos en un sitio de empresa pública, de Compañía de Tecnología de Saneamiento Ambiental de São Paulo – CETESB (VEJA, 2012; JUNGBLUT, 2012; G1 SÃO PAULO, 2012) pueden haber sido un efecto relevante en la decisión de la Cámara de los Deputados en aprobar Proyecto de Ley que tramitaba sobre el tema.

Conforme destaca La notícia Del jornal O Globo (JUNGBLUT, 2012, s/p.),

> A Câmara aprovou nesta terça-feira projeto que tipifica os chamados crimes cibernéticos, ou praticados via internet. Incluída às pressas na pauta de votação da Câmara, a proposta foi aprovada em segundos e ainda sob o impacto do caso da atriz Carolina Dieckmann, que teve 36 fotos pessoais vazadas na internet no início do mês. O projeto, de autoria do deputado Paulo Teixeira (PT-SP), altera o Código Penal e torna crime entrar indevidamente em e-mail de terceiro, por exemplo, ou roubar via internet dados pessoas de terceiros. As penas variam conforme o tipo de ação. A pena mínima é de detenção de três anos a um ano, mais multa. Esta pena inicial aumenta de um sexto a um terço, no caso de causar prejuízo econômico à vítima. [...]. O deputado Paulo Teixeira disse que o projeto quer coibir crimes como o roubo de dados pessoais e até senhas de banco, via internet.
>
> - O cidadão rouba os dados na internet, as senhas e, a partir daí, comete crimes - disse Paulo Teixeira.
>
> *O presidente da Câmara, deputado Marco Maia (PT-RS), disse que a medida estava sendo votada por causa do caso da actriz.*
>
> - A proposta criminaliza o uso indevido da internet, os famosos crimes cibernéticos. *É a penalização dos de quem invadiu os dados de Carolina Dieckmann* - disse Marco Maia (bastardillos nuestros).

Así, mientras que algunos intentan entender como el hecho realmente ocurrió para ofrecer una opinión técnica cuanto al asunto (CAPPRA, 2012; XIMENES, 2012; SUFFERT, 2012), el Congreso Nacional, en tiempo record, aprueba el proyecto en frente de un hecho insolado, sin mayores discusiones (lo que merecería análisis, en específico, del trámite legislativo). Se destaca que entre la primera divulgación de la infiltración de las fotos de la actriz y la aprobación en la Cámara de los Diputados transcurrieron apenas 11 días.

El desafío en esa dimensión dogmática está, por lo tanto, en el sistema político absorber correctamente las demandas del censo común y la precisión mediática para la producción (o no) de más derecho penal o, inclusive, aspectos que influencian en el procedimiento investigativo.

Consideraciones finales

Se procuro con en este ensayo analizar los principales desafíos (impuestos) al Estado brasileño frente a los delitos informáticos, considerando la sociedad de consumo en que estamos inseridos y su compresibilidad contemporánea. Así mismo, buscando sobrepasar esos desafíos, cada uno con su debido recorte metodológico, por las dimensiones sociológicas – especialmente a través de la (re)comprensión de los (nuevos) riesgos –, estructuralista, técnico y procedimental, más allá de la dimensión dogmática.

Sub la óptica de la dimensión sociológica, se apunta, basada en el concepto (social) del riesgo, que los desafíos del Estado brasileño en el enfrentamiento de los delitos informáticos serán de, el usar estrategias de enfrentamiento a los riesgos de la era digital, definir correctamente su amplio espectro de necesidades, de defensa y/o de seguranza cibernética. En primer caso, de el punto de vista estratégico, a través del enfrentamiento de situaciones macro y que digan respecto con los riesgos de carácter global y/o regional en relaciones a las infraestructuras básicas y de sobrevivencia de la población brasileña; en el segundo caso, de la seguranza, del punto de vista de la educación digital – principalmente, por la culturalización del comportamientos adecuados frente a los riesgos en el Internet – y del enfrentamiento específico a la criminalidad cibernética en el contexto del territorio brasileño.

Por otro lado, por la dimensión estructural, técnica y procedimental, se refiere que: (a) del punto de vista estructural, deseando en una necesidad de análisis y orientación con parámetros capases de ser aptos a establecer procedimientos uniformes en relación a los delitos informáticos en todo el Brasil, pues requiriendo métodos de los Estados que poseen organizaciones propias para realizar investigaciones criminales relativamente a los delitos informáticos registrados, pudiéndose utilizar los ejemplos y actuaciones de la Policía Federal, más allá de la necesidad de reconocer las peculiaridades de cada Estado federal, entonces, de cada región de Brasil; (b) en el aspecto técnico, enfatizándose que el desafío es encontrar profesionales de seguranza pública capases de tener un conocimiento de comprensión e investigación de técnicas criminosas actuales y citadas en estudios de empresas antivirus, además de alcanzar la comprensión de como son las «acciones en el submundo digital», e; (c) en el parámetro procedimental, puntuándose que el principal desafío es establecer una uniformidad responsable, una estandarización referencial, en el combate a los ilícitos penales informáticos.

Finalmente, afirmándose que el desafío en la dimensión dogmática está en el sistema político absorbiendo correctamente las demandas del censo común y la presión mediática para la producción (o no) de más derechos penales o, inclusive, de aspectos que influencien en el procedimiento investigativo de los delitos informáticos.

Proyectar un escenario ideal y utópico del enfrentamiento a los riesgos en los sistemas informáticos y a los delitos informáticos no es lo mismo que esperar soluciones visionarias basadas en instrumentos mágicos, como la mirada en el Thundera, debiéndose pautar en estudios actuales de la construcción social de el riesgo y la percepción del habito digital, a demás de las estructuras cognitivas y procedimentales de prevención y enfrentamiento de la criminalidad informática.

Volviendo a enfatizar, entonces, en conclusión, a el presente estudio, que es necesario fomentar búsquedas académicas que digan respecto a el fenómeno de los nuevos riesgos, a los procedimientos aptos a detectar, analizar y descifrar aplicaciones y códigos y/o acciones criminosas complejas en el ambiente informático/telemático. Son los análisis técnicas y realizadas por experto que pueden conducir para gestiones adecuadas de los riesgos, mismo que posean ser influenciadas y ser efectivos diversos de los proyectados teniendo en vista la percepción social y individual específica de cada usuario de el Internet.

REFERÊNCIAS

AGAMBEN, Giorgio. O q**ue é o contemporânio?** E outros ensaios. Tradução de Vinicius Nicastro Honesko.Chapecó: Argos, 2009.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução: Plínio Dentzien. Rio de Janeiro: Jorge Zahar Ed., 2001.

_____. **Modo Líquido**. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008.

_____. **Confiança e medo na cidade**. Tradução: Eliana Aguiar. Rio de Janeiro: Zahar, 2009.

BRASIL. **Lei nº 10.446,** de 8 de maio de 2002. Dispõe sobre infrações penais de repercução interestadual o internacional que exigem repressão uniforme, para os fins do disposto no inciso I del § 1º do art. 144 da Constituição. Disponible en: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10446.htm>. Acceso en: 05 jul. 2015.

_____. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro Verde:** segurança cibernética no Brasil. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações. Organização Claudia Canongia y Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010.

_____. Lei 12.735, de 30 de novembro de 2012. **Portal da Legislação**. Disponible en: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acceso en: 5 de jul. 2015.

_____. Lei 12.737, de 30 de novembro de 2012. **Portal da Legislação**. Disponible en: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acceso en: 5 de jul. 2015.

BORGES, Waleska; WENECK, Antônio. Caso Carolina Dieckmann: polícia busca suspeitos de divulgação de fotos. **O Globo**, 07/05/2012, às 10h05. Disponible en: <http://oglobo.globo.com/rio/caso-carolina-dieckmann-policia-busca-suspeitos-de-divulgação -de-fotos-4828719>. Acceso en: 29 dez. 2014.

CAPPRA, Ricardo. **Entendendo o caso Carolina Dieckmann X Internet**. 16/05/2012. Disponible en: <http://cappra.com.br/2012/05/16/entendendo-o-caso-carolina-dickmann-x-internet/>. Acceso en: 29 dez. 2014.

CASTILHO, Carlos et. al. **Relatório de McAfee Labs sobre ameaças**. Fevereiro de 2015. McAfee Labs, 2015.

COCHIN, Cedric et al. **Relatório do McAfee Labs sobre ameaças**. Novembro de 2014. McAfee Labs, 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014.

EGO. Ih, vazou! **Veja os famosos que tiveram sua privacidade exposta na rede**. Ronaldinho, Adriano, Blake Lively e mais tiveram imagens íntimas circulando na internet em 2011. Disponible en:<http://ego.globo.com/Fim-de-Ano/2011/noticia/2011/12/ihvazou-veja-os-famosos-que-tiveram-sua-privacidade-exposta-na-rede.html>. Acceso en: 22 dezembro 2014.

FANTÁSTICO. Polícia encontra hackers que roubaram fotos de Carolina Dieckmann. **Rede Globo**, 13/05/2012. Disponible en: <http://glo.bo/XNEVtu>. Acceso en: 29 dezembro. 2014.

F5 - Entrevista de Carolina Dieckmann dá recorde de audiência ao "Jornal Nacional". **Folha de São Paulo**, 16 maio 2012. Disponible en:<http://f5.folha.uol.com.br/televisao/1090789-entrevista-de-carolina-dieckmann-da-recorde-de-audiencia-ao-jornal-nacional.shtml>. Acceso en: 29 dezembro. 2014.

GIORGI, Raffaele de. **Direito, Democracia e Risco.** Vínculos com o futuro. Porto Alegre: SAFE, 1998.

G1 BRASIL. **Polícia Federal inaugura centro contra-ataques cibernéticos**. 04/06/2012, às 13h32. Disponible en: <http://g1.globo.com/brasil/noticia/2012/06/policia-federal-inaugura-centro-contra-ataques-ciberneticos.html>. Acceso en: 15 julho. 2015.

G1 SÃO PAULO. **Hackers postam fotos de Carolina Dieckmann nua no site da Cetesb**. 15/05/2012, às18h33. Disponible en: <http://glo.bo/KZ8gWE>. Acceso en: 29 dezembro. 2014.

IG GENTE. **Vítima de hackers, Carolina Dieckmann presta depoimento em delegacia no Rio**. 07/05/2012a, às 08h44. Disponible en: <http://gente.ig.com.br/2012-05-07/fotos-de-carolina-dieckmann-nua-estao-hospedadas-em-site-ingles.html>. Acceso en: 29 dezembro. 2014.

JORNAL NACIONAL. **'Sensação de faca no peito', diz Carolina Dieckmann sobre fotos**. 14/05/2012. Disponible en: <http://g1.globo.com/jornal-nacional/noticia/2012/ 05/sensacao-de-faca-no-peito-diz-carolina-dieckmann-sobre-fotos.html>. Acceso en: 29 dezembro. 2014.

JUNGBLUT, Cristiane. Carolina Dieckmann: Câmara aprova tipificação de crimes na internet. **O Globo**, 15/05/2012, às 20h25. Disponible en: <http://oglobo.globo.com/rio/carolina-dieckmann-camara-aprova-tipificacao-de-crimes-na-internet-4908289>. Acceso en: 29 dezembro. 2014.

LUHMANN, Niklas. **Sociología del Riesgo**. 3. ed. Ciudad de México: Universidade Iberoamericana, 2006.

_____. **A realidade dos meios de comunicação**. 2. ed. São Paulo: Paulus, 2011.

MACHADO, André. Especialistas explicam como computador de Carolina Dieckmann foi hackeado. **O Globo**, 14/05/2012, às 17h37. Disponible en: <http://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771>. Acceso en: 29 dezembro. 2014.

MACHADO, Marta Rodrigues de Assis. **Sociedade do Risco e Direito Penal.** Uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.

MARQUES, Rodrigo. **Internet:** uma Sociologia de suas Ameaças. 2013. Tese (Doutorado em Sociologia). – Programa de Pós-Graduação em Sociologia e Antropologia - UFRJ, Rio de Janeiro, 2013.

MERCÊS, Fernando. **O Submundo do Crime Digital Brasileiro:** Um Mercado de Aspirantes a Cibercriminosos? Trend Micro, 2014.

OLHARDIRETO. **Confira supostas fotos de Carolina Dieckmann nua vazam na internet**. 04/05/2012, às 23h09. Disponible en: <http://www.olhardireto.com.br/noticias/exibir.asp?noticia=Confira_supostas_fotos_de_Carolina_Dieckmann_nua_vazam_na_internet&id=254187>. Acceso en: 23 dezembro 2014.

PIPOCA MODERNA. **Fotos nuas de Carolina Dieckmann foram vistas 8 milhões de vezes**. Policía já identificou hackers. 14/05/2012. Disponible en: <http://pipocamoderna.virgula.uol.com.br/fotos-intimas-de-carolina-dieckmann-foram-vis tas-8-milhoes-de-vezes-policia-ja-identificou-hackers/176226 >. Acceso en: 29 dezembro 2014.

R7. **Identidade de quem rouba fotos íntimas de Carolina Dieckmann, ainda é mistério**. 13/05/2012c, a las 22h13. Disponible en: <http://rederecord.r7.com/video/identidade-de-quem-roubou-fotos-intimas-de-carolina-die ckmann-ainda-e-misterio-4fb04c256b71c3d8b bc9a310/>. Acceso en: 29 dezembro. 2014.

SUFFERT, Sandro. **Hackerazzi:** Carolina Dieckmann. 16/05/2012. Disponible en: <http://sseguranca.blogspot.com.br/2012/05/hackerazzi-carolina-dickmann.html>. Acceso en: 29 dezembro 2014.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. Coordenadores Alice Bianchini, Ivan Luís Marques y Luiz Flávio Gomes. São Paulo: Saraiva, 2013.

TEIXEIRA, Rodrigo. Advogado de Carolina Dieckmann diz que a "identificação dos hackers" era o que mais interessava à atriz. **Uol Entretenimento**, 14/05/2012, às 17h44. Disponible en: <http://celebridades.uol.com.br/noticias/redacao/2012/05/14/advogado-de-carolina-dieckmann-diz-que-a-identificacao-dos-hackers-era-o-que-mais-interessava-a-atriz.htm>. Acceso en: 29 dezembro. 2014.

TERRA. **Vazam na internet fotos íntimas de Carolina Dieckmann**. 04/05/2012, às 17h25. Disponible en: <http://diversao.terra.com.br/gente/vazam-na-internet-fotosintimas-de-carolina-dieckmann,b9880ce68385a310VgnCLD200000bbcceb0aRCRD.html>. Acceso en: 23 dezembro 2014.

UOL SÃO PAULO. **Supostas fotos íntimas da atriz Carolina Dieckmann caem na internet**. 04/05/2012, às 18h26. Disponible en: <http://zip.net/bvj2VN>. Acceso en: 23 dezembro 2014.

VEJA. **Hackers publicam fotos de Carolina Dieckmann no site da Cetesb**. 15/05/2012, às 18h47. Disponible en: <http://veja.abril.com.br/noticia/entretenimento/hackers-publicam-fotos-de-carolina-dieckmann-no-site-da-cetesb>. Acceso en: 29 dezembro 2014.

WENDT, Emerson. **Inteligencia cibernética**: da ciberguerra ao cibercrime. A (in)segurança virtual no Brasil. São Paulo: Delfos, 2011.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

XIMENES, Pablo. **A verdade sobre as "Técnicas de Invasão" usadas no caso Carolina Dieckmann**. 15/05/2012. Disponible en: <http://ximen.es/?p=621>. Acceso en: 29 dezembro 2014.

ZMOGINSKI, Felipe. Fotos de Carolina Dieckmann vazam na web. **Info Online**, 04/05/2012a. Disponible en: <http://info.abril.com.br/noticias/seguranca/fotos-de-carolina-dieckmann-vazam-na-web-04052012-40.shl >. Acceso en: 23 dezembro 2014.

ZMOGINSKI, Felipe. Saiba como a polícia identificou os hackers do caso Carolina Dieckmann. **Info Online,** 23/05/2012b. Disponible en: <http://info.abril.com.br/noticias/blogs/trending-blog/geral/saiba-como-a-policia-identifi cou-os-crackers-do-caso-carolina-dieckmann/>. Acceso en: 30 dezembro 2014.

NOTAS

[1] *Thundercats fue una serie de animación distribuida en 1983 y que fue al aire en 1985. Tuvo cuatro temporadas. En el Brasil, fue exhibida a partir de 1986, inicialmente en la rede de TV Globo, y después en otros canales. Tiene como personajes principales el joven «lorde» de los ThunderCats, Lion-O, y los ThunderCats Cheetara, Panthro, Tygra, WilyKit, WilyKat y Snarf, originales del planeta Thundera y, durante el viaje, tiene el estado de animación suspensa, pero, al llegar en el «Tercer Mundo», donde las cuatro temporadas se desenrollaron, Lion-O descubre que su cápsula de suspensión no consiguió inhibir su envejecimiento, siendo él un niño en el cuerpo de un hombre y pocediendo la capacidad de utilización de la Espada Justiciera, que le da la «visión además del alcance». Thundercats fue una serie de animación distribuida en 1983 y que fue al aire en 1985. Tuvo cuatro temporadas. En el Brasil, fue exhibida a partir de 1986, inicialmente en la rede de TV Globo, y después en otros canales. Tiene como personajes principales el joven «lorde» de los ThunderCats, Lion-O, y los ThunderCats Cheetara, Panthro, Tygra, WilyKit, WilyKat y Snarf, originales del planeta Thundera y, durante el viaje, tiene el estado de animación suspensa, pero, al llegar en el «Tercer Mundo», donde las cuatro temporadas se desenrollaron, Lion-O descubre que su cápsula de suspensión no consiguió inhibir su envejecimiento, siendo él un niño en el cuerpo de un hombre y pocediendo la capacidad de utilización de la Espada Justiciera, que le da la «visión además del alcance».*

[2] *Sobre la definición de crímenes o delitos digitales/informáticos, ver más en Crespo (2011) y Sydow (2013).*

[3] *Regresaremos a ese punto en la dimensión dogmática de los desafíos.*

[4] *Diferentemente, por la perceptiva realista de el riesgo (en el plano antológico), la natureleza del riesgo es tomada como un dato y las questiones giran en torno de como bien la posibilidad de malefício está identificada y/o calculada.*

[5] *Por la teoria comunicacional, los riesgos no comunicados pueden ser tornados absolutamente insignificantes.*

[6] *El art. 109, V, de la Constitución Federal establece que compete a los Juízes Federales procesar y juzgar «los crimenes previstos en tratado o convención internacionale, cuando, iniciada la execución en el País, el resultado tenga o deve ser ocurrido en el estrangero, o reciprocamente».*

[7] *Dispone el Art. 1º de la Ley 10.446/2012: «En la forma de inciso I del § 1o del art. 144 de la Constitución», cuando hay repercusión interestadual o internacional que exija represión uniforme, podrá el Departamento de policía Federal de el Ministerio de la Justicia, sin prejuício de la responsabilidad de los órganos de seguranza pública arrollados en el art. 144 de la Constitución Federal, en especial de las Policías Militares y Civil de los Estados, procede la investigación, dentro de otras, de las seguientes infracciones penales:*
I – secuestro, cárcel privada y extorción mediante secuestro (arts. 148 y 159 del Código Penal), si el agente es impedido por motivación política o cuando practicado en razón de la función pública ejercida por la víctima;
II – formación de cartel (incisos I, a, II, III y VII del art. 4º de la Ley nº 8.137, de 27 de diciembre de 1990); y
III – relativas a violación a derechos humanos, que la República Federativa del Brasil se comprometió a reprimir en decorréncias de tratados internacionales de que sea parte; y
V – hurto, robo o receptación de cargas, inclusive bienes y valores, transportadas en operación interestadual o internacional, cuando hay indicios de actuación de cuadrilla o bando en más de un Estado de Federación.
V - falsificación, corrupción, adulteración o alteración de producto destinado a fines terapéuticos o medicinales y venda, inclusive por el internet, depósito o distribución del producto falsificado, corrompido, adulterado o alterado (art. 273 del Decreto-Ley nº 2.848, de 7 de diciembre de 1940 - Código Penal). (Incluído por la Ley nº 12.894, de 2013).
VI - hurto, robo o daño contra instituciones financieras, incluyendo agéncias bancárias o cajas eletrónicas, cuando hay indícios de la actuación de asociación criminosa en más de un Estado de la Federación. (Incluido por la Ley nº 13.124, de 2015).

[8] *Si quiere saber más sobre este asunto ir a Wendt y Jorge, 2013, p. 18-20.*

[9] *Conforme a los datos levantados, no más de que 12 Estados poseen organizaciones especializadas y capases de instaurar procedimientos relativamente a los delitos informáticos o, más específicamente, a los crímenes cibernéticos (WENDT, 2014).*

[10] *Dentro los aspectos técnicos también se podria analizar: (a) la categorización de los incidentes en el orden de el Internet, realizados por el CERT.br, CAIS/RNP, Febraban etc.; (b) avaliación de riesgos, acompañamiento de riesgos y gestiones de riesgos; (c) creación, estructuración y funciones de los CSIRTs (Grupos de Respuesta a Incidentes de Seguridad en Computadores), y; (d) governancia y regulación del Internet (Mundial y/o en Brasil).*

[11] *No es objetivo de este trabajo de verificar cada una de las acciones citadas. El objetivo es apenas explicitar la complejidad envolvida para el agente investigador, que debe buscar ese tipo de conocimiento para saber realizar los actos investigativos.*

[12] *Los casos brasileños que más llamarán la atención involucran los jugadores Ronaldinho Gaúcho y Adriano, más allá de los actores Rômulo Arantes Neto, Carlos Machado y André Sigatti (EGO, 2011, s./p.).*

[13] *Excepto el reportaje asinado por Felipe Zmoginski (2012b), que entrevisto uno de los policias responsáblesles por la investigación del caso. Por lo tanto, tal circunstância ocurrió despues de la movimentación del legislativo brasileño y la consecuente aprovabación, por la Cámara de los Deputados, del PL 2.793/2011.*

[14] *Segundo Wendt y Jorge (2013, p. 39), el término phishing puede ser utilizado para definir «el fraude que consistia en el envio de e-mail no solicitado por la víctima, que era estimulada a aceder sitios fraudulentos. Los sitios tenian la intención de permitir el aceso a las informaciones eletrónicas de la persona que se ingresava, como por ejemplo, número da cuenta bancária, tarjeta de crédito, contraseñas, e-mails y otras informaciones personales. [...] Actualmente esta palabra es utilizada para definir también la conducta de las personas que envian mensajes com la finalidad de induzir la víctima a prencher formulários com sus datos privados o instalar códigos maliciosos, capazes de transmitir para el criminoso cibernético las informaciones deseadas».*

[15] *El IBOPE (www.ibope.com.br) posée sistema de medición da audiéncia, en rádio y TV, principalmente relativos a los Estados de São Paulo y Rio de Janeiro (http://www.ibope.com.br/pt-br/conhecimento/TabelasMidia/Paginas/default.aspx). El canal F5 a Folha online (http://f5.folha.uol.com.br/) divulga, constantemente, los índices de audiéncia, com base en las mediciones del IBOPE. Último aceso a los links citados en 25 jun. 2015.*

[16] *El concepto de «senso común» aqui es trabajado en el enfoque del conocimiento con que el hombre común define la vida cotidiana, dando la realidad (MARTINS, 1998, p. 3).*

[17] *El blog Pipoca Moderna, pertenese al grupo Uol, destaca estudio de la ONG Safernet estimando en aproximadamente 8 millones de visualizaciones de las fotos de la actriz Carolina Dieckman en 5 dias.*

LA IMPORTANCIA DEL ANÁLISIS FORENSE DIGITAL, EN LA PERSECUCIÓN PENAL DE LOS DELITOS INFORMÁTICOS

AUTOR: Comisario Danic MALDONADO CÁRCAMO

Ingeniero de ejecución en Informática – Magister en Derecho y Nuevas Tecnologías
Jefe de la Agrupación de Análisis Forense Informático
Brigada Investigadora del Cibercrimen Metropolitana
Policía de Investigaciones de Chile

RESUMEN: La utilización de tecnología como medio comisivo en diferentes acciones constituyentes de delitos en el campo informático, han venido a generar nuevos e importantes desafíos en materia investigativa, desafiando los tradicionales métodos de la criminalística, llevándolo incluso a su punto más alto de exigencia, toda vez que, se requiere mayores niveles de entrenamiento, y la utilización de metodologías formales en el campo de las pericias informáticas, que permitan el manejo adecuado de la evidencia digital, y de esa manera permita asegurar el debido proceso en materia de persecución penal, con un importante énfasis en el respeto a las garantías constitucionales.

Palabras claves: Ciberseguridad; Análisis Forense; Delitos Informáticos

INTRODUCCIÓN

El desarrollo que ha presentado el campo tecnológico en los últimos años, ha traído consigo muchísimos beneficios a toda la sociedad, sobre todo lo relacionado con el acceso a la información, siendo también utilizado ese mismo avancepor delincuentes,para la comisión de delitos en el ámbito informático, en algunos casos las acciones apuntan hacia los sistemas informáticos propiamente tal, y en otras, la tecnología opera simplemente como un medio comisivo.

En ese mismo orden de ideas, las técnicas utilizadas, presentan cada vez mayores grados de sofisticación, lo cual viene a requerir esfuerzos importantes en adiestramiento para poder contrarrestar el flagelo delictivo en este ámbito. En la actualidad, tenemos fenómenos como el ransomware – secuestro de información – y la utilización de criptomoneda como medio de pago. La utilización de botnet, y el permanente desarrollo de código maliciosocon diferentes fines, y en especial aprovechando vulnerabilidades de día cero, han ido generando un verdadero mercado donde se ofrecen diferentes servicios a criminales, cobrando importantes sumas de dinero para la prestación de los mismos.

Y de seguro se nos presentarán nuevos desafíos, considerando algunas áreas como la inteligencia artificial, el internet de las cosas, el avance de las ciudades inteligentes, sin duda, la tecnología constituye un actor más que relevante, además, presenta cambios vertiginosos en lapsos de tiempo muy breves, por lo que, nuestro nivel de conectividad será cada vez más alto, desde actividades domésticas hasta otras muy complejas.

Por lo tanto, contar con personal especializado y dedicado a la investigación en materia informática, juega un rol preponderante a la hora de establecer la responsabilidad que le pueda asistir a un delincuente del área cibernética, de ahí la

importancia de contar con equipos con vastos conocimientos que permitan abarcar la investigación desde su génesis hasta personal con habilidades en lo referido a pericias digitales, aplicando metodologías propias de esta ciencia forense, que permita asegurar el debido proceso, con el debido respetoa las garantías constitucionales existentes.

DELITOS INFORMÁTICOS EN CHILE

Una de las problemáticas a nivel global, dice relación con la poca estadística existente que permita dimensionar de manera precisa los alcances de la cibercriminalidad, existiendo pocos estudios o indicadores que den cuenta de la dimensión del fenómeno en sí, en términos generales, desde el punto de vista de la ciberseguridad, Latinoamérica presenta un estado intermedio de madurez, no siendo Chile la excepción.(Organización de los Estados Americanos y Banco Interamericano de Desarrollo, 2016)

A nivel nacional, existe una tendencia creciente de solicitudes por parte del Ministerio Público – entidad encargada de la persecución penal de los delitos – tanto para la realización de investigaciones relacionadas con delitos informáticos, así como también, la solicitud permanente de pericias especificas en el área, tal como es posible apreciar en el siguiente cuadro.

ANÁLISIS FORENSE DIGITAL

La reforma procesal penal en Chile, implementada en el año 2000, contituyó uno de los mayores cambios impulsados en materia de Justicia Penal en nuestro país, conformándose un nuevo sistema de carácter acusatorio, donde existe una alta valoración de la prueba proveniente de diferentes pericias efectuadas tanto a dispositivos digitales como a sistemas informáticos de tratamiento de información.

Es en ese contexto, la investigación de delitos informáticos a nivel país, ha recaido de manera exclusiva en la Brigada Investigadora del Cibercrimen de la Policía de Investigaciones de Chile, con casi dos décadas dedicados al esclarecimiento de ílicitos en el ámbito cibernético, desarrollando capacidades propias para la realización de pericias informáticas de manera independiente, contanto con profesionales del ámbito informático y electrónico, con conocimientos avanzados en el uso de herramientas especializadas para la forencia digital.

Tabla 1

Solicitudes órdenes de investigar y/o pericias

Delitos	2014	2015	2016	2017
Delitos Informáticos	366	358	468	485
Pornografía Infantil	1949	1626	1846	1778
Abuso Sexual Impropio	47	107	142	209
Propiedad Intelectual	9	15	8	6
Estafas y otras defraudaciones	532	272	240	245
Usurpación de nombre	147	135	109	106

Fuente: BRICIBMET PDI

En la actualidad, el aumento de la capacidad de almacenamiento ha ido presentando un crecimiento significativo, lo cual demanda la renovación y adquisición de tecnología, que busca justamenete acelerar el procesamiento de la evidencia digital. A continuación, es posible apreciar el crecimiento de la demanda anualengigabytepericiados por esta Brigada Especializada.

Tabla 2

Cantidad de GigaByte periciados

Años	2013	2014	2015	2016	2017
Total GB analizados	197.458	212.663	225.330	334.818	440.729
Total Informes	491	409	484	553	674

Fuente: BRICIBMET PDI

CONCLUSIONES

El desarrollo de herramientas cada vez más sofisticadas para la comisión de delitos en el área informática, demandará cada día mayores esfuerzos en el ámbito investigativo desde lo policial, con un fuerte énfasis en la generación de competencias, en manejo de evidencia digital, y su posterior tratamiento del punto de vista forense, considerando el desarrollo permanente de código malicioso de alto nivel, así como la condición transfronteriza que presenta la cibercriminalidad. Por lo que, se deberá generar espacios para el desarrollo permanente de cooperación internacional, mejoramiento del marco regulatorio, y de desarrollo de políticas públicas que vayan en la línea de educar a las personas, para generar una cultura cibernética que nos permita cumplir con el objetivo que se plantea nuestra Política Nacional de Ciberseguridad, que busca contar con un ciberespacio libre, abierto, seguro y resiliente. (Gobierno de Chile, 2017).

Por último, la Policía de Investigaciones de Chile, estratégicamente está enfocando sus esfuerzos para consolidarse como expertos en Chile, en la Investigación Criminal, y de esa manera llegar a convertirse en referentes en la región.

METODOLOGIA ARSO: ANÁLISE DE RISCOS EM SEGURANÇA ORGÂNICA

AUTOR: Silvio Jacob Rockembach
Felipe Scarpelli de Andrade

RESUMO: O estudo teve por objetivo geral desenvolver uma metodologia de análise de riscos voltada para a segurança orgânica. Para seu desenvolvimento, foram identificados os processos informacionais que, sistematizados, estabelecem uma ferramenta de apoio que auxilia a confecção do Plano de Seguraça Orgânica, garantindo eficácia e adequabilidade às medidas e procedimentos necessários para a proteção de qualquer instituição. Nesse sentido, ao considerar que a segurança orgânica deve envolver diversas práticas e rotinas, apresenta-se um modelo de análise de riscos intitulada Análise de Riscos em Segurança Orgância (ARSO), que se propõe a retratar um sistema de aprendizagem contínua, estabelecendo base confiável para que a tomada de decisão possa fornecer respostas compatíveis com o nível de proteção almejado.

Palavras-chaves: Segurança Orgânica. Plano de Segurança Orgânica. Análise de Riscos. Gestão de Riscos. Tomada de decisão.

1. Introdução

Ao se analisar o contexto no qual as organizações estão inseridas, onde há grande volume de informações difusas, ameaças físicas e cibernéticas de distintas ordens, vulnerabilidades institucionais, percebe-se, cada vez mais, a necessidade de se definir estratégias que garantam a sua sobrevivência em uma sociedade de risco (Beck, 2011), balizada na gestão da informação.

O risco é inevitável e presente em todas as situações humanas. Está presente na vida diária das organizações do setor público e privado. Existem muitas definições aceitas de risco (Berg, 2010) a depender do contexto, como seguro, partes interessadas, indústrias, segurança orgânica, processos, estratégico, entre outras.

Por se tratar de estudo do futuro, o conceito comum diz respeito à incerteza dos resultados. A norma técnica ABNT NBR ISO 31000:2018 define risco como sendo o "efeito da incerteza nos objetivos". A ISO/DIS 9003:2015, por sua vez, trata o risco como sendo o "efeito da incerteza num resultado esperado". A diferença conceitual reside no fato de como se caracterizam os resultados. Alguns descrevem o risco como tendo apenas consequências adversas, enquanto outros são neutros, ou, ainda, podem se apresentar como oportunidades.

Dessa forma, este trabalho irá adotar o conceito de que o risco se refere à incerteza que envolve eventos e resultados futuros adversos, traduzidos e classificados por meio de uma expressão de probabilidade e impacto sobre ativos institucionais, tendo como foco principal a segurança orgânica.

A simples probabilidade de ocorrência de um evento indesejado, com a possibilidade de impactos negativos, aconselha que os processos de tomada de decisão, cercados por incertezas, sejam subsidiados por conhecimentos produzidos a partir do emprego efetivo de alguma metodologia estruturada de análise.

É nesse contexto que se insere este estudo, ao apresentar uma metodologia voltada para a Análise de Riscos em Segurança Orgânica (ARSO) que seja, ao mesmo tempo, técnica e exequível.

2. Metodologia de Análise de Riscos em Segurança Orgânica (ARSO)

A metodologia ARSO pode ser traduzida como um instrumento de planejamento, identificação de oportunidades e definição de ações voltadas para a segurança orgânica. Deve ser considerada como um processo continuado de pensar o futuro em termos de riscos, pelo que identifica elementos para a melhor tomada de decisão ao apontar aspectos internos e externos à instituição, como os fatores economicos, sociais, tecnológicos, ativos, ameaças, vulnerabilidades, entre outros.

A Segurança Orgânica (SEGOR) tem por objetivo garantir o funcionamento normal da instituição por meio da implementação de um conjunto de normas, medidas e procedimentos de caráter eminentemente defensivo,voltados para a prevenção e obstrução de ações adversas de qualquer natureza.

Dessa forma, a SEGOR caracteriza-se pelo conjunto de medidas integradas e planejadas com o objetivo de proteger os ativos institucionais, sejam eles tangíveis ou intangíveis.Sendo assim, na busca pela proteção adequada, a análise de riscos surge como um elemento indispensável nesse cenário, dada a sua real capacidade de subsidiar a SEGOR para o tratamento efetivo e eficaz da segurança de recursos humanos, segurança das áreas e instalações, segurança do material, segurança da documentação, segurança das comunicações e informática, segurança das operações e segurança da informação.

A Doutrina Nacional de Inteligência de Segurança Pública (DNISP), visando atribuir eficácia às medidas preventivas de segurança, chama a atenção das instituições para a necessidade de se elaborar um Plano de Segurança Orgânica (PSO), isto é, um documento onde estejam contidos os procedimentos e as normas destinadas a orientar e disciplinar a segurança orgânica sob seus diversos aspectos.

Vale lembrar, porém, que a construção de um PSO deve sempre ser orientada por uma análise prévia de riscos. Afinal, para que a segurança orgânica possa atuar de forma sistêmica, o Plano deve ser construído de tal maneira que exista uma interação e uma complementação recíproca entre as diferentes medidas e procedimentos de segurança que o compõem. A visão proporcionada pela análise de riscos possibilita exatamente a seleção de medidas de segurança adequadas, evitando que o sistemaseja engessado a tal ponto de se tornar lento e ineficaz.

Neste contexto, portanto, a análise de risco (AR) apresenta-se como um elemento essencial na elaboração de um Plano de Segurança Orgânica, pois é por meio dela que se proporcionao equilíbrio necessário entre a segurança,a funcionalidade e o custo.

A elaboração de um PSO sem uma diagnose aprofundada e cautelosa que envolva a identificação, análise e avaliação dos riscos em segurança orgância, conduz, geralmente, à ineficácia, insuficiência ou inadequação das medidas de segurança implementadas.

> O PSO é um documento que visa orientar os procedimentos de interesse da Segurança Orgânica. A adoção de medidas de segurança sem a necessária análise dos riscos e dos aspectos envolvidos, poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação. (DNISP, 2014)

A Análise de Riscos deve, portanto, preceder a elaboração de um PSO, podendo ser definida como o processo por meio do qual se procura compreender a natureza e o grau dos riscos a que os ativos institucionais estão expostos. Entendendo-se risco como a possibilidade de uma ameaça explorar vulnerabilidades para atingir ativos da instituição, causando-lhe impactos e consequências negativas.

Nesse sentido, é fundamental que o profissional responsável pela elaboração de um PSO compreenda que um procedimento de AR é algo obrigatório e que deve ocorrer antes da elaboração de qualquer Plano. O Relatório de Análise de Riscos

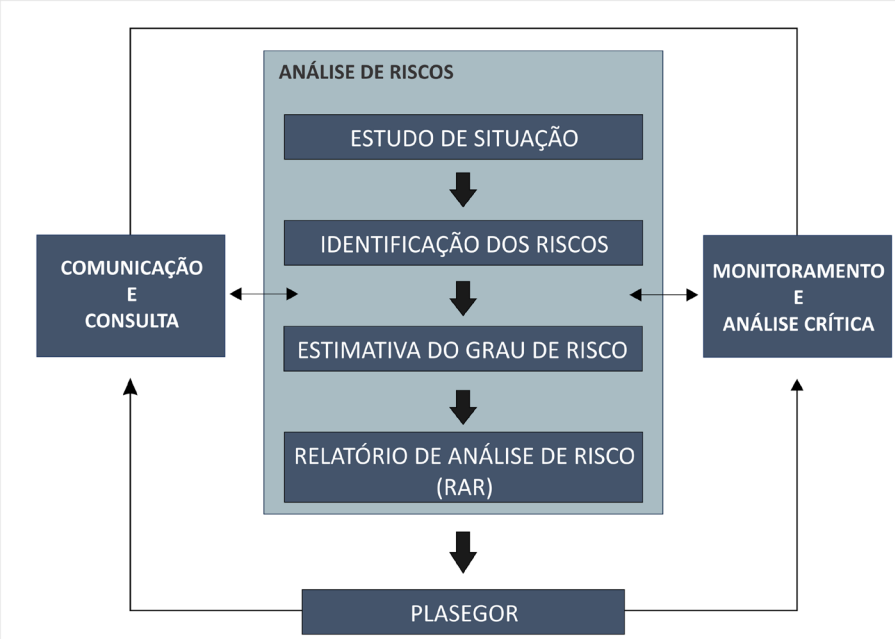
(RAR) auxilia a confecção do Plano de Seguraça Orgânica, garantindo eficácia e adequabilidade às medidas e procedimentos de segurança necessários para a proteção do sistema analisado.

Figura 1 - Visão Geral do Processo de Segurança Orgânica

Fonte: Elaborado e adaptado pelos autores.

Assim, visando o aprimoramento e o desenvolvimento da SEGOR nas instituições, é apresentado a seguir um framework da metodologia intitulada de **Análise de Riscos em Segurança Orgânica (ARSO)**.

Figura 2 - Visão Geral do Processo de Gestão de Risco em Segurança Orgânica



Fonte: Elaborado e adaptado pelos autores.

2.1 Estudo de Situação

O Estudo de situação é a primeira etapa do processo, no qual se realizará um diagnóstico inicial do sistema a ser analisado. Caracteriza-se como um conjunto de métodos que buscam o aprendizado e a uniformização das informações relacionadas à segurança orgânica.

Para tanto, faz-se necessário realizar um extenso e detalhado mapeamento dos ambientes externo e interno do sistema, a fim de identificar os elementos que, correlacionados, dão suporte à valoração do risco. O Estudo de Situação tem como objetivo fornecer apoio para a próxima etapa ("Identificação de Riscos") por meio de técnicas capazes de apontar as ameaças, que podem ser ações naturais e humanas, intencionais ou acidentais; e as vulnerabilidades que coloquem em risco os ativos a serem protegidos pela instituição. (Andrade, 2017)

No Estudo de Situação deve-se, ainda, buscar compreender como a instituição vem tratando e trabalhando o assunto segurança orgânica. Qual é a política, a cultura organizacional, quais são os princípios e as diretrizes institucionais e qual é o nível de maturidade da instituição para lidar com riscos nessa área.

Técnicas simples como o uso de checklists ou memento de verificação, Entrevista Estruturada e o Brainstorming podem auxiliar o trabalho de elaboração do Estudo da Situação. A matriz SWOT[1], por seu turno, auxilia graficamente a visualiação dos pontos fortes, pontos fracos, fraquezas e oportunidades, importantes insumos para a etapa seguinte: a Identificação dos Riscos.

2.1 Identificação dos Riscos

Esta etapa tem por finalidade identificar e avaliar os elementos do risco associados à segurança orgânica, isto é, analisar os ativos, as ameaças, as vulnerabilidades e as consequências negativas decorrentes de eventos indesejados.

Com base nas informações obtidas durante o Estudo de Situação, particularizado e categorizado pela matriz SWOT, o próximo passo é aidentificação e a valoração de cada um desses aspectos estruturantes que compõem o risco.

Importante destacar, portanto, que o método de identificação de risco apropriado dependerá da área de aplicação, ou seja, a natureza das atividades e grupos de risco, a natureza do projeto, a fase do projeto, requisitos regulatórios, requisitos do cliente quanto aos objetivos, resultados desejados e nível requerido de detalhes (Berg, 2010).

Nessa esteira, a valoração dos elementos estruturantes do risco é a etapa mais crítica no processo de avaliação de risco: quanto melhor a sua compreensão, melhores serão os resultados do processo de avaliação de riscos e mais significativas e eficazes serão as sugestões de tratamento.

Para a identificação dos riscos podem ser utilizadas diversar técnicas estruturadas de análise como, por exemplo:

- Brainstorming
- Delphi
- Lista de verificações (Check-list)
- Estrevistas estruturadas
- What if

[1] SWOT é a sigla dos termos ingleses Strengths (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças) que consiste em uma metodologia bastante popular no âmbito empresarial.

2.2 Análise dos Ativos

Para a segurança orgânica, ativo deve ser entendido como todo bem que tenha valor para a instituição, podendo ser tangível ou intangível, como por exemplo, o pessoal, as infraestruturas, as instalações, os materiais, os equipamentos, as informações, a imagem, a reputação institucional, etc.

Nesse sentido, os ativos institucionais são os primeiros itens que se deve identificar, pois a instituição deverá elencar o que se pretende proteger e qual o grau de importância de cada um desses elementos no contexto institucional.

Entender e avaliar o que se quer salvaguardar é fundamental para que se possa determinar as consequências e o grau de impacto negativo caso algo indesejável venha a ocorrer, permitindo, por meio da análise de riscos, subsidiar e orientar o gestor quanto a implementação e a priorização das ações corretivas necessárias para mitigar a possibilidade de ocorrência de eventos futuros indesejados.

Há diversas formas de se classificar um ativo. Aqui, se dará em função de três características: **Substitutibilidade**, **Custo de Reposição** e **Essencialidade**, conforme exemplo:

Tabela 1 – Tabelas de valoração do ativo

	Substitutibilidade	NOTA
Difícil	3	
Média	2	
Fácil	1	

	Custo de Reposição	NOTA
Difícil	3	
Média	2	
Fácil	1	

	Essencialidade	NOTA
Alta	3	
Média	2	
Baixa	1	

Fonte: Elaborado e adaptado pelos autores.

A Substitutibilidade refere-se à mensuração da condição de facilidade/dificuldade em se substituir um determinado ativo: Fácil, Médio ou Difícil. É possível estabelecer faixas por grau definidas quantitativamente, como também proceder à qualificação subjetiva, por meio de votação. Quando ocorrer o segundo caso, quanto mais participantes votarem nesse processo, melhor será a avaliação. Deve-se, por certo, somar a avaliação de todos e dividir pelo número de votantes.

O Custo de Reposição trata, subjetivamente, da valia do ativo e é definido de acordo com os seguintes níveis: Baixo, Médio ou Alto. Assim como na Substitutibilidade, é possível estabelecer um acordo semântico com critérios objetivos, ou seja, criar faixas de valores para cada nível de Custo de Reposição, tornando-o uma análise quantitativa ou semi-quantitativa.

A Essencialidade representa o quanto determinado ativo é considerado indispensável para o cumprimento das funções e missões institucionais, bem como para a consecução dos objetivos estratégicos corporativos, podendo ser graduada em três níveis: Alta, Média e Baixa.

Depreende-se, com base no exposto, que a análise é adstrita à quantidade e qualidade das informações para a sua devida classificação, podendo ser qualitativa, semi-quantitativa, quantitativa ou uma combinação das mesmas, a depender do contexto.

Isto posto, após a determinação dos valores de cada critério para um determinado Ativo, deve-se somar as notas obtidas e dividir por 3.

$$ATIVO = \frac{\sum \text{Substitutibilidade; Custo de Reposição; Essencialidade}}{3}$$

Este procedimento deve ser realizado para cada Ativo, conforme exemplo apresentado a seguir:

Tabela 2 – Exemplo de ativos classificados

ATIVOS	NOTA
Imagem Institucional	**3**
Servidores	**3**
Informações Sigilosas	**3**
Infraestruturas/Materiais e Equipamentos Críticos	**3**
Instalações	**2**
Materiais e Equipamentos	**1**

Fonte: Elaborado e adaptado pelos autores.

2.3 Análise das Ameaças

Ameaças são ações naturais e humanas, intencionais ou não (acidentes), que colocam em risco os ativos a serem protegidos. Referem-se normalmente à situações externas às instituições, mas podem fazer parte do contexto interno, como por exemplo um servidor mal-intencionado ou insatisfeito.

Geralmente, as Ameaças não são variáveis controláveis. No entanto, em certos casos, as ameaças podem ser neutralizadas, ou, ainda, controladas por meio de ações específicas planejadas e executadas no âmbito da Segurança Ativa (SEGAT), que se traduz pelo conjunto de medidas proativas, destinadas a detectar, identificar, avaliar, analisar e neutralizar as ações adversas de elementos, ou grupos de qualquer natureza, que atentem contra a Segurança Pública (DNISP, 2014).

Assim como verificado na classificação dos Ativos, diversas variáveis podem compor o estudo de ameaças, como, por exemplo: capacidade; acessibilidade; motivação; informações estatísticas, dados históricos, podendo a análise ser quantitativa e/ou qualitativa.

Em segurança orgânica, contudo, aconselha-se que a análise de ameaça seja feita utilizando-se o critério qualitativo pelos seguintes motivos: primeiro porque o fato de um determinado risco nunca ter ocorrido não significa que não acontecerá; e segundo porque a experiência demonstra que são raríssimas as instituições que possuem dados consolidados sobre incidentes de segurança ocorridos anteriormente.

Concomitantemente à identificaçãoda ameaça, o grupo de analistas deve relacionar quais seriam as ações adversas possíveis de serem praticadas por ela, tendo como foco o ativo que se pretende proteger.

Abaixo, segue exemplo com as ameaças Organizações Criminosas (ORCRIM) e Servidor Insatisfeito:

Tabela 3 – Análise da Ameaça e Ações adversas (ORCRIM)

ORCRIM	
ATIVO	**AÇÕES ADVERSAS**
SERVIDORES	Execução de servidores
	Ameaça a servidores
	Recrutamento
INFORMAÇÕES SIGILOSAS	Acesso
	Destruição
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Roubo/Furto
	Sabotagem
INSTALAÇÕES	Acesso não autorizado
	Depredação/Vandalismo
IMAGEM INSTITUCIONAL	Execução de servidores
	Ameaça a servidores
	Acesso Info. Sigilosas
	Infiltração
	Sabotagem Infra Criticas

Fonte: Elaborado e adaptado pelos autores.

Tabela 4 – Análise da Ameaça e Ações adversas (Servidor Insatisfeito)

SERVIDOR INSATISFEITO	
ATIVO	**AÇÕES ADVERSAS**
INFORMAÇÕES SIGILOSAS	Vazar Info. Sigilosas
	Destruir
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Sabotagem
	Roubo/Furto
INSTALAÇÕES	Facilitar o acesso
IMAGEM INSTITUCIONAL	Vazar Info. Sigilosas
	Facilitar o acesso as A&I
	Roubo/Furto MatSens

Fonte: Elaborado e adaptado pelos autores.

Após o estudo das ações adversas em que um ativo pode ser impactado, a equipe de analista precisa mensurar a ameaça, pelo que não existe risco sem algo que o enseje.

As ameaças podem ser classificadas e valoradas de diversas formas. Para a metodologia (ARSO), a valoração do nível da ameaça se dará com base na motivação, na capacidade e na acessibilidade que a ameaça possuipara perpetrar ações adversas capazes de atingir um ativo.

Tabela 5 – Tabelas de valoração da Ameaça

	Motivação	NOTA
Alta	3	
Média	2	
Baixa	1	
Não há	0	

	Capacidade	NOTA
Alta	3	
Média	2	
Baixa	1	

	Acessibilidade	NOTA
Alta	3	
Média	2	
Baixa	1	

Fonte: Elaborado e adaptado pelos autores.

A Motivação refere-se a um conjunto de motivos que direciona e influencia a vontade e a conduta de uma ameaça voltada para a prática de uma ação adversa. Sua classificação é: Baixa, Média, Alta ou "Não há" motivação (eventos da natureza por exemplo).

A Capacidade de uma Ameaça significa o nível de habilidade (condições técnicas, quantidade de elementos, recursos e logísticas) que uma determinada ameaça possui efetivamente para executar uma ação adversa, e é definida da seguinte forma: Baixa, Média ou Alta.

Por fim, a Acessibilidade refere-se ao nível de acesso que a Ameaça possui em relação a um determinado ativo, podendo ser mensurado, direta ou indiretamente, de acordo com os seguintes níveis: Baixa, Média e Alta.

Em se tratando de ativo intangível, como por exemplo, a imagem ou a credibilidade institucional, a valoração do nível de acesso (Acessibilidade) deverá ser aferida de forma indireta, devendo-se considerar o nível de acesso da ameaça em relação ao bem que seria atingido diretamente pela ação adversa.

Após a determinação dos valores de cada critério para uma determinada Ameaça, deve-se somar as notas e dividir por 3.

$$\text{AMEAÇA} = \frac{\sum \text{Motivação; Capacidade; Acessibilidade}}{3}$$

Frise-se que o procedimento para a mensuração da ameaça deve se dar de forma individualizada em relação a cada um dos ativos, levando-se em consideração cada uma das respectivas ações adversas possíveis de serem perpretadas pela ameaça considerada, conforme exemplo apresentado a seguir:

Tabela 6 – Tabelas de valoração da Ameaça por Ativo

ORCRIM	
ATIVO	**AÇÕES ADVERSAS**
SERVIDORES	Execução de servidores
	Ameaça a servidores
	Recrutamento
INFORMAÇÕES SIGILOSAS	Acesso
	Destruição
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Roubo/Furto
	Sabotagem
INSTALAÇÕES	Acesso não autorizado
	Depredação/Vandalismo
IMAGEM INSTITUCIONAL	Execução de servidores
	Ameaça a servidores
	Acesso Info. Sigilosas
	Infiltração
	Sabotagem Infra Criticas

SERVIDOR INSATISFEITO	
ATIVO	**AÇÕES ADVERSAS**
INFORMAÇÕES SIGILOSAS	Vazar Info. Sigilosas
	Destruir
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Sabotagem
	Roubo/Furto
INSTALAÇÕES	Facilitar o acesso
IMAGEM INSTITUCIONAL	Vazar Info. Sigilosas
	Facilitar o acesso as A&I
	Roubo/Furto MatSens

Fonte: Elaborado e adaptado pelos autores.

Análise de Vulnerabilidades

Vulnerabilidades são as fragilidades, fraquezas e deficiências existentes no sistema de segurança orgânica que podem vir a ser exploradas por uma ou mais ameaças, ou seja, são as características do sistema de proteção que facilitam, ou oportunizam, a concretização do risco. Por estarem contidas no contexto interno de uma organização, as vulnerabilidades representam o principal elemento sobre o qual o gestor pode atuar para reduzir ou mitigar o risco.

Basicamente, existem duas formas para se reduzir o nível do risco: a primeira é controlar e/ou neutralizar a ameaça; a segunda é minimizar as vulnerabilidades.

Vale lembrar que quando se pensa em Plano de Segurança Orgânica o foco do trabalho deve ser direcionado exatamente para a minimização das vulnerabilidades, lembrando que o controle e neutralização de ameaça não cabe ao segmento da segurança orgânica, mas sim ao segmento de segurança ativa.

Com efeito, quando se trata de gestão de risco em segurança orgânica, é normalmente atuando sobre as vulnerabilidades que uma instituição pode modificar a equação do risco.

Neste contexto, portanto, a análise desta componente é fundamental e deve ser bem detalhada. Para a identificação das vulnerabilidades, a metodologia ARSOrecomenda utilizar um memento de verificação, que pode ser adaptado com base na Entrevista Estrutura e/ou do check list, aplicados na etapa do Estudo de Situação.Deve-se atentar para a necessidade de segmentar o estudo em categorias vulneráveis, a fim de se verificar quais itens, dentro de cada categoria vulnerável, apresentam as fragilidades mais significativas.

O procedimento de elaboração do memento de verificação deve ser adaptado para cada ambiente, minucioso e completo. Por conseguinte, cada categoria mostrará de forma mais clara quais são as falhas, fragilidades e deficiências do sistema institucional de segurança orgânica e qual o grau de vulnerabilidade específico correspondente a cada um dos aspectos que o compõem.

Em resumo, a análise de vulnerabilidades deve ser segmentada em diversas categorias vulneráveis, lembrando que elas podem sofrer alterações em função do ambiente analisado – uma delegacia que possui carceragem deve se preocupar com categorias vulneráveis distintas daquelas que lidam com procedimentos cartorários, por exemplo. Deve-se atentar para o fato de que embora seja possível elencar distintas categorias vulneráveis, o ambiente deve ser analisado de forma sistêmica, considerando todas as categorias como parte integrante de um conjunto, chamado de sistema de segurança orgânica.

A DNISP, por exemplo, identifica as seguintes categorias como vulneráveis: o pessoal, a documentação, as instalações, o material, as operações de ISP, as comunicações, telemática e a informática. Entretanto, a Doutrina não aborda a "Segurança da Informação" como uma categoria autônoma.

Ao considerar que as categorias podem sofrer alterações em função do ambiente analisado, ou da demanda, por vezes, setorizada, bem comoa importancia da "Segurança da Informação" no cenário atual, a metodologia ARSO adota uma visão mais moderna dos aspectos de SEGOR, elencando as seguintes categorias/subcategorias vulneráveis:

1. Segurança dos recursos humanos
2. Segurança das áreas e instalações
3. Segurança da documentação e material
4. Segurança da informação (que pode se dividir em subcategorias)

    4.1. Segurança da informação nos recursos humanos

    4.2. Segurança da informação nas áreas e instalações

    4.3. Segurança da informação na documentação e material

    4.4. Segurança da informação nos meios de tecnologia da informação e comunicações.

Não obstante, frise-se que o objetivo da metodologia ARSO é subsidiar e orientar a elaboração de um PSO e não abrangerá a categoria vulnerável "Segurança das Operações". Embora seja plenamente possível adaptar esta estrutura para a referida análise, a Segurança das Operações merece um estudo a parte ao considerar a sua especificidade, diversidade e

multiplicidade de variáveis envolvidas em uma operação. Dessa forma, embora seja possível adequar esta metodologia para a Sgurança das Operações, recomenda-se um estudo específico para este mister, que precisaria ser construído caso a caso.

Uma vez definidas, cada categoria deverá ter seus itens analisados e distribuídos a fim de se obter uma nota, que poderá variar de 1 a 3, em função dos seguintes critérios: vulnerabilidade baixa – nota (1); vulnerabilidade média – nota (2); e vulnerabilidade alta – nota (3).

Tabela 7 – Tabela de referência para valoração da Vulnerabilidade

VULNERABILIDADE	DESCRIÇÃO	NOTA
Baixa	O controle existe e é perfeitamente adequado e eficiente	1
Média	O controle existe, é adequado, mas a sua eficiência demanda pequenos ajustes na forma de execução	2
Alta	Não existe o controle ou os controle utilizado é complemente inadequado e ineficiente (demanda substituição completa do controle)	3

Fonte: Elaborado e adaptado pelos autores.

A fim de se exemplificar o procedimento, considerar-se-á as seguintes categorias: Segurança dos Recursos Humanos; Segurança das Informações; Segurança das Áreas e Instalações, com suas respectivas avaliações. É importante lembrar que para uma análise completa faz-se necessária a avaliação de todas as categorias vulneráveis da instituição, sob pena de não se ter uma avaliação completa do sistema.

Tabela 8 – Exemplos de valoração da Vulnerabilidade

Segurança dos Recursos Humanos	NOTA
Identificação e classificação, dentro do sistema analisado, das atividades de risco	1
Política de segurança institucional para proteção de membros em situação de risco	2
Educação para o uso de redes sociais	2
Protocolos de atendimento à integrantes em situação de risco	3
Segurança das Informações	NOTA
Classificação de cargos e funções segundo níveis de sensibilidade atende as necessidades atuais de segurança	1
Inteligência participa ativamente dos processos de seleção de pessoal	2
Assinatura do Termo de Compromisso de Sigilo (TCMS)	1
Procedimento normatizado para o credenciamento de segurança	3
Estão definidos itinerários para o fluxo de funcionários	3
Estão definidos itinerários para o fluxo de visitantes	2
A condição de visitante pode ser rapidamente reconhecida por qualquer integrante da instituição	1
Classificação e demarcação física visual dos locais de acesso restrito	3
Procedimentos restritivos quanto a entrada e utilização de câmeras, telefones, pen drives, gravadores nas áreas e instalações	2
Segurança das Áreas e Instalações	NOTA
Todos os andares ou blocos do complexo estão sob o controle da instituição	2
Infraestruturas críticas estão devidamente identificadas	3
Existem regras claras para o acesso , isto é, quem pode entrar, por onde pode entrar, onde pode entrar, quando pode entrar, por que pode entrar, para que pode entrar	3
As barreiras físicas existentes são adequadas e suficientes para cada loca	2
Os itinerários e horários de ronda são alternados periodicamente	1
Existe plano de prevenção e combate a incêndio	3
Estrutura de CFTV cobrem todos os acessos e áreas sensíveis do complexo	2
Os sistemas de CFTV permitem visualização e identificação	1
Os sistemas de CFTV permitem organização, classificação e recuperação rápida de eventos pra análise posterior	1
Existe protocolo para inspeção de materiais, bolsas, equipamentos conduzidos na entrada e saída	2
Existem acessos ao complexo que não estejam sob o controle da instituição	3

Fonte: Elaborado e adaptado pelos autores.

Após a identificação dositens vulneráveis com as suas respectivas notas, deve-se proceder à média encontrada por categoria, ou seja, divide-se o somatório das notas da categoria pelo número de itens checados em cada categoria.

$$\text{Média de Vulnerabilidade por categoria} = \frac{\sum \text{notas itens categoria}}{\text{nº itens checados.}}$$

No caso em tela, tem-se as seguintes notas agrupadas: Segurança dos Recursos Humanos – 2,0; Segurança das Informações – 2,0; Segurança das Áreas e Instalações – 2,09.

O passo seguinte é verificar o quanto vulnerável encontra-se o sistema de segurança orgânica da instituição em termos percentuais por meio do Fator de Vulnerabilidade (FV). Logo, o FV do exemplo citado é a soma das notas de vulnerabilidade dividido pelo número de categorias: 6,09/3 = 2,03. Em termos percentuais, procede-se a seguinte equação: 6,09/9*100 ou 67,67% do índice de vulnerabilidade máxima, que é de 09. Percebe-se, portanto, que a vulnerabilidade é considerável e merece ações para mitigá-la.

Tabela 9 – Exemplos de valoração da Vulnerabilidade

Categoria Vulnerável	% Vulnerabilidade	NOTA	Nota Máxima	VULNERABILIDADE TOTAL
Segurança de Recursos Humanos	32,84%	2	3	67,67%
Segurança das Informações	32,84%	2	3	
Segurança das Áreas e Instalações	34,32%	2,09	3	
TOTAL	100%	6,09	9	

Fonte: Elaborado e adaptado pelos autores.

Por meio da análise das vulnerabilidades decorre a confecção da análise de todas as categorias vulneráveis, cujo resultado servirá de base para a recomendação de ações mitigadoras, ao final do relatório, caso o risco encontrado seja considerado alto, conforme exemplo:

a) **Segurança dos Recursos Humanos:** representa 32,84% da vulnerabilidade total do sistema de segurança orgânica. A melhoria do nível de segurança desta categoria demanda a elaboração de protocolos e a implementação de procedimentos voltados para: a identificação e classificação das atividades de risco; a proteção e assistência de membros em situação de risco decorrente de atividade funcional; a conscientização e orientação sobre o uso e exposição em redes sociais (...)

b) **Segurança das Informações:** representa 32,84% da vulnerabilidade total do sistema de segurança orgânica. A melhoria do nível de segurança desta categoria demanda a implementação de medidas voltadas para: a classificação de cargos e funções segundo níveis de sensibilidade; exigência de credencial de segurança para acesso a áreas e a documentos sigilosos; assinatura de Termo de Compromisso de Sigilo (TCMS) por todos os servidores (...)

c) **Segurança das Áreas e Instalações:** representa 34,02% da vulnerabilidade total do sistema de segurança orgânica. Nesta categoria destaca-se a necessidade de se reduzir as vulnerabilidades por meio de procedimentos relacionados a disposição de barreiras físicas, readequação dos sistemas de CFTV, controle de acesso de pessoas e veículos, identificação das infraestruturas críticas (...)

Mais uma vez, ressalta-se que é na diminuição da vulnerabilidade que deve se concentrar o Plano de Segurança Orgânica, pois é atuando sobre esta componente que o tomador de decisão encontra alternativas capazespararedução o grau de risco.

2.4 Análise das Consequências

A metodologia ARSO considera a avaliação dos efeitos que um determinado ativo venha a sofrer no caso do risco se concretizar, ou seja, a componente consequência influirá no risco final. Esta avaliação é importante, na medida que um determinado ativo pode ser impactado por diferentes eventos adversos, como, por exemplo, ameaça, lesão ou morte. Dessa forma, a análise das consequênciasse dará em função da valoração dos efeitos negativos causados a um ativo pela ocorrência das ações adversas possíveis de serem praticadas por uma ameaça.

Para a valoração do grau de consequência, deve-se considerar as ações adversas identificadas na análise das Ameaças e classificá-las com base nos seguintes critérios:

Tabela 10 – Critérios para valoração da Consequência

CRITÉRIOS PARA VALORAÇÃO DAS CONSEQUÊNCIAS		
GRAU	NOTA	Descrição
ALTA	**3**	Compromete a imagem da instituição, com impactos negativos no ambiente interno e/ou externo. Perda ou abalo da confiança na instituição. Morte, invalidez permanente, risco de vida ou necessidade de tratamento médico hospitalar emergencial. Abala consideravelmente o moral de um número significativo de membros, ocasionando a redução do ritmo e a intensidade das atividades funcionais por eles desempenhadas. Perda ou suspensão da capacidade de execução de atividades essenciais. Compromete segredos estratégicos (desestabiliza). Destruição, dano irreparável ou grave aos recursos financeiros, informacionais, materiais e/ou instalações.
MÉDIA	**2**	Ocasiona um desgaste temporário para a imagem da instituição, mas não chega a comprometer, de uma forma geral, a confiança na instituição. Não há risco de vida imediato; vítimas com necessidade de tratamento médico hospitalar não emergencial. Abala o moral de membros, sem interferir, contudo, no ritmo e intensidade das atividades funcionais por eles desempenhadas. Perda ou Suspensão da capacidade de execução de atividades secundárias (de apoio). Compromete segredos operacionais Dano significativo recuperável, mas oneroso aos recursos financeiros, materiais, informacionais e/ou instalações.
BAIXA	**1**	Não repercute sobre a Imagem da Instituição. Não influencia na confiança na instituição. Não há risco de vida imediato; vítimas com ferimentos leves tratáveis no próprio local ou sem lesões aparentes. Não afeta o moral dos membros. Interferência ou tumulto em processos internos; sem paralisação ou suspensão de qualquer atividade. Não afeta nenhum tipo de segredo institucional. Danos podem ser sanados pela manutenção orgânica.

Fonte: Elaborado e adaptado pelos autores.

A seguir, exemplo aplicado:

Tabela 11 – Exemplo de valoração da Consequência

IMAGEM INSTITUCIONAL			
AMEAÇA	**AÇÃO ADVERSA**	**CONSEQUÊNCIA**	**NOTA**
ORCRIM	Execução de servidores	ALTA	3
	Ameaça a servidores	MÉDIA	2
	Acesso Info. Sigilosas	ALTA	3
	Infiltração	MÉDIA	2
	Sabotagem Infra Criticas	MÉDIA	2
SERVIDORES INSATISFEITOS	Vazar Info. Sigilosas	ALTA	3
	Facilitar o acesso as A&I	MÉDIA	2
	Roubo/Furto Mat.Sens.	MÉDIA	2

Fonte: Elaborado e adaptado pelos autores.

2.7 **Estimativa do Grau de Risco**

Uma vez identificados e mensurados os componentes do risco: os ativos, as ameaças, as vulnerabilidades e as consequências, é possível, por meio de uma equação, obter a valoração do grau de risco.

A correlação dos elementos do risco pode ser traduzida como uma Ameaça que se vale de uma Vulnerabilidade para atingir um Ativo, causando Impactos negativos (Consequências) para a instituição, podendo ser traduzida pela seguinte equação:

RISCO=PROBABILIDADE X IMPACTO

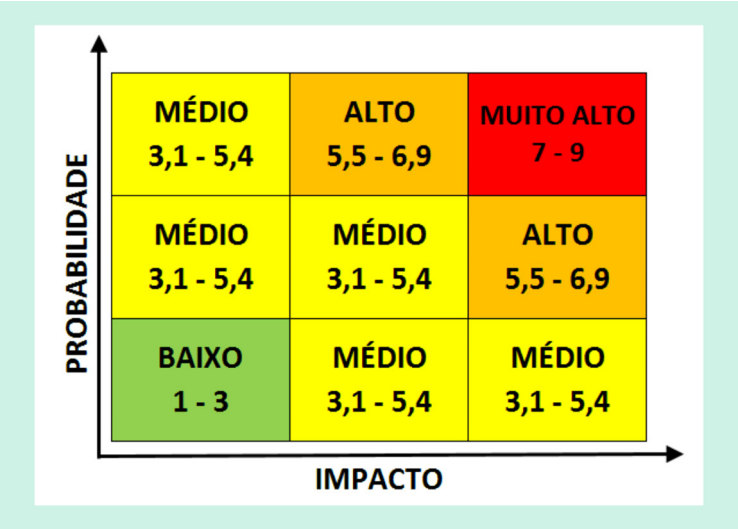
Sendo que:

$$\textbf{PROBABILIDADE} = \frac{\text{Fator Vulnerabilidade} + \text{Nível de Ameaça}}{2}$$

$$\textbf{IMPACTO} = \frac{\text{Ativo} + \text{Consequência}}{2}$$

O grau do Risco é definido de acordo com os critérios utilizados na metodologia e apresentados em uma Matriz de Risco. A Matriz de Risco da metodologia ARSO pode alcançar valor máximo de 9, sendo designado quatro possíveis estágios:**risco BAIXO (1 – 3); risco MÉDIO (3,1 – 5,4); risco ALTO (5,5 – 6,9) e risco MUITO ALTO (7 – 9)**.

Figura 3 – Matriz de Riscos



Fonte: Elaborado e adaptado pelos autores.

O risco pode ser apresentado de forma agrupada, ou seja, com base no valor médio das ameaças, do fator de vulnerabilidade, valor médio dos ativos e valor médio das consequências, por meio da seguinte equação: Risco Agrupado = (nota médias das ameaças + fator de vulnerabilidade) / 2 x (nota média dos ativos + nota média das consequências) / 2.

Tabela 12 – Exemplo de Valoração de Riscos Agrupado

NOTA MÉDIA AMEAÇA	FATOR VULNERABILIDADE	NOTA MÉDIA ATIVO	NOTA MÉDIA CONSEQUÊNCIAS	RISCO	CLASSIFICAÇÃO
2	2,03	2,5	2,5	5	MÉDIO

Fonte: Elaborado e adaptado pelos autores.

A visão global propiciada pelo quadro acima nos conduz a seguinte conclusão analítica: considerando as deficiências e vulnerabilidades encontradas atualmente no Sistema de Segurança Orgânica, verifica-se que os ativos institucionais se encontram expostos a um grau de risco Médio diante das ameaças hoje existentes.

Para o relatório de análise de risco sugere-se, contudo, que os riscos sejam apresentados por ativo, destacando-se asameaças e as consequências. Esse procedimento é o mais indicado, haja vista que o risco depende diretamente da ameaça, sendo possível camuflar uma análise quando feita por meio de médias.

Tabela 13 – Exemplo de Valoração de Riscos Detalhado

IMAGEM INSTITUCIONAL							
PROBABILIDADE			IMPACTO			GRAU DO RISCO	
FATOR VULNERABILIDADE	AMEAÇA	NOTA	NOTA DO ATIVO	CONSEQUÊNCIA	NOTA	RISCO	CLASSIFICAÇÃO
2,03	ORCRIM	2,3	3	Execução de servidores	3	6,4	ALTO
		2,3		Ameaça a servidores	2	5,4	MÉDIO
		2		Acesso Info. Sigilosas	3	6	ALTO
		3		Infiltração	2	6,2	ALTO
		2,3		Sabotagem Infra Criticas	2	5,4	MÉDO
	SERVIDOR INSATISFEITO	3		Vazar Info. Sigilosas	3	7,5	MUITO ALTO
		2		Facilitar o acesso as A&I	2	5	MÉDIO
		1,6		Roubo/Furto Mat Sens	2	4,5	MÉDIO

Fonte: Elaborado e adaptado pelos autores.

Esta forma de representação do pensamento permite que o analista perceba de forma sistêmica, contextualizada e inter-relacionada todos os aspectos essenciais envolvidos em uma análise de risco voltada para subsidiar a gestão da segurança orgânica.

Com base nesta análise de risco é possível apontar quais os itens de categorias vulneráveis devem ser melhorados e priorizados diante dos riscos apresentados, bastando verificar, junto às categorias vulneráveis, aqueles que obtiveram umanota de avalição alta. Portanto, ao identificar quais itens postulados no memento de verificação obtiveram nota alta na vulnerabilidade, o analista terá a capacidade de indicar contramedidas adequadas, capazes de interferir de forma efetiva na equação do risco através da redução dos índices de vulnerabilidade.

Esta análise é muito importante pois servirápara definir e ajustar o grau de rigor das medidas e procedimentos de segurança que deverão compor o Plano de Segurança Orgânica, podendo ser apresentada da seguinte forma:

Tabela 14 – Exemplo de Valoração de Riscos Detalhado e Medidas de tratamento

IMAGEM INSTITUCIONAL							
PROBABILIDADE			IMPACTO			GRAU DO RISCO	
FATOR VULNERABILIDADE	AMEAÇA	NOTA	NOTA DO ATIVO	CONSEQUÊNCIA	NOTA	RISCO	CLASSIFICAÇÃO
2,03	ORCRIM	2,3	3	Execução de servidores	3	6,4	ALTO
		2,3		Ameaça a servidores	2	5,4	MÉDIO
		2		Acesso Info. Sigilosas	3	6	ALTO
		3		Infiltração	2	6,2	ALTO
		2,3		Sabotagem Infra Criticas	2	5,4	MÉDO
	SERVIDOR INSATISFEITO	3		Vazar Info. Sigilosas	3	7,5	MUITO ALTO
		2		Facilitar o acesso as A&I	2	5	MÉDIO
		1,6		Roubo/Furto Mat Sens	2	4,5	MÉDIO
MEDIDAS SUGERIDAS							

Fonte: Elaborado e adaptado pelos autores.

Além da forma de apresentação acima sugerida, há também diversas técnicas estruturadas de análise que permitem visualizar graficamente as causas e as soluções para os riscosidentificados, como, por exemplo, o método de Análise da Árvore de Falhas, o método de análise de Árvore de Evento e o Diagrama de Bow-Tie.

O Método de Análise da Árvore de Falhas (Fault Tree Analysis - FTA) foi desenvolvido por volta de 1960, por W.A.Watson, da Bell Laboratories e aperfeiçoada pela Boeing Corporation. Consiste em um processo lógico e dedutivo que, partindo de um evento indesejado e pré-definido conhecido também como Evento Topo, busca-se as possíveis causas de tal evento. Este evento topo também pode ser definido como um evento indesejado, ou seja, o risco.

Segundo Mentes & Helvacioglu (2011), FTA (Fault Tree Analysis) é uma técnica de análise sistemática e dedutiva orientada graficamente, utilizada para determinar as causas e probabilidade de ocorrência de um determinado acidente indesejada. Outra definição é dada por Ferdous (2007), na qual a FTA é uma ferramenta bem reconhecida para avaliar a segurança e confiabilidade em sistema, desenvolvimento e operação.

Nesse sentido, o FTA procura melhorar a confiabilidade de produtos e de processos por intermédio da análise sistemática de possíveis falhas e suas consequências ao orientar a adoção de barreiras preventivas.

Portanto, o diagrama da árvore de falhas mostra o relacionamento hierárquico entre os modos de falhas identificados. O processo de construção da árvore tem início com a percepção ou previsão de uma falha, uma ação adversa, uma consequência ou até mesmo um risco, sendo possível decompô-lo e detalha-lo até eventos mais simples. Dessa forma, a análise da árvore de falhas é uma técnica top-down, pois parte de eventos gerais que são desdobrados em eventos mais específicos. Hellman & Andery (1995) afirmam que a análise da árvore de falha (FTA) é uma metodologia sistemática e padronizada capaz de fornecer bases objetivas para funções diversas tais como análise de modos comuns de falhas em sistemas, justificativas de alterações em sistemas e demonstração de atendimentos a requisitos regulamentares.

A análise de árvore de evento – ETA (Event Tree Analysis) é uma lógica indutiva que utiliza o método de diagrama para identificar os vários resultados possíveis de um determinado evento inicial. A ETA é comumente usada para identificar as consequências que podem resultar após a ocorrência de um evento potencialmente perigoso (Andrews & Dunnett, 2000). Assim como a ferramenta FTA, esta técnica auxilia na prevenção de que resultados negativos ocorramao fornecer uma avaliação do risco com a probabilidade de ocorrência. A ETA usa um tipo de técnica de modelagem, que ramifica os eventos de um único evento usando a lógica booleana.

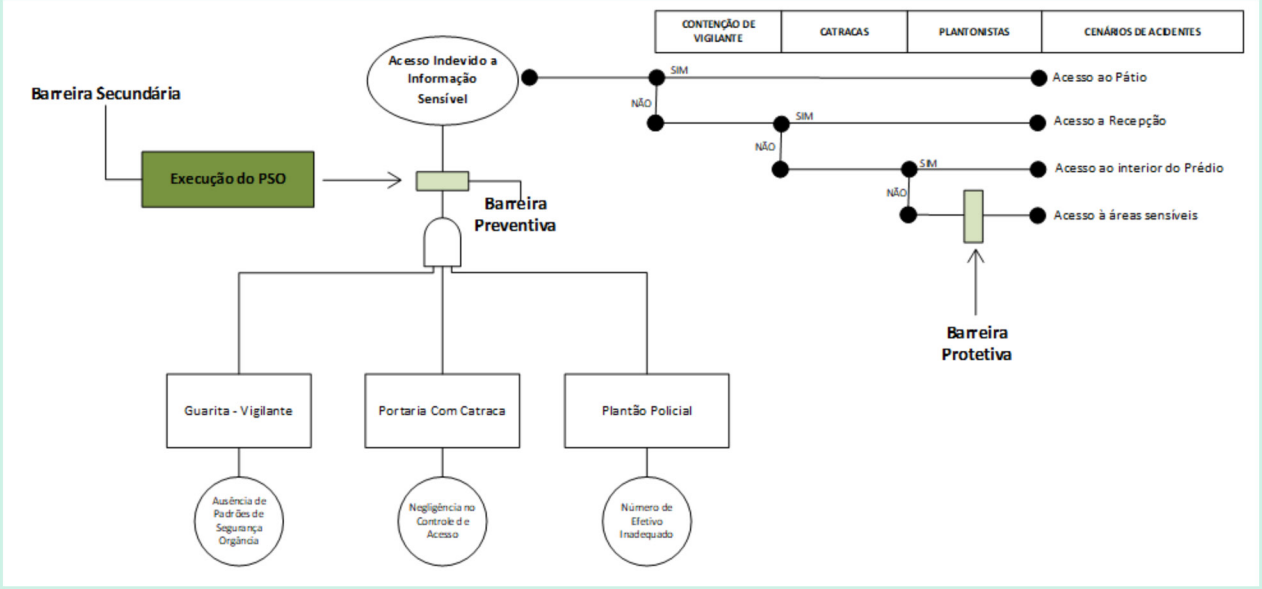
A árvore de eventos começa com o evento inicial de modo que as consequências deste evento percorram um caminho de forma binária. Cada evento cria um percurso no qual uma série de sucessos e falhas ocorrerá onde a probabilidade global de ocorrência para esse caminho pode ser calculada.

Bow-Tie é uma metodologia que transforma de forma esquemática e simples a descrição dos caminhos de um risco, desde as suas causas até as suas consequências. Dessa forma, o foco do Bow-Tie está nas barreiras entre as causas e as consequências. De acordo com Badreddine & Amor (2013), a metodologia é uma ferramenta que descreve todo o cenário de um dado risco graficamente, e propõe barreiras preventivas e de proteção para reduzir a sua ocorrência e mitigar o impacto.

O Evento Topo é posicionado no centro do diagrama, suas causas a esquerda e seus efeitos a direita, permitindo a visualização das relações entre os elementos do sistema modelado. Com efeito, é possível empregar as técnicas FTA e ETA no Diagrama Bow-Tie em seus lados esquerdo e direito, respectivamente.

Figura 4 – Bow Tie com FTA e ETA

Veja o exemplo das técnicas no Diagrama Bow-Tie:



Fonte: Elaborado e adaptado pelos autores.

O produto da análise de riscos, ou seja, o cenário apresentado por meio do grau de riscos e as suas respectivas conclusões e medidas corretivas sugeridas, servirão de base para que o gestor identifique quais ações deverão compor o PSO. A metodologia ARSO é, portanto, uma modelagem que se vale de ferramentas analíticas a fim de assessorar a tomada de decisão no sentido de tornar as medidas de SEGOR adequadas e eficazes, equilibrando o emprego dos recursos e dos meios necessários à proteção efetiva dos ativos institucionais.

Nesse sentido, cumpre ressaltar que a AR, quando realizada no contexto de um PSO, serve para orientar a elaboração de normas de segurança, de planos de contingência, de planos de emergência, elaboração de protocolos de segurança e dos procedimentos. Dessa forma, em havendo necessidade de implementação de controles de segurança e sendo o recurso disponível limitado, há diversas técnicas específicas para a definição de prioridades.

A Matriz GUT, ferramenta que auxilia a priorização de resolução de problemas pode ser útil nesse processo, na medida em que classifica a prioridade de tratamento de cada risco em função da Gravidade (do risco), da Urgência (de redução do risco) e pela Tendência (do risco piorar com rapidez ou de forma lenta).

Dessa forma, caso não seja possível a implementação de todos os controles de segurança ao mesmo tempo, é possível estabelecer uma ordem de prioridade para a sua implementação, utilizando-se para tanto dos parâmetros abaixo especificados:

Figura 5 – Matriz GUT adaptada

Nota	Gravidade/Risco	Urgência	Tendência
4	Muito Alto	Precisa de ação imediata	Irá piorar imediatamente
3	Alto	Urgente	Irá piorar a Curto Prazo
2	Médio	Pouco urgente	Irá piorar a Médio/longo Prazo
1	Baixo	Sem urgência	Não irá piorar

Fonte: Elaborado e adaptado pelos autores.

3.Conclusão

A segurança orgânica deve envolver diversas práticas e rotinas, que, consolidadas, geram, dentre outras medidas, a elaboração de um Plano de Segurança Orgânica. Este Plano, contudo, necessita de suporte informacional para a sua confecção.

Conclui-se que o processo decisório voltado para elaboração de um PSO eficiente depende de assessoramento técnico e emprego de metodologia estruturada capaz de garantir, a partir de uma visão sistêmica, eficácia e adequabilidade às medidas e procedimentos de SEGOR.

Nesse sentido, foi apresentado um modelo de análise de riscos intitulada metodologia ARSO que se propõe, ao analisar um conjunto de componentes correlacionados, retratar um sistema de aprendizagem contínua e uma abordagem holística em relação à gestão estratégica da segurança orgânica.

BIBLIOGRAFIA

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 31000/2009. Gestão de Riscos – Princípios e diretrizes, ABNT, 2009.

_____ NBR ISO/IEC 31010/2012. Gestão de Riscos – Técnicas para o processo de avaliação de riscos, ABNT, 2012.

ANDRADE, Felipe Scarpelli: Análise de Riscos e a Atividade de Inteligência. Revista Brasileira de Ciências policiais. 2017. Disponível em: <https://periodicos.pf.gov.br/index.php/RBCP/article/view/462/311> Acesso em 13 de julho de 2018.

ANDREWS, J.D. and DUNNETT, S.J., 2000. Event-tree analysis using binary decision diagrams. IEEE Transactions on Reliability, 49.

AVEN, Terje. Foundations of Risk Analysis. Wiley, 2012.

*BADREDDINE, A., Amor, N.B.: A Bayesian approach to constructo bow tie diagrams for risk evaluation.**ProcessSafetyand Environmental Protection 91(3), 159-171 (2013).***

BECK, Ulrich. Sociedade de risco: rumo a uma outra modernidade. Tradução de Sebastião Nascimento. São Paulo: Ed. 34, 2011.

BERG, Heinz-Peter. Risk Management: Procedures, Methods and Experiences.RT&A, 2, 2010.

BRASIL. Ministério da Justiça. Doutrina Nacional de Inteligência de Segurança Pública.Brasília, DF, SENASP, 2014.

BRODER, James F. and TUCKER, Eugene. Risk Analysis and the Security Survey. Elsevier, 2012.

Ferdous (2006). Methodology for computer aided fuzzy fault tree analysis. Thesis Submitted To Memorial University of Newfoundland, Canada.

HELMAN, H.; ANDERY, P. R. P. Análise de falhas (aplicação dos métodos de FMEA - FTA). Belo Horizonte: FundaçãoChristianoOttoni, 1995.

LANDOLL, Douglas J. The Security Risk Assessment Handbook. Auerbach Publications, New York, 2006.

Mentes, A. and I.H. Helvacioglu, 2011. An application of fuzzy fault tree analysis for spread mooring systems. Ocean Eng., 38: 285-294.

PEDOFILIA EN INTERNET: CARACTERIZACIÓN DEL GROOMER Y EXPLOTACIÓN SEXUAL DE MENORES A TRAVÉS DE INTERNET.

AUTOR: Comisario Mauricio Araya Ortiz, Psicólogo.

RESUMEN: El trastorno por pedofilia, es la atracción sexual hacia menores de edad y puede traer consecuencias legales adversas cuando estos sujetos intentan concretar sus fantasías en el mundo real o virtual, utilizando internet para proteger su identidad con el anonimato que esta promete. Por lo anterior, comprender los alcances de ésta parafilia y los usos de internet como herramienta para los ellos, es relevante para efectos de proteger a los menores de los depredadores sexuales virtuales.

Palabras claves: Parafilia, boylovers, grooming, P2P, Child Porn.

MARCO LEGAL:

La pedofilia en sí misma, no es un delito, sino un trastorno clasificado dentro de las parafilias, que afecta principalmente la vida sexual y social del individuo y que le puede llevar a efectuar actos ilegales, como es el almacenamiento o distribución de pornografía infantil, el abuso sexual de menores o hasta la violación, los cuales sin son hechos delictuales.

Cuando hablamos de pornografía infantil nos referimos específicamente a la pornografía que involucre menores de 18 años, siendo sancionando en nuestro país todo quien la produzca, comercialice, distribuya, difunda, exhiba, o maliciosamente la adquiera o almacene, cualquiera sea su soporte, lo cual, según lo estipula el Art. 374 bis del Código Penal chileno.

Así también el exponer a una persona menor de 14 años a actos de significación sexual a le hiciere ver material pornográfico (art. 366 quarter, del Código Penal), o bien para procurar su excitación sexual o la de otro, le conminare a realizar acciones de significación sexual, constituye Abuso Sexual.

CONDUCTA PEDOFILA

Para iniciar desde lo básico, comenzaremos por referirnos al significado de la pederastia en nuestra sociedad, para lo cual nos remitiremos al sentido que le otorga nuestro lenguaje. El diccionario de la Real Academia de la lengua española, define la pederastia como un abuso deshonesto cometido contra los niños. Es relevante señalarlo porque la realidad, es un constructo de realidades consensuadas, que se co-construye mediante el lenguaje.

Por otra parte una parafilia es una alteración del objeto sexual, cuyo principal característica es la existencia de repetidas fantasías de tipo excitatorio que persisten por más de 6 meses, pudiendo ser de tipo exclusivo o bien episódico. Algunas de las más conocidas son la zoofilia, necrofilia, la urolagnia y la coprofilia. En ésta, la persona siente excitación o gratificación sexual en presencia del estímulo que le genera dichas emociones.

Estos mismos principios se aplican a la pedofilia, la cual según el **manual CIE 10 (*Clasificación de los trastornos mentales y del comportamiento*)** en el apartado F.65.4, indica que *se trataría de "una preferencia sexual por los niños, nor-*

malmente de edad prepuberal o de la pubertad temprana." Algunos de los afectados sienten atracción únicamente por las chicas, otros únicamente por los chicos y otros están interesados por ambos sexos.

Así también el *"**Manual estadístico de los trastornos mentales,** **DSM V"***, en la sección de parafilias, en el apartado 302.2, describe la pedofilia, indicando que se aplica tanto a los individuos que admiten directamente su atracción hacia pre púberes, (generalmente menores de 13 años) como a aquellos que lo niegan categóricamente, a pesar de haber pruebas objetivas de lo contrario. Sus criterios diagnósticos refieren que el sujeto tenga al menos 16 años o más y sea por lo menos 5 años mayor que el niño, tenga excitación sexual intensa y recurrente con niños pre púberes por al menos por 6 meses y que ha ya cumplido sus fantasías o bien estas generen un malestar importante o problemas interpersonales.

Sin embargo, agrega que si estos sujetos no refieren sentir culpa, vergüenza o ansiedad a causa de los impulsos parafílicos, y estos impulsos no les limitan funcionalmente, y sus antecedentes legales demuestran que nunca ha cedido a esos impulsos, entonces estos sujetos tendrían una orientación sexual de pedofilia y no un trastorno de pedofilia. (Esto se agregó en la última revisión del DSM, ya que en su cuarta versión que rigió desde el año 1994 al 2013, no se hablaba de orientación sexual pedófila).

En este punto se vuelve importante aclarar que el pedófilo no siempre sentirá malestar por sus impulsos como describe el DSM V, sino que como vemos en la actualidad, intentan ser aceptados como una opción sexual más, como es el caso de NAMBLA, sigla de 'North American Man/Boy Love Association' organización formada en 1978, que difunde que el amor entre un hombre y niño es "disfrutable, consentido y hermoso". Actualmente esta asociación se opone a las leyes que fijan una edad de consentimiento para los niños, abogando que estas serian más bien benéficas para el menor.

Para el Dr. Ricardo Capponi, existen dos tipos de pedófilos. El primero de ellos es **ocasional**, en el cual el sujeto, enfrentado a grandes montos de angustia, estrés o estados depresivos buscar pedofilia, pero una vez superado el evento, se normaliza.

El segundo tipo de pedófilo, es exclusivo. Estos sujetos puede subdividirse en 3 tipos: **Romántico, Cínico y Sádico**. El primero de éstos tiene sentimientos de amor por el menor, erotiza las relaciones. El segundo tipo, si bien es similar al anterior, incorpora la manipulación para sus objetivos, y el tercero, busca ejercer el poder sobre el menor mediante el miedo, humillación y sufrimiento. Pueden llegar a ejercerles daño físico.

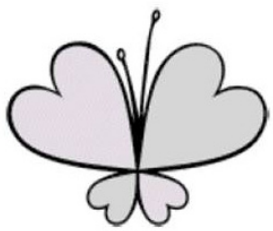
Este tipo de pedófilos en particular, es decir, el exclusivo, es el que puede llegar a establecer redes mediante internet con otros pederastas, buscando pares con intereses similares, logrando así sentirse aceptados y validados, convirtiéndose internet en un lugar virtual donde obtener consejos, compartir historias y por supuesto, material pornográfico infantil.

ACTIVIDAD PEDOFILA ONLINE: Boylovers, Grooming y P2P.

El grupo antes descrito, se autodenomina "boylovers", como una forma de quitarse el estigma social que la sola mención de la palabra pedofilia evoca en el inconsciente colectivo, están plenamente consientes de la ilegalidad de lo que hacen, y del riesgo que corren si son descubiertos, por lo que son sumamente cuidadosos y herméticos en sus actividades, mostrándose reacios a la hora de recibir a un nuevo miembro, el cual solamente será integrado al círculo cercano tras un largo tiempo de compartir y mostrar la devoción a su *'philia'* en los foros, donde protegen su identidad mediante nicks.

(U) LBLogo aka "Little Boy Lover"

(U) GLogo a.k.a. "Girl Lover," Childlove

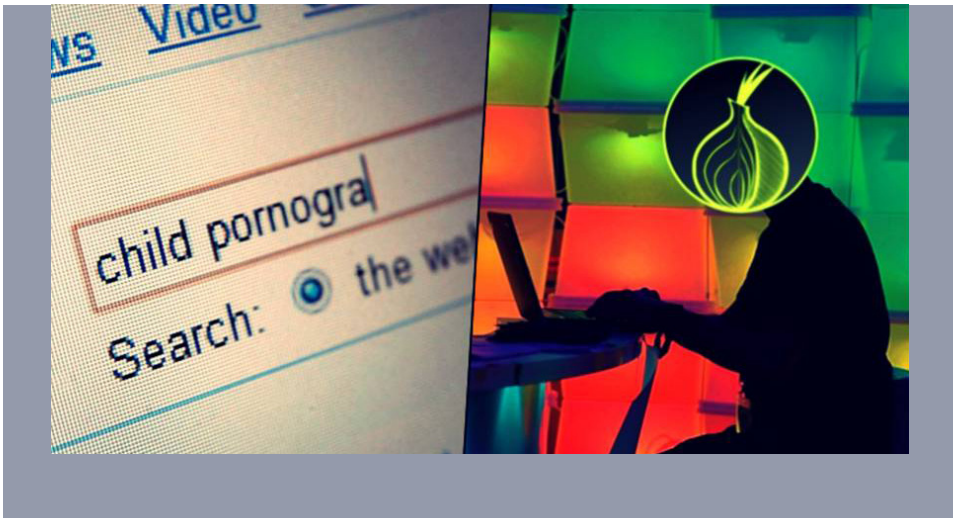


(U) CLogo a.k.a. "Child Lover"

A la observación no participante de los foros y correos electrónicos de un grupo de pederastas, en su mayoría chilenos, se pudo constatar que estos establecen vínculos de amistad, compartiendo sus experiencias emocionales y sexuales con menores. En estos mensajes por correo electrónico, hablan abiertamente de los niños de quienes se han "enamorado", además solicitan consejos y ayuda, convirtiéndose así en una red de apoyo de importancia para el pedófilo. Esta red posee una pseudo-jerarquía, demarcando algunos roles en virtud al nivel de experiencia del pederasta, siendo él o los de mayor experiencia, reconocidos como líderes, cuya opinión es respetada y le son solicitados sus consejos. De esta manera se enseñan estrategias de acercamiento y seducción de los menores, y les animan a actuar y no quedarse en la pasividad.

En la mayoría de estos mensajes y correos, se observan una suerte de códigos de lenguaje que surgen de forma lógica por la necesidad de ocultar su afición, logrando así hablar de modo encubierto de tal forma que solo otro boylover entienda el contenido del mismo. Entre estos se utilizan términos tales como TCQ (chilenismo: ta' como quiere) o PK (peque') para referirse a los niños. Otro termino comúnmente utilizado al relatar sus experiencias es el llamado "factor 'S' o 'SX', utilizado como sinónimo de relación sexual con los menores. Siendo así que para contarle al grupo que se concretó una violación de menor, lo plantearían del modo: "ayer hubo un factor S con PK". Es válido mencionar que todos en el grupo cerrado saben quiénes son los niños-pareja de los demás integrantes, llamados dentro del grupo como SYF, siglas del término inglés 'Special Young Friend' o "amiguito especial."

Otras "palabras código" mediante la cual se identifican en la red para intercambiar material pornográfico infantil, es el término "Pizza de Queso", que viene del inglés "Cheese Pizza", cuyas siglas son CP, las mismas de "Child Porn", por lo tanto, cuando en un foro empiezan a hablar de pizzas de queso, están solicitado material de estas características. Siguiendo el mismo ejemplo, aparece el homólogo en español "Caldo de Pollo". En ocasiones cuando se ofrece o solicita "Caldo de Pollo", obviamente sin hacer mención de la pornografía, se abre un "hilo" donde diversas personas ponen sus correos o números de Whatsapp para ser agregados al grupo, que para un visitante normal al foto, jamás levantaría sospechas. De aquí deriva la importancia de realizar "patrullajes virtuales", a fin de detectar éste tipo de actividades y evaluar si corresponde o no a distribución de pornografía infantil."



Por otra parte el grooming, consiste en un adulto que se hace pasar por niño o adolescente en las redes sociales, salas de chat, o salas de juegos virtuales, que busca establecer contacto y amistad con menores de edad, varones o mujeres, y tras establecer una relación sentimental o de amistad, empezará a pedirle fotografías o videos íntimas de si misma, con las cuales posteriormente podrá extorsionar y amenazar, para así lograr fotografías más explícitas o bien reunirse con la joven y concretar una violación. Este tipo de agresor, que incurre en manipulaciones directas, engaños, tales como falsear su identidad, sexo, historia, etc, y la falta de empatía (desinterés en el bienestar del niño), describe un pedófilo cínico según la clasificación del Dr Capponi. Otra técnica utilizada, esta vez con adolescentes (hefebofilia) sería el de fingir que se es reclutador para una agencia de modelaje, solicitando el curriculum (que incluye colegio, celular, dirección y correo electrónico) y modelar ante la webcam con distintas prendas de ropa y finalmente desnudas, con la promesa de contratarlas como promotoras o modelos. Sin embargo al tener un mayor nivel de madurez, es más posible que estas pidan ayuda cuando empiecen las amenazas o solicitudes sospechosas.

También existen los pedófilos ocasionales, (descritos anteriormente) que cuando son sometidos a grandes montos de angustia o presión, se vuelcan a la pornografía infantil, con grandes montos de culpa. Algunos de estos, tras visualizar y procurar su excitación sexual con el material descargado, sienten grandes montos de culpa, por lo que eliminan el material. Como consecuencia, ante el análisis policial, la totalidad del material se encuentra eliminado. Estos suelen llevar vidas normales con pareja adulta.

Otro punto relevante a señalar, y que se ha verificado tras innumerables pericias efectuadas por los Oficiales Policiales de la Brigada de Ciber Crimen a los equipos computacionales con almacenamiento de material pornográfico infantil, es la existencia de comorbilidad con otras parafilias, siendo los más comunes de encontrar, fotografías o videos de zoofilia, incesto, coprofilia y urolagnia, sadomasoquismo, llegando a encontrar incluso recipientes con orina o heces en sus habitaciones en varias oportunidades.

Finalmente, existen diversas plataformas para realizar descargas de material pornográfico infantil, las llamadas P2P, en donde los archivos son compartidos por la comunidad, entre esas Emule, Torrent, Ares, Gigatribe etc. Vale señalar que para toda actividad en internet es necesario que el ISP (Internet Service Provider), provea una dirección IP, la cual deja registro en los sitios web visitados, permitiendo su posterior rastreo por parte de la Policía. Del mismo modo mientras se realiza la descarga en un programa descentralizado como los P2P, es posible obtener la dirección IP de quien descarga el archivo mientras ésta conectado y compartiendo material. Sin embargo el cómo realizar éstas investigaciones excede los alcances del presente artículo.

REFERENCIA

Asociación Estadounidense de Psiquiatría. (2013). *'DSM V. Manual diagnóstico y estadístico de los trastornos mentales'*. Washington, DC.

Capponi, Ricardo (2002). La pedofilia. *'Mensaje'*. Consultado en http://www7.uc.cl/facteo/centromanuellarrain/download/capponi_pedofilia.pdf.

Organización Mundial de la Salud. (1992). '*CIE-10. Clasificación de los trastornos mentales y del comportamiento'* . Madrid: Ed. Panamericana.

"MODIFICANDO O PARADIGMA INVESTIGATIVO"

AUTOR: Katia de Mello Dantas

RESUMO: Embora a tecnologia tenha permitido grandes avanços na sociedade, isso não ocorre sem desafios. Abusos sexuais isolados, passam a contar com o apoio de comunidades de abusadores sexuais que intercambiam informações e imagens com velocidade ímpar; e crianças são constantemente vitimadas a cada vez que uma imagem é compartilhada. Grandes volumes de materiais de abuso infantil são apreendidos todos os dias, e investigar esses crimes pode ser complicado, trabalhoso e traumatizante para o investigador. Este artigo pretende discutir a importância de mudar o paradigma investigativo para centrar o foco na vítima, de forma a permitir não só a judicialização do infrator, mas a restituição psicossocial da vítima e de seus direitos. O artigo ressalta ainda a importância de se utilizar de ferramentas tecnológicas existentes para aprimorar o processo de identificação de vítimas através da automação e de ferramentas de inteligência artificial, com um enfoque em permitir maior proteção tanto as vítimas como os investigadores envolvidos no processo, a fim de minimizar o chamado "estresse traumático secundário" ou "trauma vicário".

Palavras-chaves: material de abuso sexual infantil; pornografia infantil; inteligência artificial;ferramentas forenses; tecnologia; abordagem centrada na vítima;estresse traumático secundário; trauma vicário.

Modificando o paradigma investigativo: atenção à vítima e cuidado com o investigador

O advento da Internet e outros avanços tecnológicos recentes, trouxeram desenvolvimentos significativos nas áreas científicas e sociais, na maneira como nos comunicamos, como conduzimos investigações e muitas outras áreas. A disponibilidade e acessibilidade à Internet continuam a melhorar, trazendo crescimentosconstante e significativo do número global de usuários da Internet –hoje mais de 50% da população mundial utiliza ativamente os serviços da Internet.[1] Em 2018, o número de usuários da Internet finalmente ultrapassou a marca de 4 bilhões de usuários em todo o mundo,[2]sendo que 3 bilhões destes fazem uso das chamadas mídias sociais.[3] Somente na América Latina, 67% da população acessa ativamente a Internet, um aumento de 2.318% desde o ano 2000,[4] crescendo constantemente nos últimos anos.

E o número de crianças fazendo uso da internet não é menos surpreendente. Embora a porcentagem exata de crianças que são usuários da Internet não seja conhecida, um estudo recente do Fundo das Nações Unidas para a Infância(UNICEF) e projeções da União Internacional de Telecomunicações (UIT) estimam que uma em cada três crianças está on-line, a maioria delas em países em desenvolvimento.[5]Em particular, pesquisas mostram que os jovens estão acessando as tecnologias de informação e comunicação (TIC) em taxas mais altas do que os adultos - 70% dos jovens (com idades entre 15 e 24 anos), quando comparados a 48% dos adultos.[6]

Enquanto a maioria das crianças e adolescentes usa a Internet para fins educacionais (para aprender algo novo, para estudar, entre outros),[7] crianças e adolescentes vêm usando as mídias sociais em uma idade cada vez mais jovem. O acesso às redes sociais tem aumentado significativamente, em parte facilitado pelo aumento do uso da internet através de smartphones (atualmente usado por 68% da população mundial,[8]e de forma exclusiva por 49% da população pesquisada no Brasil[9]). E as crianças não são uma exceção;1 em cada 5 crianças (23%) tem conta em alguma rede social entre 8 e 11 anos, e 7 em cada 10 (74%) já são usuários ávidos destas mesmas redes sociais antes dos 13 anos de idade.[10]Como se a violação da regra de idade mínima imposta pela maioria das redes sociais para seus usuários – 13 anos de idade – não fosse suficientemente inquietante, o acesso à Internet dessas crianças tem se tornado cada vez mais pessoal, mais privado e menos supervisionado.[11] Isso é particularmente preocupante

quando se consideraque há cerca de 750.000 predadores online a qualquer dado momento.[12]

A exploração sexual infantil online pode assumir muitas formas, mas uma das mais comuns, e que resultam em evidência marcante de tal abuso online, é legalmente conhecida em muitos países como "pornografia infantil". Vale a pena mencionar os esforços de organismos internacionais em construir uma nomenclatura mais apropriada em torno do termo, que vem sendo internacionalmente referida como material de abuso sexual infantil (conhecida CSAM, por suas siglas em inglês e assim referida daqui por diante).[13] Mais do que uma simples imagem ou vídeo, esse material é a documentação de abuso sexual real, o qual possui finalidades múltiplas para os abusadores sexuais de crianças, tais como: gratificação sexual; como "munição" para chantagear a criança em submissão adicional; ou mesmo para garantir acesso a fóruns ou grupos de notícias formados por outros abusadores.[14]

O volume preciso de CSAM circulando na Internet não é conhecido, mas estimativas indicam que os números são enormes e estão crescendo. Em 2016, os membros do INHOPE receberam 8.474.713 relatórios confirmados de CSAM, com 83% das vítimas sendo do sexo feminino, 40% das vítimas sendo pré-púberes e 1% abaixo dos 2 anos de idade.[15] Nos Estados Unidos, o *Cybertipline*,linha de denúncias gerida e coordenada pelo *National Center for Missing and Exploited Children*(Centro Nacional de Cidadelas para Crianças Desaparecidas e Exploradas ou NCMEC, como é conhecido por sua sigla),recebeu mais de 27 milhões de denúncias por suspeita de exploração sexual infantil online entre 1998 e 2017.[16] Segundo o NetCleanReport2016 [Relatório NetClean 2016], muitos policiais relataram que um caso padrão de investigação pode incluir entre 1 e 3 terabytes (TB) de dados, representando de 1 milhão a 10 milhões de imagens e milhares de horas de material de vídeo.[17]

Abusadores sexuais infantisutilizamas tecnologias de informação e comunicaçãonão somente para organizar, manter e aumentar o tamanho de suas coleções, mas também para intercambiar informações sobre como melhor abordar uma vítima, como evadir detecção por policiais, e até mesmo como uma maneira de legitimar seus desejos,haja vista a "normalização" de seus desejos e comportamentos que grupos de abusadores online pode oferecer. No entanto, para aceder a fóruns e redes da Internet que permitam dito intercâmbio e compartilhamento de interesses, desejos e até mesmo experiências, muitas vezes se faz necessário o compartilhamento de novos materiais,estratégia que tem como objetivo desencorajar a infiltração de agentes policiais encobertos.[18]Atualmente, poucas agências policiais no mundo podem compartilhar CSAM como tática de agente infiltrado, sendo a Austrália um exemplo de país que permite o uso de tal recurso.[19]

Embora nem todos os infratores tenham natureza sofisticada, crescentemente os infratores têm buscado se afastar da web indexada, conhecida como "clear web", recorrendo a técnicas de anonimização e criptografia, o que tem tornado a investigação destes crimes cada vez mais tecnicamente sofisticada, desafiadora e demorada. Adicionalmente, a simples posse e/ou distribuição de CSAM costumam ter sentenças geralmente mais baixas do que outros crimes relacionados, como corrupção de menores ou abuso/exploração sexual infantil. Neste cenário, a identificação visual das vítimas e/ou infratores se faz importante para garantir não somente sentenças maiores, mas a diminuição da produção de tais materiais.No entanto, é sabido que a identificação de agressores somente pelas imagens é tarefa árdua, pois os CSAMs provavelmente conterão apenas a face das vítimas em vez do infrator a fim de, justamente,evitar a detecção.

Um estudo recente descreveu os desafios enfrentados durante as investigações de CSAM, como a evolução da tecnologia e as habilidades técnicas demonstradas pelos abusadores; aumento do volume de dados a serem investigados; gestão de laboratório e comissão de casos; recursos limitados disponíveis; manipulação, análise e relatórios de evidências; cooperação insuficiente; dificuldades na realização de identificação das vítimas; condições estressantes de trabalho; e operações/estruturas legais não padronizadas.Desta forma, infere-se que a investigação deste delito exige um alto nível de coordenação e cooperação.[20]

Dado o alto nível de treinamento necessário para realizar investigações avançadas, a coordenação entre as distintas forças policiais atuando em um mesmo país se faz altamente necessária. Globalmente, algumas agências de policiais optaram por dividir as tarefas internamente para garantir que diferentes tipos de abusadores fossem atingidos pelas distintas táticas de policiamento. No Reino Unido, por exemplo, as forças policiais locais são encarregadas de investigar infratores tecnologicamente menos sofisticados, enquanto o *ChildExploitation and Online Protection Centre*(Centro de Exploração Infantil e Proteção Online, ou CEOP) e a *National Crime Agency* (Agência Nacional de

Crimes ou NCA) investigam casos mais complexos, como redes internacionais, streaming ao vivo, crime organizado e CSAM encontrados na Dark Net.[21]Nos Estados Unidos, a coordenação entre as distintas forças policiais – tanto no âmbito federal quanto no âmbito local –se deu por meio das*Internet Crimes Against Children Task Force* (Forças Tarefa contra Crimes Cibernéticos Contra Crianças, ou ICACs), uma rede nacional altamente treinada e capacitada em investigação de delitos cibernéticos, composta por 61 forças-tarefa coordenadas que representam mais de 4.500 agências policiais e promotores do âmbito federal, estadual e local.[22]

Do ponto de vista tecnológico, cada vez mais as agências policiais em todo o mundo estão percebendo os benefícios de promover uma mudança de paradigma em suas investigações, afastando-se de uma abordagem centrada no abusador sexual para uma abordagem mais centrada na vítima. Esta mudança de paradigma para uma abordagem centrada na vítima, além de oferecer uma oportunidade de reduzir a disponibilidade de CSAM online, haja vista que atacaa produção de CSAM em sua fonte e não apenas sua distribuição, permite a identificação e recuperação de vítimas de abuso sexual infantil, oferecendo a essas vítimas uma chance de reinserção psicossocial e reabilitação, sem abdicar daidentificação e condenação da pessoa responsável pelos atos. No mais, ao encontrar indícios de produção de CSAM, permite-se ainda a condenação por delitos conexos que aumentem a pena do abusador e a possibilidade de sua condenação dada a vinculação inequívoca com o delito.

A abordagem centrada nas vítimas e a identificação de vítimas pode ainda ter um aspecto restaurativo e preventivo, permitindo a possibilidade de minimizar a redistribuição de materiais já identificados. Hojeem dia, grandes as principais redes sociais – comoGoogle e Facebook, por exemplo - já fazem uso de softwares de reconhecimento facial e tecnologias de hash robustas[23], como o Photo DNA[24] e o F1[25] (para vídeos), que impedem a disseminação nestas redes deste material, impedindo re-vitimizaçãode vítimas já identificadas. Além do aspecto restaurativo, do ponto de vista do direito das vítimas, o uso destas tecnologias permite ainda a identificação mais rápida de alvos futuros, ou seja, a identificação de usuários que possuem tais materiais e os estejam compartilhando.Considerando as enormes cifras de CSAM apreendidos a cada operação, depender apenas dos sets de valores *hash* existentes e a produção de novos materiais que continuarão a circular, a identificação de vítimas tem um fator preventivo importante.[26]

Nos Estados Unidos, o Programa de Identificação de Crianças Vítimas (CVIP) do NCMEC processou mais de 236 milhões de arquivos de CSAM apreendidos por agências policiais desde sua criação em 2002 e, desde então, aproximadamente 14.500 crianças foram identificadas por estas agências policiais em cooperaçãocom o NCMEC.[27]No Reino Unido, uma resposta mais coordenada ao CSAM começou em 2014, com a criação do *Child Abuse ImageDatabase* [Base de Dados de Imagens de Abuso Infantil] ou CAID pelo *Home Office*[Ministério do Interior Britânico], com o objetivo de coletar todos os CSAM apreendidos pelas agências de segurança no Reino Unido, permitindo que cada novo material fosse automaticamente comparado com o banco de dados existente, classificado por nível de severidade e qualquer CSAM recém-produzidofosse rapidamente identificado para ser o foco de um processo de análise de imagens para a identificação da vítima.[28] No Canadá, o *NationalChildExploitationCoordination Centre* (NCECC) [Centro Nacional de Coordenação de Exploração Infantil]da *Royal CanadianMounted Police*(RCMP) [Polícia Montada Real do Canadá] recebeu mais de 33.000 relatórios em 2017, um aumento de 93% em relação ao ano anterior, com a identificação de 844 vítimas no Canadá cujas séries foram carregadas no banco de dados da INTERPOLe 385 informações de abusadores sexuais infantis canadenses foram carregadas no mesmo banco durante o período do relatório.[29]

Outra iniciativa surgida nos EUA com ramificações em todo o mundo é a iniciativa conhecida por *Project VIC*.[30] O Project VIC e sua rede de parceiros trabalham em conjunto para fornecer aos investigadores, examinadores forenses digitais, e policiais acesso à avanços tecnológicos úteis que possam facilitar a identificação de vítimas e aumentar a eficiência da investigação. Frente à multitude de ferramentas, modelos e padrões de compartilhamento e análise de informações, o*Project VIC* pesquisou e avaliou diversos modelos para adotar um padrão de compartilhamento de dados e um modelo de compartilhamento de dados chamado VICS (*Video and ImageClassification Standard* ou Padrão de Classificação de Imagem e Vídeo), que permitiu a criação de um ecossistema de ferramentas e serviços que os investigadores podem usar em seu fluxo de trabalho diário a fim de criar um processo mais eficiente com menos duplicação de esforços. Os arquivos inseridos na biblioteca onde são *crowdsourced*, ou seja, os arquivos podem ser

analisados de maneira colaborativa e os*hash sets*das imagens identificadas também são armazenados na nuvem. A partir do uso desses ambientes virtuais de crowdsourcing e do uso de tecnologias e algoritmos de *hashing*, como o PhotoDNAe o F1, é possível fazer umaverificação cruzada de novos materiais apreendidos com *hash sets* existentes encontrados na nuvem, o que permite reduzir a duplicação de esforços além de permitir que o trabalho de identificação seja mais eficiente.[31]

Globalmente, a INTERPOL criou e administra um banco de dados de imagens e vídeos que permite que investigadores especializados compartilhem dados com as autoridades de todo o mundo –oInternational Child Sexual ExploitationDatabase (ICSE) [Banco de dados de Exploração Sexual Infantil Internacional]. Disponível através do sistema global de comunicações policiais seguras da INTERPOL (I-247), o banco de dados ICSE utiliza software de comparação de imagens e vídeos para facilitar a identificação de vítimas, abusadores e lugares, permitindo que usuários certificados acessem o banco de dados diretamente e em tempo real.[32] Até julho de 2018, 14.289 vítimas foram identificadas e mais de 6.200 abusadores sexuais infantis foram presos pela polícia trabalhando com o programa ICSE.[33]

Com o aumento de volumes apreendidos de CSAM, o uso de novas ferramentas tecnológicas e o investimento em novas tecnologias para auxiliar na detecção automatizada de CSAM, além da classificação e identificação de vítimas é primordial e ainda amplamente necessário.[34]Embora ainda incipiente e ainda reste muito a fazer, autoridades policiais, ONGs e o setor privado vêm unindo esforços no desenvolvimento de ferramentas e recursos para preencher as lacunas na identificação de vítimas de CSAM e na redução do trauma de estresse secundário gerado pela exposição repetida a essas imagens abusivas.

No Brasil, autoridades policiais desenvolveram uma tecnologia algorítmica chamada NuDetective Ferramenta Forense para identificar arquivos de pornografia infantil. Desenvolvido por Peritos Criminais Federais, o algoritmo faz uma rápida análise de imagens no computador na própria cena do crime para avaliar se contem imagens contendo como base a nudez humana, além de fazer uma análise de nomes de arquivo buscando por palavras suspeitas que podem remeter à possível CSAM.[35] Isso não apenas levou a uma redução drástica no número de arquivos a serem analisados – de 330.595 para apenas 183 arquivos suspeitos[36] – mas abriu ainda a possibilidade de prender o suspeito em flagrante. Em mais de 5 anos, o software permitiu a prisão de mais de 150 infratores no Brasil e atualmente está sendo usado por agências policiais na Argentina, Áustria, Noruega, Nova Zelândia, Paraguai, Portugal e Suécia.[37]

Em2018,o*CanadianCentreforChildProtection*[Centro Canadense de Proteção Infantil] lançou uma nova ferramenta chamada *Project Arachnid*[Projeto Aracnídeo], um "*webcrawler*" [rastreador da rede] automatizado que rastreia tanto a rede clara quanto a escura, seguindo materiais encontrados em links previamente reportados à Cybertip.ca como contendo CSAM. O Projeto rastreou com sucesso, em uma avaliação inicial de seis semanas atuando, 230 milhões de páginas da Web individuais, das quais 5,1 milhões continham CSAM, além de detectar mais de 40.000 imagens únicas de CSAM.[38]A equipe da Internet Watch Foundation (IWF) no Reino Unido também está trabalhando para automatizar a busca por CSAM na dark net, que rastreará serviços ocultos em busca de CSAM conhecido, alertando analistas sobre novos conteúdos encontrados.[39]

Uma das razões mais importantes em buscar soluções tecnológicas para minimizar a exposição de investigadores e peritos à CSAM é o fato de que a investigação e o processamento deste material estar associado à altos níveis de estresse traumático secundário, também chamado de trauma vicário, e *burnout*[esgotamento] em policiais e agentes envolvidos no processo. Em 2012, o ICMEC realizou uma revisão de literatura acadêmica sobre pesquisas existente no tangente à estresse traumático secundário, particularmente enfocado em casos de investigação de CSAM e descobriu que a visualização de bebês, crianças pequenas ou adolescentes explorados sexualmente pode colocar um policial sob maior risco de sofrer sofrimento psicológico, que pode levar a reações semelhantes ao Transtorno de Estresse Pós-Traumático (TEPT).[40] Estudos revisados descrevem trauma secundário como um conjunto de sintomas que inclui: pensamentos intrusivos, evitação, hiper-excitação, fadiga crônica, tristeza, raiva, flashbacks (da criança vítima durante contato normal com outras crianças), baixa concentração, desapego, exaustão emocional, vergonha, perturbação da atividade sexual normal (com a visão da memória do abuso sexual) e doença física.[41]Estudos mais recentes realizados entre policiais especializados em delitos cibernéticos contra crianças reportaram sintomas como ganho de peso, dificuldades com o sono, depressão, estresse, problemas com intimidade sexual e dificuldades de relacionamentos românticos, edemostrou que 43.7% dos respondentes

demostraram estresse secundário traumático de moderado a grave, e demonstrou que a dificuldade em visualizar material perturbador como o mais forte fator de predição de estresse traumático secundário, seguidos de 1)frequência de visualização de imagens, 2) uso de negação como mecanismo de enfrentamento, e 3) aumento do uso de álcool.[42]

Além da interferência na vida pessoal do indivíduo, o estresse traumático secundário também pode interferir no local de trabalho do indivíduo, reduzindo a eficácia e até mesmo levando ao absenteísmo, o que pode afetar significativamente a capacidade operacional das organizações policiais. Mas é importante frisar que, mais do que sofrer as consequências do estresse traumático secundário, fatores organizacionais podem ser também fatores de risco e influenciar diretamente na ocorrência de estresse traumático secundário.[43]Alguns fatores de risco organizacionais incluem a falta de apoio profissional, falta de supervisão adequada, falta de treinamento ou equipamentos adequados, carga excessiva de trabalho, entre outros fatores.

Para mitigar os efeitos do estresse traumático secundário, se faz urgente o desenvolvimento e implementação de políticas adequadas e de salvaguardas processuais para garantir o bem-estar de seus funcionários, além de garantir treinamento adequado e ferramentas tecnológicas a serem implementadas como uma resposta preventiva ao trauma secundário. Pesquisas também demonstraram a importância de implementar ou adotar estratégias de enfrentamento positivas, como o uso de humor, apoio social e condicionamento físico como atenuantes do estresse traumático secundário.[44] Algumas agências ou organizações policiais que trabalham na investigação e persecução penal de CSAM online em todo o mundo desenvolveram medidas de proteção para reduzir o trauma secundário e o *burnout*, como oferecer aos investigadores a oportunidade de se engajar em tarefas diferentes de vez em quando, serviços e outros programas de apoio ao bem-estar, e aconselhamento obrigatório ou de auto-referência.[45]

Agências policiais pertencentes ao Virtual Global TaskForce[46] (VGT) [Força Tarefa Global Virtual], por exemplo, oferecem uma variedade de serviços de saúde psicológica e iniciativas para apoiar os funcionários que trabalham em casos de exploração infantilonline.[47] Muitas agências da VGT realizam avaliações de investigadores por psicólogos antes, durante e após a designação do funcionário para a posição, de maneira a determinar a adequação da colocação inicial e para avaliar quaisquer questões em curso relacionadas à sofrimento psíquico, o que está de acordo com as recomendações da pesquisa analisada, já que encontrar a "pessoa certa" para o trabalho foi identificado como um fator atenuante para reduzir o risco de estresse traumático secundário.[48] Igualmente, a detecção precoce de "sinais de alerta" também reduz o risco de maior sofrimento psicológico.[49]

Haja vista que pesquisas também identificaram alguns fatores de risco em potencial (como abuso na infância ou outra história de abuso sexual)[50] para o desenvolvimento de estresse traumático secundário, a avaliação psicológica pré-entrada proposta pelos membros da VGT pode ser uma alternativa não apenas avaliar os fatores de risco para este papel, mas também servir de oportunidade para a criação de indicadores para a medição de referência a fim de monitorar o contínuo do bem-estar psicológico do policial. Outras iniciativas ou políticas para limitar o sofrimento psicológico no ambiente de trabalho incluem: fazer pausas regulares que envolvam movimento físico; evitando múltiplas entradas sensoriais (ou seja, áudio e vídeo); limitando o tempo gasto visualizando imagens em um turno, alternar períodos de investigações com casos não correlatos ao abuso sexual infantil, entre outros.[51] Também é importante investir no desenvolvimento de estratégias organizacionais apropriadas para apoiar a aplicação da lei que investiga o CSAM lidar com os efeitos da investigação desses casos.

Outras estratégias bem documentadas incluem o acesso a oportunidades de treinamento - tanto relacionadas às suas habilidades de investigação quanto às habilidades de "*coping*"[enfrentamento] -, investimentos em equipamento apropriado e treinamento sobre os últimos desenvolvimentos, dados os desafios técnicos trazidos pela mudança rápida de novos desenvolvimentos técnicos.[52]Neste sentido, as ferramentas tecnológicas são aliadoscríticos na proteção e cuidado dos pesquisadores. Agentes da *Homeland Security Investigation* [Investigação de Segurança Interna] (HSI), do *Bureau of Federal Intelligence* [Agência Federal de Inteligência] (FBI) e outras agências policiais nos EUA – e outras partes do mundo – usamferramentas tecnológicas como Net Clean e GriffeyeAnalyze para gerenciar seus casos de CSAM, que incluem opções de importação/exportação; agrupamento e pesquisa de metadados; API aberta para usar aplicativos de terceiros necessários para resolver os casos, entre outros.[53] Essas ferramentas já contemplam tecnologias como o Photo DNA e F1, que permitem um hashing de imagem e vídeo robusto, além de análises avançadas com algoritmos para

filtragem, classificação e pesquisa. Ferramentas como o GriffeyeAnalyze e o Net Clean suportam a aplicação da lei, agrupando todos os arquivos relacionados às mesmas vítimas em séries e pré-classificando as imagens como imagens de abuso ou imagens "pertinentes". Ao compilar todas essas imagens juntas em série, essas ferramentas permitem que as autoridades policiais verifiquem vítimas e séries não identificadas, bem como trabalhem na revisão de materiais não-abusivos em busca de pistas, reduzindo assim a incidência de traumas vicários entre os investigadores.

O setor privado tem trabalhado em parceria com agências de aplicação da lei para desenvolver ferramentas de inteligência artificial e "aprendizagem profunda" para reconhecimento de imagens, buscando identificar quando novos materiais CSAM são compartilhados, buscando classificar automaticamente a gravidade do abuso ou a idade da vítima, entre outros. Em março de 2018, o Departamento de Ciência e Tecnologia do Departamento de Segurança Doméstica dos EUA começou a trabalhar em um projeto chamado CHEXIA (ChildExploitationImageAnalytics) para desenvolver e testar algoritmos de reconhecimento facial para vasculhar imagens de exploração infantil encontradas na internet e na web escura. A ideia do projeto é automatizar a identificação de vítimas, ajudando os investigadores a encontrar vítimas e perpetradores mais rapidamente, enquanto são confrontados com enormes quantidades de CSAM gráfico e violento.

Conclusão

O abuso sexual de crianças on-line é um crime multifacetado que transcende as fronteiras nacionais, exigindo, portanto, uma abordagem abrangente para reduzir a disponibilidade de CSAM e, ao mesmo tempo, aumentar a proteção às crianças sem deixar de lado o cuidado com as autoridades que investigam esses crimes. A indústria, as empresas de tecnologia e as principais redes sociais têm trabalhado lado a lado com as agências policiais em todo o mundo para encontrar soluções – técnicase processuais – parareduzir a disponibilidade do CSAM e sua distribuição em seus canais de serviços e na Internet de uma maneira geral. No entanto, volumes de CSAM apreendidos continuam a crescer a cada ano, colocando mais pressão sobre as agências de aplicação da lei já sobrecarregadas.

Mais do que abordagens tecnológicas, é fundamental que as organizações policiais em todo o mundo compreendam a importância de uma abordagem centrada na criança vítima e a implementem em suas investigações, de maneira a não deixarmos uma só criança vitimizada sem a atenção e cuidado necessário.É fundamental ainda incorporar medidas para garantir que os casos de abuso sexual de crianças sejam investigados de maneira detalhada em cada denúncia, de maneira a investigar se o abuso foi documentado em um arquivo digital ou não. Tais medidas poderiam ter um tremendo impacto na redução da produção desses materiais, e um grande fator restaurador para crianças vítimas, que poderiam ter suas imagens identificadas,*hashed*e incluídas em bases de dados internacionais de forma a evitar mais exposição e re-vitimização.

Embora não seja a única solução para todos os problemas, a tecnologia vem auxiliando as organizações policiais e de proteção infantil a reduzir o trauma dos sobreviventes do CSAM, ao tentar remover o conteúdo da Web por meio do uso de valores *hash* e webcrawlers robustos. No entanto, ainda há muito a ser feito no desenvolvimento de tecnologias e automação para a identificação de crianças vítimas. Essas ferramentas, além de aumentar a eficiência investigativa, têm um fator altamente preventivo do desenvolvimento do estresse traumático secundário, por minimizar a exposição de investigadores e outros atores envolvidos na investigação e persecução penal à estes conteúdos extremamente degradantes e violentos.

No entanto, tão importante medidas tecnológicas e o treinamento de agentes a respeitos dessas ferramentas e seu uso adequado, é essencial que os órgãos responsáveis pelas agências policiais compreendam a importância de tomar as medidas necessárias para minimizar o trauma secundário e o *burnout*. Criar um ambiente propício e desenvolver estratégias adequadas a realidade de cada corporação é fundamental. Pesquisas recentes apontam para uma mudança necessária na cultura policial de maneira a melhor capacitar os policiais a expressarem construtivamente seus sentimentos sem que isso seja visto como uma fraqueza.[54]

Embora existam muitas pesquisas realizadas no âmbito internacional, poucos são os dados encontrados na América Latina relativos ao estresse traumático secundário em investigadores ou peritos forenses incumbidos de investigar casos de CSAM. Sabe-se do alto grau de rotatividade nas agências policiais da região que têm contribuído em grande parte para a dificuldade em especialização das investigações em muitos países. Quanto desta rotação é reflexo de estresse traumático secundário é uma pergunta ainda sem resposta. Estudos adicionais acerca de como as organizações poli-

ciais na América Latina vêm a questão da identificação de vítimas e das alternativas ao estresse traumático secundário poderiam ajudar a fechar as lacunas existentes e a encontrar soluções adequadas à realidade da região. Os ganhos em eficiência investigativa e em proteção dos direitos humanos dos envolvidos são, sem sombra de dúvidas, imensuráveis.

1. *Internet World Stats [Estatísticas Mundiais da Internet], disponível em: http://www.internetworldstats.com/stats.htm (visitado pela última vez em 30 Junho de 2018).*
2. *Digital in 2018: World's Internet UsersPass The 4 Billion Mark [Digital em 2018: Usuários Globais da Internet Ultrapassam a Marca de 4 Bilhões de Pessoas],disponível em: https://wearesocial.com/blog/2018/01/global-digital-report-2018 (visitado pela última vez em 13 de julho de 2018).*
3. *Idem.*
4. *Internet World Stats[Estatísticas Mundiais da Internet], disponível em: https://www.internetworldstats.com/stats10.htm (visitado pela última vez em 30 de Junho de 2018).*
5. *Livingstone, S., Carr, J. and Byrne, J. (2016). One in three: internet governance and children'srights [Um em Três: Governança na Internet e Direitos das Crianças], disponível em: https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf(visitado pela última vez em 02 de Julho de 2018).*
6. *International Telecommunications Union, ITU (2017). Facts and Figures 2017 [União Internacional de Telecomunicações, Fatos e Estatísticas de 2017], disponível em: http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2017.pdf (visitado pela última vez em 30 de junho de 2018).*
7. *Byrne, J., Kardefelt-Winther, D., Livingstone, S., Stoilova, M. (2016) Global Kids Online researchsynthesis, 2015–2016[Síntese daPesquisa Global de Crianças Online 2015-2016]. UNICEF Office ofResearch– Innocenti and London SchoolofEconomics and Political Science., disponível em: http://globalkidsonline.net/synthesis-report/ (visitado pela última vez em 02 de Julho de 2018).*
8. *Aproximadamente 1 milhão de novos usuários se uniram à principalrede social do país, todos os dias, durante 12 meses. Dados da Digital em 2018. Idem nota de rodapé 2.*
9. *CETIC.BR (2017). TIC Domicílios 2017, disponível em: https://cetic.br/media/analises/tic_domicilios_2017_coletiva_de_imprensa.pdf (visitado pela última vez em 25 de Julho de 2018).*
10. *Ofcom (2016). Children and parents: media use and attitudesreport [Crianças e Pais: relatório do uso de mídia e atitudes], disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf (visitado pela última vez em 01 de Julho de 2018).*
11. *UNICEF (2017).The State of the World's Children 2017, Children in a Digital World [O Estado das Crianças do Mundo 2017, Crianças em um Mundo Digital], disponível em: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf (visitado pela última vez em 01 de Julhode 2018).*
12. *NajatM'jidMaalla, UN SpecialRapporteur(2009).Promotion and ProtectionofAllHumanRights, Civil, Political, Economic, Social and Cultural Rights, including the RighttoDevelopment –Reportof the SpecialRapporteuron the saleofchildren, childprostitution and childpornography[Promoção e Proteção de Todos os Direitos Humanos, Direitos Civis, Políticos, Econômicos, Sociais e Culturais, incluindo o Direito ao Desenvolvimento – Relatórioda Relatora Especial sobre a venda de crianças, prostituição infantil e pornografia infantil], A/HRC/12/23, disponível em: https://documents-ddsny.un.org/doc/UNDOC/GEN/G09/146/27/PDF/G0914627.pdf?OpenElement(visitado pela última vez em 02 de Julho de 2018).Ver também Henry, S., Video: Shawn Henry on Cyber Safety, Federal Bureau ofInvestigation (FBI), May 2011 [Shawn Henry fala sobre Segurança Cibernética, Bureau Federal de Investigações (FBI), maio de 2011], disponível em: https://www.fbi.gov/news/videos/henry_051611(visitado pela última vez em 01 de Julhode 2018).*
13. *Para mais informações sobre as discussões em torno da decisão de se afastar do termo "Pornografia Infantil", consulte a publicação: Diretrizes Terminológicas para a Proteção das Crianças contra Exploração Sexual e Abuso Sexual, página 35 (versão em inglês), disponível em inglês e espanhol em:http://luxembourgguidelines.org(visitado pela última vez em 12 de Julhode 2018).*
14. *VG (2017).Breaking the Dark Net: Why the Police Share Abuse PicstoSave Children [Quebrando a Rede Escura: Por que a polícia compartilha fotos de abuso para salvar as crianças], Disponível em:https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (visitado pela última vez em 16 de Julho de 2018).*
15. *INHOPE (2016) AnnualReport 2016 (Relatório annual 2016 – INHOPE], Disponível em:http://www.inhope.org/Libraries/Annual_reports/Annual_report_2016.sflb.ashx?download=true(visitado pela última vez em 16 de Julho de 2018).*
16. *National Center for Missing &Exploited Children (NCMEC), Cybertipline [linha de denúncia do Centro Nacional dos EUA para Crianças Desaparecidas e Exploradas – NCMEC], disponível em:http://www.missingkids.org/gethelpnow/cybertipline(visitado pela última vez em 16 de julho de 2018).*
17. *Net Clean Report 2016, InvestigationswithTerabytesof Data and MillionsofImages [Relatório Net Clean 2016, Investigações com Terabytes de Dados e Milhões de Imagens], disponível em:http://www.netclean.com/the-netclean-report-2016/insight-2/(visitado pela última vez em 16 de julho de 2018).*
18. *Patrick Lussier, Eric Beauregard. Sexual Offending: A Criminological Perspective. Chapter 13: Online Sexual Exploitationof Children [Ofensa Sexual: Uma Perspectiva Criminológica. Capítulo 13: Exploração Sexual Online de Crianças]. Ed: Routledge, Apr 20, 2018.*
19. *VG (2017).Breaking the Dark Net: Why the Police Share Abuse PicstoSave Children [Quebrando a Rede Escura: Por que a polícia compartilha fotos de abuso para salvar as crianças], Disponível em:https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (visitado pela última vez em 16 de Julho de 2018).*
20. *Virginia N. L. Franqueira; Joanne Bryce;Noora Al Mutawa;*

Andrew Marrington (2018). InvestigationofIndecentImagesof Children cases: Challenges and suggestionscollectedfrom the trenches [Investigação de casos de Imagens Indecentes de Crianças: Desafios e sugestões coletadas das trincheiras], disponível em: https://www.sciencedirect.com/science/article/pii/S1742287617302669(visitado pela última vez em 17 de Julho de 2018).

21. Demos, Technology Briefing Series: Online Child Sexual Abuse Imagery [Série de Resumos sobre Tecnologia: Imagens de Abuso Sexual Infantil Online], disponível em: https://www.demos.co.uk/wp-content/uploads/2018/01/Technology-Briefing-1-Online-CSAI-19.01-1.pdf(visitado pela última vez em 16 de Julho de 2018).

22. Internet Crimes Against Children Task Force, AboutUs[Forças Tarefa contra Crimes Cibernéticos Contra Crianças, Sobre Nós],disponível em: https://www.icactaskforce.org/Pages/About%20Us.aspx(visitado pela última vez em 3 de Julho de 2018).

23. Os hashes são números que servem como "impressões digitais" exclusivas que podem ser usadas para comparar imagens. Normalmente, uma pequena modificação em uma imagem pode alterar o valor de HASH, mas técnicas de hash mais robustas permitiram a atribuição de números mais precisos que podem ajudar a identificar imagens da mesma pessoa, como o PhotoDNA, por exemplo. Duas imagens diferentes não podem compartilhar o mesmo hash. Agências policiaisvêm utilizando os valores de hash para fazer uma verificação cruzada de imagens contra os hashes de imagens de CSAM já conhecidas/identificadas,de maneira automatizada, para garantir a eficiência da investigação e economizar tempo e recursos humanos.

24. Para mais informações sobre o PhotoDNA, ver:Microsoft.com, PhotoDNA CloudService [Serviço em Nuvem do PhotoDNA], disponível (em inglês) em:https://www.microsoft.com/en-us/photodna(visitado pela última vez em 3 de Julho de 2018).

25. Para mais informações sobre o F1, ver: Project VIC, Technology [Tecnologia], disponível (em inglês) em: http://projectvic.org/technology/(visitado pela última vez em 3 de Julho de 2018).

26. Richard Brown, Eric Oldenburg, and Jim Cole, "Project VIC: HelpingtoIdentify and Rescue Children from Sexual Exploitation" [Projeto VIC: Ajudando a Identificar e Resgatar Crianças da Exploração Sexual], Police Chief online, June 6, 2018. (visitado pela última vez em 13 de Julhode 2018).

27. National Center for Missing and Exploited Children [Centro Nacional para Crianças Desaparecidas e Exploradas], Key Facts [Fatos Principais], disponível em: http://www.missingkids.org/KeyFacts. (visitado pela última vez em 13 de Julho de 2018).

28. Idem nota 21.

29. Royal CanadianMounted Police (2017), 2016-17 DepartmentalResultsReport [Relatório de Resultados Departamentais da Policia Real Montada do Canadá, 2016-17], disponível (em inglês) em: http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2016-17-departmental-results-report(visitado pela última vez em 13 de Julho de 2018).

30. Para mais informações sobre o projeto, ver: Project VIC, disponível (em inglês) em: http://projectvic.org/technology/(visitado pela última vez em 3 de Julho de 2018).

31. Idem Nota 26.

32. INTERPOL, Victimidentification [Identificação de Vítimas],disponível (em inglês) em: https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification. (visitado pela última vez em 13 de Julho de 2018).

33. Idem nota anterior.

34. Idem nota 21.

35. Pedro, M.S. Eleutério, Ferramenta Forense NuDetective, disponível em: http://www.eleuterio.com/nudetective.html (visitado pela última vez em 13 de Julho de 2018).

36. IEEE Cloud Computing, Tech Fights Crime: The WaysAlgorithms and Websites Police for ChildExploiters and Criminals, NuDetective [Tecnologia combate crimes: as maneiras que os algoritmos e sites policiam exploradores de crianças e criminosos, NuDetective]. Disponível em: https://publications.computer.org/cloud-computing/2017/10/13/how-tech-algorithms-cloud-security-fight-crime-child-abuse/ (visitado pela última vez em 13 de Julho de 2018)

37. IPOG Blog. NuDetective: ferramenta forense de combate à pedofilia. Disponível em: https://blog.ipog.edu.br/tecnologia/nudetective-ferramenta-pedofilia/(visitado pela última vez em 13 de Julho de 2018)

38. Canadian Centre for Child Protection, Project Arachnid - Groundbreaking tool to remove online child sexual abuse material[Centro Canadense de Proteção à Criança. Projeto Aracnídeo– Ferramentainovadora para remover material online de abuso sexual infantil], disponível (em inglês) em:https://www.cybertip.ca/app/en/projects-arachnid(visitado pela última vez em 13 de Julho de 2018).

39. Idem nota 21.

40. Kimberly Penna, ICMEC (2012), The Psychological Harm Project. [O Projeto de Danos Psicológicos. Conferência Global Virtual Taskforce 2012. Reunião do Conselho de Diretores em Abu Dhabi, Emirados Árabes Unidos. 10 de dezembro de 2012.

41. Idem Nota 40.

42. Bourke ML, Craun SW (2014). Copingwithsecondarytraumatic stress: differencebetween U.K. and the U.S. childexploitationper sonnel[Lidando com o estresse traumático secundário: diferença entre a equipe de exploração infantil do Reino Unido e dos EUA.] Traumatology: An International Journal, 20(1), 57-64, disponível em: http://dx.doi.org/10.1037/h0099381(visitado pela última vez em 18 de Julho de 2018).

43. Bell, H., Kulkarni, S., & Dalton, L. (2003). Organizationalpreventionofvicarious trauma [Prevenção organizacional de trauma vicário]. Families in Society, 84, 463–470, disponível em https://www.ce-credit.com/articles/100716/PrevVicariousTrauma.pdf(visitado pela última vez em 18 de Julho de 2018).

44. Idem Nota 40.

45. MacEachern, A.D., Dennis, A.A., Jackson, S. et al. J Police Crim Psych (2018).SecondaryTraumatic Stress: Prevalence and SymptomologyAmongst Detective OfficersInvestigatingChildProtection Cases [Estresse Traumático Secundário: Prevalência e Sintomatologia Entre Detetives Investigando Casos de Proteção à Criança], disponível em:https://link.springer.com/article/10.1007/s11896-018-9277-x(visitado pela última vez em 13 de Julho de 2018).

46. O Virtual Global Taskforce [Força Tarefa Virtual Global] (VGT) é uma aliança internacional de 13 agências policiais e 19 parceiros do setor privado que trabalham juntos para combater a exploração e abuso sexual de crianças e outras formas de exploração sexual infantil transnacional. Os países/agências membros da VGT incluem: Austrália: Polícia Federal Australiana; Canadá: Polícia Real Montada do Canadá – CentroNacional de Coordenação da Exploração Infantil; Colômbia: Polícia Nacional da Colômbia; EUROPOL; INTERPOL; Holanda: Polícia Nacional Holandesa; Nova Zelândia: Polícia da Nova Zelândia; Filipinas: Polícia Nacional das Filipinas; República da Coréia: Polícia Nacional Coreana; Suíça: Unidade de Coordenação de Cibercrime da Suíça; Emirados Árabes Unidos: Ministério do Interior para os Emirados Árabes Unidos; Reino Unido: Comando de Exploração Infantil e Proteção On-line da Agência Nacional de Crime (NCA); e Estados Unidos da América: Departamento de Investigações de Segurança Interna de Imigração e Alfândega dos EUA (DHS/HSI/ICE).

Os parceiros do setor privado da VGT incluem: Blackberry, ECPAT, International Centre for Missing &Exploited Children [Centro Internacional para Crianças Desaparecidas e Exploradas – ICMEC], INHOPE [Associação Internacional de Linhas Diretas da Internet], International Justice Mission [Missão Internacional de Justiça], Kik, Unidade de Crimes Digitais da Microsoft, Centro NCMEC, NetClean, PayPal, Telstra, The Code [O Código], World Vision Australia, Ziuz, Carteira Internacional de Condução em Informática - Arábia (ICDL-Arábia), Web-IQ, Coalizão Infantil de Resgate (CRC), MagnetForensics, NationalChildren's Advocacy Center (NCAC)

47. *Idem Nota 40.*
48. *Idem Nota 40.*
49. *Idem Nota 40.*
50. *Craun SW, Bourke ML, Bierie DM, Williams KS (2014) A longitudinal examinationofsecondarytraumatic stress amonglawenforcement[Um exame longitudinal do estresse traumático secundário entre os agentes da lei]. VictimsOffenders 9(3):299–316, disponível em: https://www.tandfonline.com/doi/abs /10.1080/15564886.2013.848828. (visitado pela última vez em 18 de Julho de 2018).*
51. *Idem Nota 50.*
52. *GundaWößner& Julian Graf, Psychological Stress and Coping Strategies among Child Pornography Police Investigators: A Qualitative Analysis (2016). Available at: https://www.mpicc.de/ files/pdf4/Woessner_Graf_2016_transl.pdf.(visitado pela última vez em 13 de Julho de 2018).*
53. *GriffeyeAnalyze, disponível em: https://www.griffeye.com/the-platform/analyze-di/. (visitado pela última vez em 13 de Julho de 2018).*
54. *Idem Nota 50.*

CURSO CIBERCRIMEN Y CIBERDELITOS

AUTOR: Ministerio de Seguridad de la República Argentina

RESUMEN: En consonancia con la creciente importancia de los delitos informáticos y del rol de la tecnología en todos los delitos, desde el Instituto Conjunto de Conducción Estratégica –ICCE– del Ministerio de Seguridad de la República Argentina, y con el compromiso de brindar una oferta académica de la más alta calidad, se lanzó el 9 de abril del corriente año el Curso Cibercrimen y Ciberdelitos.

Palabras claves: Desarrollo tecnológico – Cibercrimen – Ciberdelitos – Entornos digitales – Investigación Criminal

La constante evolución tecnológica, y los desafíos que plantea la investigación de nuevas formas delictivas en entornos digitales; supone también nuevos desafíos para la formación de los funcionarios encargados de hacer cumplir la ley.

En este marco, desde el Instituto Conjunto de Conducción Estratégica –ICCE– bajo la coordinación de la Secretaría de Coordinación, Formación y Carrera del Ministerio de Seguridad de la República Argentina, cuya misión es brindar formación especializada y conjunta a Oficiales de las Fuerzas Policiales y de Seguridad, policías provinciales y funcionarios civiles responsables de la seguridad interior, se puso en marcha en abril de 2018, con una duración anual, el curso "Cibercrimen y Ciberdelitos".

Su objetivo principal consiste en brindar a funcionarios policiales de jerarquías intermedias de áreas de investigación de delitos tales como narcotráfico, trata de personas, homicidios y contrabando, conocimientos básicos -tanto tecnológicos como jurídicos y procedimentales- para la investigación de delitos en entornos digitales.

En este sentido, durante su desarrollo, además de analizar qué es un delito informático y sus diferentes tipos y características, se busca comprender las metodologías, procesos y desafíos que comporta la investigación criminal de los mismos.

Entre los principales contenidos abordados se encuentran los siguientes: legislación vigente en Argentina, recolección, preservación y sustentación de la prueba; toma de denuncia de diferentes delitos; registro de delitos con y sin orden judicial; estudios de casos de delitos "ordinarios" que incluyen utilización de diferentes tecnologías como medios accesorios o comisivos; red profunda; fraude electrónico, suplantación de identidad y estafas en internet; pedofilia y grooming; y robo de información.

De esta forma, se busca relacionar conocimientos teóricos con ejercicios prácticos, para posibilitar la adquisición de competencias necesarias para el óptimo desempeño de las acciones de prevención e investigación de delitos cibernéticos.

ENSINO A DISTÂNCIA EM SEGURANÇA PÚBLICA NO BRASIL: REDE EAD/SENASP[1]

AUTOR: Sidiclei Silva de Araujo[2]

RESUMO: Introdução: Apresenta-se circunstância histórica e mudança de paradigmas quanto ao uso do novo método como modalidade de ensino a distância no desenvolvimento e capacitação dos profissionais em Segurança Pública nas mais diversas instituições em todo o território brasileiro. Objetivos: o principal resultado, é pertinente ao uso de uma ferramenta tecnológica de estudos e o alcance da mesma em um cenário distinto, perfazendo uma constante na capacitação em Segurança Pública. Procedimentos Metodológicos: Este estudo pode ser caracterizado como sendo um estudo de caso único, exploratório e qualitativo, sendo realizado na coordenação de ensino a distância da Secretaria Nacional de Segurança Pública - Senasp, como técnica de coleta de dados utilizada nessa pesquisa "observação in loco" que auxiliou na obtenção de maiores informações sobre a instituição. Resultados: sendo apresentado os principais itens definidores da estratégia assim como o aprofundar das questões relativas aos indicadores presentes na área de educação a distância. Com base nas informações encontradas, foi trabalhada a questão do Ambiente Virtual de Aprendizagem-AVA e a estruturação dessa ferramenta para a utilização da gestão educacional em Segurança Pública. Conclusão: O objetivo principal deste trabalho foi atingido, sendo possível mapeamento histórico e estratégico do uso da modalidade de ensino a distância enfatizando os recursos tecnológicos empregados pela Senasp detalhados nesse artigo.

Palavras-chaves: ensino a distância; segurança pública; cursos Senasp.

Introdução

A Rede de Educação a Distância da Secretaria Nacional de Segurança Pública – (Rede EaD/Senasp), inaugurou a dialogicidade[3] na relação educacional em Segurança Pública, promoveu o uso de novas tecnologias de informação e comunicação, por analogia a uma ***Revolução Copernicana***[4] na educação em Segurança Pública no Brasil.

Destaco o uso da mesma similaridade por inúmeros pensadores, a título de exemplo, cita-se, o filósofo e educador norte americano (JONH DEWEY, 1932): "o novo lugar do aluno no processo de aprendizagem". Na mesma linhagem o referido modelo educacional proposto pelo ***escolanovismo***[5], reforçado por (LOURENÇO FILHO, 1978), e os escolanovistas brasileiros (ANÍSIO TEIXEIRA, 1930), com destaque a (ROQUETTE PINTO, 1922) visionária do ***ensino a distância***[6], dentre outros pensadores que defenderam o uso da tecnologia subordinada a um projeto educacional como se observa abaixo:

> "O ensino a distância é uma prática muito antiga, mas que recebeu grande impulso com as novas tecnologias da informação e da comunicação. As possibilidades de troca de grandes massas de dados através da rede de informática em tempo real viabilizam o desenvolvimento dos cursos via internet (OLIVEIRA, COSTA E MOREIRA, 2004, p.136)."

Da mesma forma, a equipe educacional da Senasp, realizou estudos interdisciplinares, buscando a organização dos elementos básicos da investigação no campo da educação a distância, com ênfase aos elementos práticos do cotidiano, bem como as necessidades técnicas, táticas e procedimentais, na seara de Segurança Pública, observando fatores em comum devido as peculiaridades regionais do Brasil. Organizando assim, os cursos com fundamentação legal, embasamentos técnicos e procedimentos mais atualizados, outrora abordados somente pelo ensino tradicional culminando a um projeto de educação a distância.

Fundamentação Jurídica

De acordo com o marco legal, a Lei de Diretrizes e Bases da Educação Nacional difundiu o ensino a distância, por conseguinte o incentivo e reconhecimento do Governo Federal Brasileiro, no que tange à incorporação do método de aprendizagem retrocitado nas instituições públicas (Art. 80 da Lei nº 9.394 de 20 de dezembro de 1996).

Nesse passo, cabe destacar a redação do Art. 1º do decreto presidencial nº 5.622, de 19 de dezembro de 2005, conforme segue:

> "Art. 1º Para os fins deste Decreto, caracteriza-se a educação a distância como modalidade educacional na qual a mediação didático-pedagógica nos processos de ensino e aprendizagem ocorre com a utilização de meios e tecnologias de informação e comunicação, com estudantes e professores desenvolvendo atividades educativas em lugares ou tempos diversos. (BRASIL, 2005, P.1)."

O entendimento supramencionado se encontra respaldado na Lei 8.112, de 11 de dezembro de 1990, "Art. 3º V - estimular a participação do servidor em ações de educação continuada, entendida como a oferta regular de cursos para o aprimoramento profissional, ao longo de sua vida funcional".

A Senasp com o objetivo de ampliar o conhecimento educacional na área de Segurança Pública, democratizou o acesso ao conhecimento, prezando por uma educação de qualidade e balizador na padronização de ações. Desse modo, a Rede EaD-Senasp, proporcionou, por intermédio do Ambiente Virtual de Aprendizagem-AVA, o alcance educacional em todas as regiões do país, promovendo o acesso ao conhecimento na totalidade dos espaços geográficos, culturais e sociais, anteriormente inalcançáveis pela educação tradicional.

O cenário discursivo

Mediante o exposto, bem como o cenário jurídico e a existência de diferentes fatores, no ano de 2005 foi idealizada a Rede EaD-Senasp[7], com o desígnio de perscrutar de forma estratégica o desenvolvimento tecnológico disponível à época, ao oportunizar cursos na modalidade a distância, alinhados com as macropolíticas de Segurança Pública.

Com essa inovação houve um redimensionamento das formas de pensar, fomentando discussões acadêmicas, linhas de pesquisas nos diversos assuntos relacionados à temática proposta, potencializando o processo coletivo da construção do conhecimento, momento que propiciou a arquitetura da maior Rede de Educação a Distância em Segurança Pública do Brasil.

Assim sendo, a elaboração de um AVA peculiar, desenvolvido em linguagem de programação ASP.NET, customizado para atender às necessidades educacionais da Senasp e atuar como escola virtual composta por salas de aula online. Consequentemente, favoreceu a execução de cursos livres de 40 e 60 horas/aula no formato SCORM, contendo vídeos, chats, fóruns e materiais complementares, sendo que detinham a distribuição em turmas de até 50 (cinquenta) profissionais, com o acompanhamento direto de um docente virtual denominado Tutor.

Em relação à parte tecnológica do AVA, menciona-se que sua composição se dá por elementos práticos de gestão: *administrativa, conteúdo, coordenação, tutoria, financeiro e aluno*. Nesse sentido, os fatores que merecem destaque são: *a*

agilidade no acesso à informação, otimização do tempo e melhoria na tomada de decisões da Coordenação de Ensino a Distância.

Preliminarmente, os cursos livres decorriam em 04 (quatro) ciclos de estudos ao ano e o AVA contava com as seguintes vantagens: *flexibilidade de horários de estudos, sem limitador ao acesso de alunos, sem restrição geográfica e gratuito*. Mesmo com inúmeros benefícios as inscrições apresentavam baixa procura, relacionados às questões de resiliência, acessibilidade à equipamento de informática, preconceito, "analfabetismo digital" e o pouco conhecimento a respeito dos cursos na modalidade à distância disponíveis no país.

Nesse ínterim, a Rede EaD/SENASP obteve baixa adesão atribuída também à rápida evolução das tecnologias de informação somada ao fato do público alvo que detinha pouco acesso às novas tecnologias. Concomitantemente, ocorria uma coalizão de saberes, no sentido de buscar as soluções na "*inclusão digital",* fato, este, que gerou unidades de estudos, conhecidas como telecentros[8] e resultou em 270 (duzentas e setenta) unidades em todo o país. Assim, a Senasp passou a exercer o papel efetivo de órgão condutor dos processos de educação a distância em Segurança Pública.

A Rede EaD-Senasp obteve reforço do Programa Nacional de Segurança Pública com Cidadania-PRONASCI[9], este, efetuava o repasse de **bolsas**[10] de estudos incentivando os profissionais dessa seara à capacitação por meio dos cursos, o que gerou uma procura exponencial.

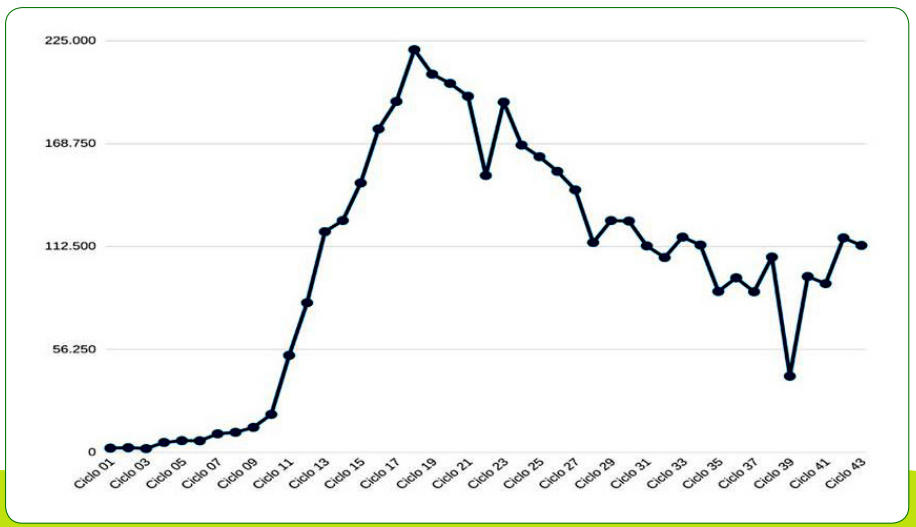


Figura 1 – matrículas no período 2005 a 2018
Fonte: Elaborado pelo autor a partir dos referenciais da coordenação de ensino a distância da SENASP

O número de matrículas cresce substancialmente, tendo origem com 2.154 (duas mil cento e cinquenta e quatro) matrículas no ciclo 01 (um) indo ao vértice de 223.000 (duzentos e vinte e três mil) matrículas no ciclo 18 (dezoito), com ênfase nos temas relacionados aos diversos cursos matriculados, ampliando o conhecimento com o uso das inúmeras ferramentas síncronas e assíncronas disponíveis no AVA.

Retrato da educação, na modalidade a distância da Rede EaD-Senasp

As caraterísticas e vantagens da modalidade de ensino, o AVA se torna uma ferramenta estratégica na capacitação dos profissionais em Segurança Pública do país, contando com números relevantes, 712.000 (setecentos e doze mil) alunos cadastrados entre Policias Civis, Militares, Bombeiros, Profissionais de Perícia, Guardas Municipais, Policiais Federais, Policiais Rodoviários Federais e Servidores do Sistema Prisional. É importante ressaltar mais de 3,8 milhões de matrículas efetivadas perfazendo um montante de 3,3 milhões de aprovações.

Sob o mesmo ponto de vista, descrevo o período histórico de cursos da Rede EaD-Senasp, do mesmo modo, ciclo 01 (um) ao ciclo 43 (quarenta e três), 13 (treze) anos de efetiva promoção do conhecimento, perfazendo os indicadores de matrículas e aprovações revelam a trajetória de plena contribuição educacional da Senasp. Visto que, no ciclo 43 (quarenta e três) cerca de 15,5% dos alunos cadastrados no AVA, uma vez que, 112.000 (cento e doze mil) matrículas nos mais de 73 (setenta e três) **cursos**[11] disponíveis, a saber, alinhados ao perfil profissional do aluno.

Desta maneira, os cursos Direitos Humanos, Crimes Ambientais, Gerenciamento de Crises, Condutor de Veículos de Emergência, Identificação Veicular I, Polícia Comunitária, Espanhol Básico I, Aspectos Jurídicos da Abordagem Policial, Emergência Pré-Hospitalar I e Inglês I, ocupam as primeiras posições no número de matrículas, ingressantes e concluintes, alterando apenas de posição entre eles a cada ciclo. O curso Direitos Humanos se destaca em primeiro lugar, num total de 210.000 (duzentos e dez mil) matrículas, enquanto o curso Condutor de Veículo de Emergência, figura em segundo 167.000 (cento e sessenta e sete mil) matrículas. Em terceiro e quarto lugar, aparecem Crimes Ambientais, com o total de com 159.000 (cento e cinquenta e nove mil) e o curso Gerenciamento de Crises, com 143.000 (cento e quarenta três mil) matrículas.

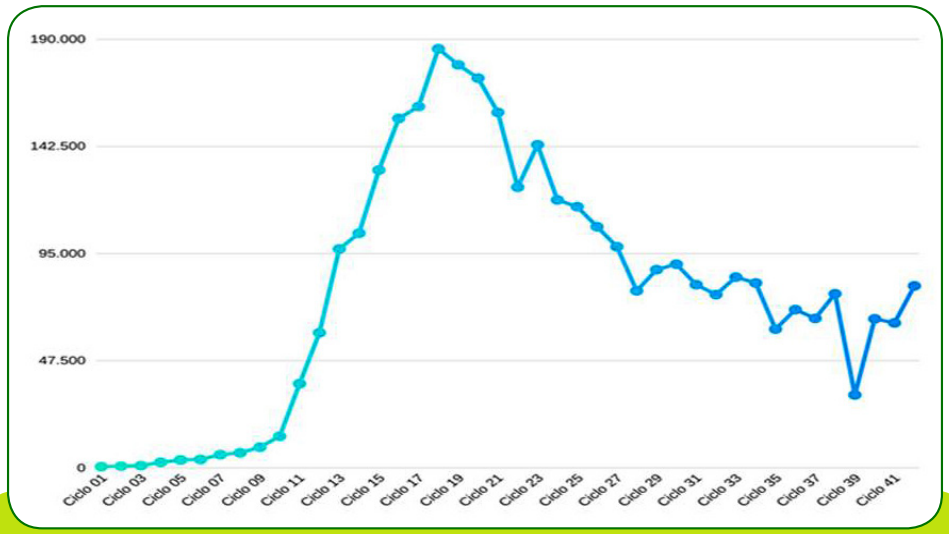


Figura 2 – aprovações no período 2005 a 2017
Fonte: Elaborado pelo autor a partir dos referenciais da coordenação de ensino a distância da SENASP

Cabe destacar ações que foram implementadas no início de 2017, com o objetivo de ampliar a qualidade do ensino a distância, bem como incentivar a capacitação. Destaco a feitura da Coordenação Pedagógica, sobretudo as modificações da docência virtual, atualizações do manual de tutoria e reformulações da metodologia de ensino. Da mesma forma, formação continuada dos tutores, que visa aprimorar a qualidade da prestação de serviço de docência online, ao mesmo tempo, processos seletivos de tutores, que por sua vez submetidos a um rigoroso método de seleção, alinhados ao perfil profissional do curso selecionado.

Também, a elaboração da **Portaria nº 50**[12], regulamenta o uso dos brevês da Rede EaD-Senasp. Em síntese a referida portaria visa o reconhecimento e valorização do profissional de Segurança Pública, mediante a capacitação pessoal e crescimento intelectual, conforme a classificação por número de cursos conclusos. Mediante o exposto as honrarias são distribuídas em 3 (três) tipos, cito: *bronze, prata e ouro*, desde que, o aluno conquiste a aprovação em 20 cursos, obtêm o direito ao uso do brevê ***Bronze***, posterior à conclusão de 40 cursos faz jus ao brevê ***Prata*** e, por conseguinte a conclusão de 60 cursos o brevê ***Ouro***.

Figura 3 – brevê bronze
Fonte: Elaborado pelo autor, coordenação de ensino a distância da Senasp.

Figura 4 – brevê prata
Fonte: Elaborado pelo autor, coordenação de ensino a distância da Senasp.

Figura 5 – brevê ouro
Fonte: Elaborado pelo autor, coordenação de ensino a distância da Senasp

Considerações finais

Dentre outros aspectos, vale destacar a historicidade da educação a distância, no Brasil, acessível no início do século XX, está por sua vez, se torna mais evidente com o uso da tecnologia de informação e comunicação ao final do século XXI. Ademais, o ensino a distância evoluindo para um estudo mais agradável e motivado pelas temáticas apresentadas aos discentes, com conteúdos relevantes, nos mais diversos assuntos das áreas em Segurança Pública, bem como a aceitação do ensino a distância, como fonte de relevância educacional.

No bojo dessa prerrogativa de mudança, as análises de resultados, foram satisfatórias, mediante a sustentabilidade, alcance e a democratização de conteúdos atuais, esclarecendo métodos e técnicas outrora pouco explorados, cito, referenciais de qualidade: 1. Estabelecer boa comunicação entre aluno e tutor; 2. Qualificar os tutores disponíveis para os atendimentos dos alunos; 3. Garantir que o aluno tenha evolução educacional.

Em conclusão, os problemas apresentados na implantação do ensino a distância à Segurança Pública do Brasil, bem como, o término do projeto Bolsa Formação, por consequência redução de matrículas nos cursos da Rede EaD-Senasp, descrito na Figura 1. Evidencia que a metodologia educacional empregada, reordenou, valores e práticas pedagógicas, gerando alterações no cenário educacional permanecendo com média de 102.000 (cento e dois mil) matrículas nos ciclos, inquestionavelmente a maior Rede de Educação a Distância em Segurança Pública da América Latina.

REFERÊNCIAS

BRASIL. **Lei nº 8.112**, de 11 dezembro de 1990, dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Diário Oficial da República do Brasil. Brasília, Distrito Federal, 14 de abril de 1991.

BRASIL. **Lei nº 9.394**, de 20 dezembro de 1996, estabelece as diretrizes e bases da educação nacional. Diário Oficial da República do Brasil. Brasília, Distrito Federal, 23 de dezembro de 1995.

BRASIL. **Decreto nº 5.622**, de 19 de dezembro de 2005, regulamenta o Art. 80 da Lei nº 9.394, de dezembro de 1996, estabelece as diretrizes e bases da educação nacional. Diário Oficial da República do Brasil. Brasília, Distrito Federal, 20 de dezembro de 2005.

BRASIL. **Decreto nº 5.707**, de 23 de fevereiro de 2006, institui a Política e as Diretrizes para o Desenvolvimento de Pessoal da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei no 8.112, de 11 de dezembro de 1990. Diário Oficial da República do Brasil. Brasília, Distrito Federal, 24 de fevereiro de 2006.

RELATÓRIO DE PESQUISA, Educação a distância para a segurança pública: uma experiência exitosa no âmbito do decreto nº 5.707/06, Brasília/DF, maio de 2012.

LOURENÇO FILHO, Manuel B. **Introdução ao estudo da escola nova: bases, sistemas e diretrizes da Pedagogia contemporânea**. - 12ª Ed. - São Paulo: Melhoramentos, 1978.

OLIVEIRA, Celina Couto de; COSTA, José Wilson da. & MOREIRA, Mercia. Ambientes informatizados de aprendizagem. In: COSTA, J. W. & OLIVEIRA, M. A. M. (Org.) **Novas linguagens e novas tecnologias: educação e sociabilidade**. Petrópolis, RJ: Vozes, 2004. 149 páginas.

TEIXEIRA, Anísio. **A Pedagogia de Dewey**. In: DEWEY, John. Vida e Educação. 5. ed. São Paulo: Companhia Editora Nacional, 1959.

ROQUETTE-PINTO, Edgard. **Ensaios brasilianos**. São Paulo: Companhia Editora Nacional, 1940.

NOTAS

[1] *Artigo publicado na Revista MERCOPOL, selecionado pela CEAD/SENASP/MSP, 2018.*

[2] *Especialista em Educação a Distância (WPOS), Gestor de Políticas Públicas, 3º Sargento da Policial Militar do Acre, Instrutor do Centro Integrado de Segurança Pública – CIEPS, Instrutor da Academia de Polícia Civil -ACADEPOL/AC, tutor virtual da Plataforma de Educação a Distância da Secretaria Nacional de Segurança Pública-SENASP, atualmente mobilizado pela SENASP lotado na Coordenação de Ensino a Distância no Ministério da Segurança Pública em Brasília, e-mail: sidiclei.araujo@ac.gov.br.*

[3] *Dialogicidade é a essência da educação como prática da liberdade.*

[4] *Revolução Copernicana constituiu-se no processo histórico que redundou na substituição do sistema geocêntrico (Geocentrismo) pelo sistema heliocêntrico (Heliocentrismo), inclusive no que diz respeito às profundas consequências acarretadas por essa substituição para a história da humanidade.*

[5] *Escolanovismo escola nova no Brasil, o movimento ganhou impulso na década de 1930, após a divulgação do Manifesto dos Pioneiros da Educação Nova (1932). Nesse documento, defendia-se a universalização da escola pública, laica e gratuita.*

[6] *A primeira transmissão realizada no Brasil foi em 1922, com o discurso do então presidente Epitácio Pessoa, em meio às comemorações do Centenário da Independência. A primeira estação de rádio foi fundada em Recife, em 1919, por Augusto Pereira e Oscar Moreira. Foi também uma das primeiras instalações radiofônicas do mundo, transmitindo, na época, para o centro de Recife e alguns subúrbios próximos. Estruturada profissionalmente como a rádio fundada por Roquette-Pinto no Rio de Janeiro em 1923 (ALBIN, 2006. p. 13)*

[7] *Publicação da criação da Rede EaD-SENASP no Diário Oficial da União, Seção 03, nº 198 em 14/11/2005*

[8] *Telecentros foram estruturados com telessala, sala web, sala de tutoria, sala de conexão e a devida designação de gestores portaria nº 11, de 1 de novembro de 2005*

[9] *Lei nº 11.530, de 24 de dezembro de 2007, institui o Programa Nacional de Segurança Pública com Cidadania - PRONASCI e dá outras providências.*

[10] *Bolsa Formação, decreto 6.390, de 8 de março de 2008, regulamenta o art. 8º- F da Lei nº 11.530/2007*

[11] *Relação de cursos da Rede EaD-Senasp http://portal.ead.senasp.gov.br/academico/editoria-a*

[12] *Portaria nº 50, de 04 de outubro de 2017 "Regulamenta a criação e concessão de brevê ou bóton a serem conferidos aos profissionais de Segurança Pública aprovados em cursos da Rede Nacional de Educação a Distância em Segurança Pública - Rede EaD-Senasp, em razão de seu aprimoramento intelectual". Tem o direito de uso do Brevê Bronze 20 cursos aprovados, Brevê Prata 40 cursos aprovados e Brevê Ouro 60 cursos aprovados*

CURSO DE ANALISIS FORENSE DE EVIDENCIA DIGITAL – EL PAcCTO

AUTOR: José Luis Caramé Soto, Teniente de la Guardia Civil (España)
Destinado en Unidad Central Operativa – Departamento de Delitos Telemáticos
Graduado en Derecho. Cuenta con formación y certificaciones en informática forense y lucha contra el cibercrimen

RESUMEN: En las fechas comprendidas del 28 de mayo al 1 de junio de 2018, se llevó a cabo en la ciudad de Asunción (Paraguay) un curso de Especialización en Análisis Forense y Evidencia Digital dirigida a la lucha contra la Pornografía Infantil mediante herramientas informáticas. Este curso fue organizado por EL PAcCTO1 e impartido por personal de Guardia Civil (España) y dirigido a personal de la Policía Nacional y el Ministerio Público de Paraguay. En este artículo se pretenden mostrar los aspectos de mayor importancia transmitidos a los participantes durante el desarrollo de la formación, como son los principios del análisis forense de evidencias digitales y la importancia de la tarea de identificación de víctimas en la lucha contra la explotación sexual de menores.

Palabras claves: Análisis Forense; Evidencias Digitales; Explotación Sexual de Menores; Identificación de Victimas.

Una parte esencial de cualquier investigación en el ámbito del cibercrimen es el análisis forense digital. Tiene como objetivo el **averiguar cómo se desarrollaron los hechos investigados** y, en particular, qué persona o personas se encuentran detrás del ilícito objeto de estudio. La lucha contra la explotación sexual de menores a través de internet no es una excepción en cuanto a la importancia del análisis forense para determinar la autoría de un delito.

Si bien el título de la capacitación a la que hace referencia el artículo contiene las palabras "pornografía infantil", en este artículo se evitará ese término. Es el nombre utilizado en multitud de normativas legales, pero la comunidad de expertos[1] en la lucha contra esta lacra, lleva tiempo concienciando de la importancia de usar términos como "**explotación sexual de menores**" para evitar que los archivos de este tipo de contenido sean puestos al mismo nivel que un vídeo sexual consentido entre adultos.

Los delitos que la mayor parte de legislaciones contienen en relación a la explotación sexual de menores en línea son los de **producción** (asociada generalmente a casos de abusos sexuales o utilización de menores con fines sexuales), **distribución** y **tenencia** (o acceso) a vídeos o fotografías en los que se muestran abusos sexuales a menores de edad o desnudez con fines sexuales (centrada en genitales o mostrando a los menores en posturas con una clara componente sexual). Además, son cada vez más países los que han tipificado como delito la actividad conocida como ***grooming***, actividad consistente en que un adulto, generalmente haciéndose pasar por un menor, intenta ganarse la confianza de un niño o adolescente, terminando generalmente en un chantaje o extorsión con fines sexuales.

En la capacitación desarrollada en Asunción, se estudiaron desde una perspectiva forense los diferentes aspectos dentro de una operación contra la explotación sexual de me-

nores en línea. El análisis forense tiene su importancia en prácticamente todas las fases de este tipo de investigación: identificación del posible autor o lugar donde se ha realizado el ilícito, registro en el posible lugar de los hechos, clonado del material informático intervenido y, finalmente, análisis de las evidencias digitales.

Existen muchas definiciones de lo que es el análisis forense digital. En general, todas ellas indican que se trata de la **aplicación de diversas técnicas informáticas con el objetivo de extraer información de interés** (visible u oculta) **sin alterar el estado original de la evidencia**.

Identificación del autor / lugar de los hechos

El primer paso cuando nos encontramos con un delito de explotación sexual de menores en Internet, es **averiguar quién es el autor, la víctima o el lugar donde se han cometido los hechos**.

Existen diferentes vías para lograr esta identificación, siendo en varias de ellas importante aplicar los principios de la informática forense, aunque no hayamos todavía entrado en el análisis. **La información en internet es volátil**, por lo que cualquier evidencia que hallemos que pruebe la comisión de un delito o pueda ayudar a llegar al autor (o la víctima) del mismo, debe ser documentada y preservada.

La información de interés en esta fase de la investigación es de muy diversos tipos. Obviamente, el contenido visual y sonoro de los archivos multimedia con contenido ilícito son la vía de investigación más importante en los casos de producción (aquí comienza la tarea de **identificación de víctimas**, sobre la que se hablará más adelante), pero también cualquier otro rastro que el supuesto delincuente haya podido dejar (conexiones IP, *user-agent*, apodo, perfil en redes sociales, etc).

Registro

Una vez identificado el autor de los hechos investigados o el lugar desde el que se ha cometido el delito llega uno de los momentos clave de la investigación, el registro. Se trata del mo**mento más importante de la investigación en cuanto a la obtención de evidencias se refiere**. A diferencia del resto de fases del proceso investigativo, su duración es muy limitada en el tiempo y, generalmente, no es sencillo repetirla, por lo que, si se cometen errores en la obtención y preservación de evidencias, son difícilmente subsanables.

En esta fase, normalmente en el domicilio o lugar de trabajo del autor de los hechos, debe **recogerse toda evidencia susceptible de contener información útil para el esclarecimiento de los hechos investigados**.

Puede hacerse un paralelismo entre la forma de actuar en la escena de un delito informático con la de cualquier otro delito. Si en un homicidio es importante no alterar evidencias como huellas dactilares, sangre o cabellos que puedan hallarse en el lugar de los hechos, debemos actuar de igual forma con las evidencias digitales, **evitando modificar cualquier información de utilidad para la investigación**.

Lo más obvio para cualquier investigador es el **recoger cualquier soporte digital que tenga relación con el delito**, tanto aquellos evidentes (discos duros, memorias USB, CDs, DVDs), como aquellos menos convencionales (cámaras, videoconsolas, dispositivos GPS, *smartwatches*, etc).

Pero debemos tener en cuenta también que el registro puede ser, quizá, el único momento en que se puedan obtener otras informaciones de gran interés para resolver los delitos investigados. Un claro ejemplo de esto es la información disponible en la **memoria RAM** de un ordenador. La información que contiene este tipo de memoria se destruye al apagar el dispositivo, por lo que, si no se hace un volcado de esta información de forma previa a apagar al dispositivo, cualquier dato de interés que se halle en la RAM desaparecerá para siempre. El registro es también un momento idóneo para **preservar información que se encuentre almacenada en remoto**, como pueden ser cuentas de correo electrónico, perfiles de redes sociales o servicios de almacenamiento de datos en línea. El investigado puede tener su sesión de usuario abierta en diferentes servicios de este tipo, haciendo la información accesible durante el registro.

Todos los pasos dados por el investigador durante el registro deben basarse en los principios de la informática fo-

rense, es decir, obtener la información de interés sin modificarla, siempre atendiendo, por supuesto, a la normativa legal del país del investigador y a la autorización judicial necesaria para realizar cada una de las acciones descritas. Una vez obtenida esta información debe ser preservada para evitar su modificación o destrucción.

Clonado de las evidencias originales

En el marco de un análisis forense digital correcto, el clonado es un paso imprescindible. Consiste en la realización de copias exactas de todos aquellos dispositivos que hayan sido intervenidos por su relación con los hechos investigados.

Esta copia tiene como fin **evitar cualquier modificación o destrucción de la información original**. De esta forma el analista podrá trabajar con tranquilidad y si comete algún error durante el estudio de la copia, nunca afectará a la evidencia original. De este modo, también se garantiza que, llegado el caso, la defensa del supuesto autor pueda realizar una contrapericial de la evidencia o que el investigador pruebe replicando sus pasos sobre la evidencia original que la información que ha hallado durante su análisis efectivamente se encuentra en el dispositivo intervenido.

Análisis de las evidencias

Esta fase es en la que se desarrolla el análisis forense digital propiamente dicho, pero la realización de los pasos previos de la forma correcta es indispensable para poder llevar a cabo esta tarea de forma adecuada.

El objetivo del análisis es hallar las evidencias del delito investigado para **identificar de forma inequívoca a su autor** o autores. Haciendo de nuevo un paralelismo con la investigación de otros tipos delictivos, en el análisis informático es de aplicación también el conocido **principio de intercambio de Locard**, que dice que "*siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto*". Trasladándolo al mundo informático, cualquier acción realizada con un dispositivo digital deja evidencias de dicha actividad. El objetivo del análisis forense es encontrar estas trazas.

El análisis de las evidencias debe detectar aquellos **rastros de actividades de interés**. Por ejemplo, si investigamos un caso de distribución de archivos digitales con contenido de abuso sexual a menores a través de una red P2P, será importante analizar con detalle las evidencias de actividad de aquellas aplicaciones que hagan uso de esta red.

En esta fase es importante también es detectar aquella información que aparentemente, en un análisis superficial, no parece estar ahí, pero con los procedimientos y herramientas adecuadas se puede hacer visible, como pueden ser archivos borrados, ocultos o cifrados.

El objetivo del análisis – La importancia de la identificación de víctimas

Hasta ahora se han estudiado las diferentes fases del análisis sin entrar en el objetivo del mismo. Desde un punto de vista pragmático, lo que se pretende es demostrar la autoría del hecho investigado. Por ejemplo, si tenemos un reporte de NCMEC[2] sobre el envío de un archivo pedófilo a través de una red social y encontramos el archivo en cuestión y las credenciales de la red social con las que se ha enviado, la investigación está completa.

Pero es importante pensar en cuál es el **objetivo** de este tipo de investigaciones. Lo que se busca es proteger la **indemnidad sexual de los menores**. Quedarse en el delito consistente en el envío del archivo pedófilo a través de Facebook es apenas rozar la superficie. Proteger a la infancia es una tarea global, marcada como prioridad por los países componentes de **INTERPOL** en la resolución AG-2011-RES-08[3], adoptada por la Asamblea General en noviembre

de 2011. En ella, se decide promover un manejo orientado a las víctimas del material de explotación sexual infantil a nivel nacional, mediante la recolección sistemática, el establecimiento de equipos nacionales de identificación de víctimas y la conexión a la *International Child Sexual Exploitation* (**ICSE**) *image and video database*, gestionada por INTERPOL.

En estas investigaciones es importante descender hasta el último detalle. El primero y más importante es: ¿**quién es el menor** que aparece en esa imagen? ¿de dónde es? ¿está identificado? ¿**está siendo víctima de abusos** actualmente? Además, no es habitual que una persona investigada por este tipo de delitos tenga un solo archivo, sino que tenga muchos más, y esas mismas preguntas debemos hacérnoslas sobre todos los archivos que se hallen en los dispositivos intervenidos.

Para evitar tener que comprobar cada uno de los archivos, existen **bases de datos internacionales** en las que se comparte información sobre el estado de identificación tanto de la persona que ha cometido el ilícito como de la víctima que aparece en los archivos pedófilos, siendo el mejor ejemplo la, anteriormente mencionada, base de datos ICSE.

Una vez hecho un *triage* que nos permita centrarnos en los archivos que necesitan un análisis más profundo, es donde empieza la tarea de **identificación de víctimas**. El objetivo de esta labor es identificar a autores de abusos sexuales a menores presentes o pasados y, sobre todo, **rescatar** a aquellos menores que estén siendo todavía víctima de abusos.

Es importante estudiar si los menores que aparecen en las imágenes son del entorno del delincuente. Para ello es importante analizar con detalle la **información audiovisual** de los archivos de interés, pero también los **metadatos**[4]que pueden revelar, entre otros, la ubicación donde se han creado los archivos o el dispositivo con el que han sido producidos. Este trabajo es una etapa más del análisis forense, ya que se basa en extraer información (sea multimedia o sean metadatos) mediante el uso de herramientas informáticas sin alterar la evidencia original.

El estudio de estos detalles puede permitirnos descubrir casos de abusos sexual o de producción de material de explotación sexual de menores relacionados con el investigado, su entorno o quizá otra persona en nuestro país. En caso negativo, las vías de **cooperación internacional** (como la mencionada base de datos ICSE) permiten compartir información con expertos en la materia de otros lugares del mundo para, finalmente, hallar a la víctima y, en su caso, detener los abusos de los que pueda estar siendo víctima.

La explotación sexual de menores en un **fenómeno global**. Es fácil encontrar casos en los que el agresor es de un país, viaja a un segundo con fines de turismo sexual, donde comete abusos sobre menores, graba estos abusos y posteriormente distribuye el material producido a cualquier otro lugar del mundo. Por tanto, **la lucha contra esta lacra debe enfocarse también desde una perspectiva global**. La mejor forma de colaborar en esta lucha es utilizar las vías de cooperación internacional establecidas al efecto y dedicar el esfuerzo necesario al trabajo de identificación de víctimas.

Notas

1 *International Working Group on Sexual Explotation of Children http://luxembourgguidelines.org/. Este grupo ha desarrollado una guía de terminología para armonizar términos y definiciones en cuanto a la protección de menores.*

2 *National Center for Missing and Exploited Children http://www.missingkids.com. Recibe comunicados de actividades aparentemente pedófilas reportados por los diferentes prestadores de servicios de Estados Unidos (como pueden ser Facebook, Twitter, etc.), y los remite a los países afectados.*

3 *Resolución AG-2011-RES-08 disponible en castellano en https://www.interpol.int/content/download/12398/85465/version/4/file/AG-2011-RES-08Es.pdf*

4 *Los metadatos son "datos sobre el dato". Generalmente incluyen información como la fecha de creación de un archivo, de modificación, etc. En archivos multimedia puede guardar información también sobre el dispositivo que han sido creados, la ubicación, etc.*

INSTITUTO SUPERIOR DE EDUCACION POLICIAL DE LA POLICIA NACIONAL DEL PARAGUAY

AUTOR: Policía Nacional

RESUMEN: En el año 1935 no se podía hablar de Policía de seguridad como una institución, dicha función era ejercida por voluntarios y por la guardia territorial quienes eran considerados como eficaces garantías del orden y la tranquilidad de la población, pero en la época ya la sociedad consideraba que la función policial debería constituirse como una profesión, a fin de disponer de agentes aptos y conocedores de sus deberes. Con tal objeto fue creada una Escuela de Policía en la Capital, cuya organización propuso mejorar con el correr del tiempo para que las ciudades y municipios sean cubiertos por estos ciudadanos egresados de la escuela y miembros de esta institución y no individuos tomados al azar.

El plantel de profesores fue conformado por un grupo excepcional de distinguidas personalidades, quienes sin otros intereses que la de contribuir con un emprendimiento tan noble y patriótico (todos aceptaron el cargo ad honoren), se prestaron generosamente con un caudal de inteligencia y vocación docente, al esfuerzo primigenio que fundó las bases de la primera casa de enseñanza profesional Policial. Según testimonios memorativos de los alumnos de aquella época la vida cuartelera era rigurosísima ciento por ciento espartana, con rigor altamente disciplinario, digna de la mejor tradición prusiana.

Tras dos años de intensos estudios, egresaron los primeros 47 Oficiales de Orden Público Tránsito e Investigaciones (OPTI), para las siguientes promociones el ciclo lectivo ya se extendió a tres años de duración.

Aún con todos los problemas y limitaciones previsibles en una entidad educativa recientemente formada y de muy escasos recursos económicos, no puede decirse sin embargo, que la primera Escuela de Policía fuese deficitaria en el cumplimiento de la alta misión encomendada, como fuerza rectora del pensamiento y la militancia profesional de varias remesas de jóvenes ciudadanos paraguayos que tomaron sobre sí, una elevada exigencia y el difícil ideal de ser "guarda del hermano" como representantes dignos de servidores heroicos y leales agentes de la Institución guardiana de la paz y el Orden Público.

La escuela adquirió definidos perfiles. En lento pero seguro proceso, afianzó, dio vida y continuidad a sus fundamentos conceptuales, así como fue dando vigor y consistencia a su esquema organizativo, para dar lugar a la creación de la Dirección de Institutos Policiales de Enseñanza encargada de la coordinación de las actividades educativas de la escuela de formación policial que fueron creándose a través de los años. La ley Nº 867 "Orgánica Policial de la Policía de la Capital" de 1982 establece según el artículo 211 la función de: "planificar, coordinar, orientar, supervisar y hacer cumplir los planes y programas de enseñanza".

Posteriormente se elaboraron proyectos que de alguna manera contribuyeron a evolucionar la educación Policial, que permitió la incorporación por el Ministerio de Educación y Cultura bajo la Resolución número 10.721 del año 2002 como parte del Sistema de Educación Nacional , que

dio lugar a la elaboración y presentación de un proyecto que sirvió para la promulgación de la Ley 2946/06; Que Reconoce al Instituto Superior de Educación Policial y la habilitación por la Agencia Nacional de Evaluación (ANEAES) que finalmente abrió la posibilidad de la creación de un Sistema de Educación, conforme a las aspiraciones y políticas de la fuerza policial, haciéndose necesaria la creación de un establecimiento de nivel universitario con validez nacional, orientado a afianzar la profesionalización de la misma, y lograr potenciar su nivel en materia científica y técnica.

Desde el año 2006 el Instituto Superior de Educación Policial (ISEPOL) es la entidad responsable de la formación personal, académica y profesional de los estudiantes a través de la implementación de planes y programas de estudios en el campo de las Ciencias Policiales, orientados a desarrollar una educación crítica y reflexiva en procesos de formación y perfeccionamiento permanente, que favorezca el desenvolvimiento profesional con efectividad en la función policial. Generar capacidad de análisis, de organización y de acciones estratégicas, combinando convenientemente la teoría y la práctica, con un enfoque multidisciplinario y sistémico, tendientes a la prevención de los hechos punibles, al mantenimiento del orden público, la seguridad de las personas y sus bienes, en búsqueda constante de competencias, habilidades y aptitudes que ayuden a diagnosticar, prevenir y/o rectificar acciones que favorezcan la utilización racional de los recursos y la optimización de las gestiones de pertinencia institucional en pro de la seguridad ciudadana.

El Instituto Superior de Educación Policial con doce años de vida institucional, ofrece actualmente varias ofertas educativas de formación, capacitación, actualización, especializaciones y maestrías, en el ámbito de las ciencias policiales, conforme a la ley Nº 4995/13 de Educación Superior y otras normas vigentes. Cada unidad académica componente del ISEPOL, administra según la misión particular; cursos, carreras y programas, con un diseño curricular orientado al logro de las competencias profesionales, en respuesta a la necesidad de la institución policial y a la política de seguridad interna del estado.

El proceso de admisión de postulantes a los distintos cursos, carreras y programas ofertadas por el ISEPOL a través de las unidades académicas se han consolidado con el mejoramiento constante de los reglamentos de admisión como así también el logro del acuerdo específico de cooperación interinstitucional entre la Universidad y Nacional de Asunción y la Policía Nacional, obteniendo eficacia, seguridad, objetividad en la evaluación, precisión y rapidez en la publicación del resultado de los exámenes vía internet, en la página web del Centro Nacional de Computación de la Universidad Nacional de Asunción y del Instituto Superior de Educación Policial.

El Instituto Superior de Educación Policial, para el cumplimiento de sus fines se estructura orgánicamente en Dirección General; Consejo Asesor Superior; Dirección de Postgrado y Capacitación; Dirección de Grado; Dirección de Pregrado; Secretaría General; Asesoría Técnica Pedagógica; Departamento de Cultura y Becas; Departamento de Estudio, Evaluación y Acreditación; Centro de Investigación; Centro de Recursos Didácticos; y Sub Unidad de Administración y Finanzas.

La Dirección General del Instituto Superior de Educación Policial, es el órgano central, responsable de planear, organizar, dirigir, coordinar y supervisar los cursos, planes y programas desarrollados en las unidades académicas dependiente del ISEPOL.

El Consejo Asesor Superior del Instituto es un órgano de decisión y asesoría del Instituto Superior de Educación Policial, con carácter permanente, profesional, técnico, de alta especialización en materias policiales, pedagógicas, administrativas y jurídicas.

La Dirección de Posgrado y Capacitación a través de las unidades académicas que la integran ofertan programas de Especialista en Seguridad Pública; Especialista en Inteligencia e Investigaciones; Maestría en Gestión y Asesoramiento Policial; Maestría en Ciencias Policiales. Los programas de las maestrías ya cuentan con resolución de habilitación de los programas académicos respectivos por el Consejo Nacional de Educación Superior.

La Dirección de Grado a través de las unidades académicas que la integran ofertan carreras de Licenciatura en Ciencias Policiales; Licenciatura en Criminalística; Licenciatura en Entrenamiento Físico Policial, todas ellas con resolución de habilitación por el Consejo Nacional de Educación Superior.

La Dirección de Pregrado a través de las unidades académicas que la integran ofertan cursos de Tecnicatura en Seguridad Pública; Tecnicatura en Seguridad Urbana y Turística; Tecnicatura en Operaciones Tácticas Policiales; Tecnicatura en Estudios Musicales, todas ellas con resolución de habilitación por el Ministerio de Educación y Ciencia.

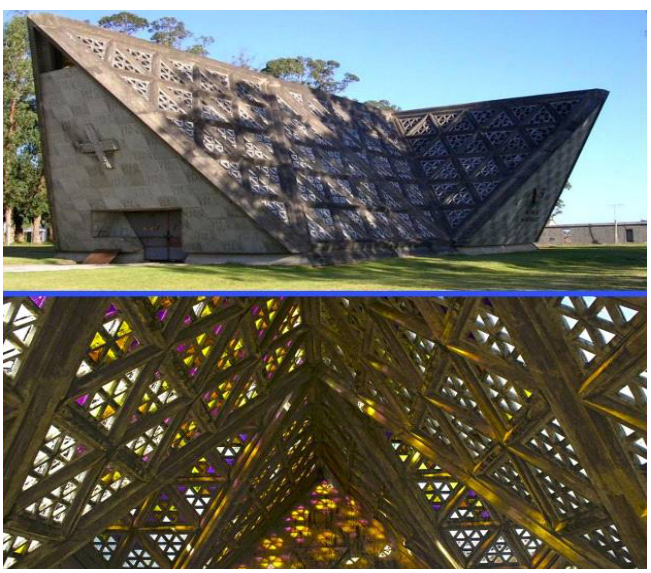
SOCA: TAN CERCA, TAN LEJOS

AUTOR: Of.Ppal.Jorge Mila Brun

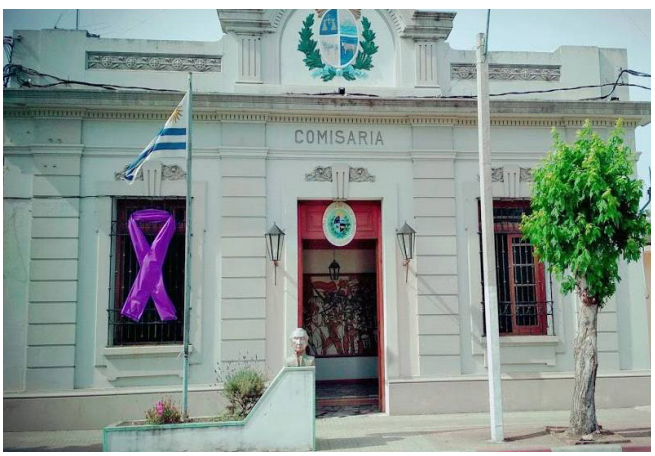
RESUMEN: La Ciudad "Dr Francisco Soca" es una pequeña ciudad del Departamento de Canelones, que guarda entre sus calles valiosos trozos de historia y una situación delictiva inusual en el Uruguay actual que da lugar a un desarrollo importante de aspecto Social Comunitario de la Policía.

Sobre el actual trazado de la Antigua Ruta Nacional N° 8, a la altura del Kilómetro 57, sobre la Margen Este del "Arroyo Mosquitos", se encuentra la Ciudad "Dr Francisco Soca".

Un pequeño poblado que no supera las 3.000 personas, sus calles anchas guardan postales de un Uruguay del 1900: un viejo cine con capacidad para 700 personas permanece intacto, sin vandalizar, sin grafittis, tras un manto de fino polvo su interior aun resguarda la antigua máquina de proyecciones cinematográficas; una espaciosa y arbolada plaza se ubica en el centro de la ciudad, mirada por la Capilla "Santo Tomás de Aquino", el antiguo Liceo, la Policlínica, el Juzgado, el Municipio; impecable y prolija; la "Capilla Susana Soca", obra del Arquitecto Catalán Antoine Bonet, de hormigón armado y vidrio, es uno de los tesoros arquitectónicos de la Ciudad.



La comisaria, con inmensas puertas de madera, ventanales altos con rejas, coronada por un inmenso Escudo Nacional empotrado en la mampostería del exterior, se erige como un faro, como un referente de la historia reciente de nuestro país y un guardián, no solo de los derechos y garantías de la sociedad, sino también de una de las obras del pintor uruguayo Carlos Paez Vilaró que engalana el hall del edificio.



En las calles, el tiempo parece haberse detenido, quizá en alguno de los famosos paradores de la década del 50',hoy vacíos; las casas permanecen de puertas abiertas, las ventanas sin rejas , los cercos poco mas que decorativos, los niños jugando en las calles hasta altas horas de la noche, los

vehículos afuera, sin trancar y muchas veces con los vidrios bajos, dan cuenta de un Uruguay distinto al que conocemos.

Con mas de 500 Km2 de Territorio, la Jurisdicción del Área de Seguridad 8va, presenta un 80% de zona rural, abocada principalmente a la producción ganadera, la forestación y las actividades ecuestres, destacándose el funcionamiento de mas de 40 haras.

Pese a la basta extensión de zona rural, el principal delito que se registra en esa zona y que refiere a la matanza y/o sustracción de animales, presenta un promedio anual en los últimos 10 años (2007 –2017) de quince denuncias por año, presentando el más alto índice en 2009, donde se registran 26 hechos.

El Hurto, uno de los delitos que presenta los mas altos índices a nivel nacional, en el mismo periodo presenta un promedio de cincuenta y tres denuncias por año, presentando el mayor registro en 2016, año en que se registraron 84 eventos.

La rapiña, un tipo delictivo que preocupa por el imperio de la violencia inminente para que se configure, por la plurisubjetividad de los derechos afectados, y por ser un indicador del *"deterioro y el descrecimiento del valor de la vida propia y ajena"*, registra un promedio de una denuncia anual entre 2007 y 2017 ,presentando el mas alto índice en 2016, año en el que se registran tres hechos.

El homicidio, el tipo delictivo que por definición es el mas violento, y el que afecta el Derecho Humano mas preciado: la vida, apenas aparece en la estadística delictiva de la ciudad de Soca, en 10 años no se registran hechos de muertes que configuren como tal.

Esencialmente las tareas que se realizan en la Seccional pueden agruparse en policiamiento administrativo y de gestión de denuncias, policiamiento prevento represivo y policiamiento comunitario.

Promedialmente se gestionan 890 eventos al año mediante el Sistema de Gestión de Seguridad Pública que abarcan Delitos, Faltas, Siniestros y Novedades de carácter administrativo.

Las tareas prevento represivas, se gestionan en función de la georeferenciación del delito y la aglomeración de eventos en un determinado punto en el mapa de la ciudad de acuerdo a los eventos ingresados mediante el Sistema de Gestión de Seguridad Pública.

Finalmente el Policiamiento Comunitario, compuesto por un conjunto de estrategias de acercamiento a la comunidad, idealizada en función de temáticas que atañan y preocupan a la sociedad:

"Violencia Basada en Género y Generaciones", generándose instancias de concientizacion y jornadas de capacitación destinadas a la población en general, técnicos de trabajo social comunitario y policías en diferentes temáticas: "No me digas Feliz día" (Actividad realizada en marco del 8 de Marzo), talleres sobre Violencia Doméstica, cine-foro sobre Trata y Tráfico de personas en conjunto con CONNAPES[1], Sensibilización para el tratamiento de la población trans conjuntamente con la Comisión de Género de la Intendencia y el Colectivo Ovejas Negras, Talleres sobre Bullying con docentes y embarazo adolescente con la médico referente de la comunidad.

"Siniestralidad Vial", destacándose sobre esta temática la realización de "Escuelitas de Tránsito" en las Escuelas Primarias que Funcionan en la Jurisdicción, explicándose a los niños que participan de ellas lo concerniente a la reglamentación de tránsito, señales viales y aspectos de seguridad en la conducción de bicicletas, jornadas lúdicas en el marco del "Mayo Amarillo" para lo que se integran todas las instituciones educativas de la ciudad, desde los centros de atención a la primera infancia, escuelas primarias, liceo y Escuela Técnica, también se dictan charlas de "Manejo y Transporte" destinada a conductores de camiones, desarrolladas con apoyo de la Dirección Nacional de Policía de Tránsito y las empresas de transporte pesado con asiento en la ciudad; este año de acuerdo a la consigna de la UNASEV[2] **"VOS CON DROGAS AL VOLANTE #MALAIDEA"** se desarrollaron diferentes intervenciones en territorio, haciendo participe a la población, recorriendo una pista de obstáculos bajo los efectos de las drogas simulados por lentes que entorpecían la visual del recorrido.

"Drogadicción y Consumo de Drogas", sobre esta temática se han realizado diferentes charlas y talleres en especial con adolescentes, apoyados por la médico referente de la localidad y el Jefe del Departamento Anti Drogas de Pando, así como charlas al personal de la unidad referente al Protocolo de Actuación Policial sobre Ley de Marihuana y sus derivados.

Anualmente se realizan varias Escuelas de Seguridad Ciudadana, consistentes en charlas, talleres y seminarios destinados a formar ciudadanos como Promotores en Seguridad Ciudadana, los cuales reciben capacitación sobre el funcionamiento de una Unidad Policial, Policía Científica, Violencia Doméstica, Drogas, el Servicio 9.1.1 y el Marco Normativo y Legal, asímismo se plantean algunos temas optativos según los intereses del público asistente como por ejemplo tenencia responsable de armas de fuego y delito automotor; los promotores trasladan estos conocimientos al barrio, convirtiéndose en referentes tanto para los demás ciudadanos como para la policía, mejorando notoriamente las solicitudes de respuesta policial. Además la Escuela de Seguridad Ciudadana se constituye en la base metodológica para la conformación de espacios de trabajo conjunto como las Mesas Locales de Convivencia y Seguridad Ciudadana, y para llevar adelante de forma exitosa el programa "Vecino Alerta."

Actualmente en la ciudad se encuentra funcionando una Mesa Local de Convivencia y Seguridad Ciudadana que se encuentra conformada desde el año 2013 y se reúne los primeros martes de cada mes bajo la denominación "Red Social Soca" estando integrada por un representante de cada una de las instituciones que funcionan en la zona, autoridades locales, comunicadores y ciudadanos que se acercan a participar, desde este espacio interinstitucional se conforman actividades mensuales para la comunidad y se tratan diversas problemáticas, articulándose desde allí con el responsable institucional, buscando una pronta y eficaz solución al problema.

Otro espacio que funciona en la localidad es el llamado "Espacio de intervisión", que se genera tras visualizarse la necesidad de poder contar con un espacio técnico donde quienes toman contacto con una situación de violencia, vulneración de derechos, abandono u otra para lo cual sea necesario la reunión de quienes trabajan el problema desde sus distintos ámbitos para poder judicializar la situación o allanar el camino a la institución que trabajará el problema. Desde este espacio se generan recomendaciones a ONG's, se articulan programas de realojamiento y asignación de viviendas para familias en situación de construcción irregular y se confeccionan informes a la justicia, en el que cada técnico informa desde su óptica profesional una situación.

La mayor riqueza a nivel profesional que presenta la comunidad de Soca es brindar las condiciones ideales para un desarrollo de una actividad comunitaria variada, pudiendo realizar distintos talleres, instancias formativas de sensibilización y capacitación, generar proyectos , así como tener un acercamiento cabal con la población, instancias que muchas veces, en otras localidades donde los índices de criminalidad son mas altos, no da lugar a un desarrollo tan diverso de esta metodología de trabajo

Notas

(1) Comité Nacional para la Erradicación de la Explotación Sexual comercial y no comercial de la niñez y la adolescencia.

(2) Unidad Nacional de Seguridad Vial

CESIÓN DE DERECHOS DE AUTOR

NOMBRE/S COMPLETO/S, profesión, cargo, remito el artículo denominado "**NOMBRE DEL ARTÍCULO**", de mi autoría, para análisis del Cuerpo Editorial y posible publicación en la **Revista MERCOPOL - Año XI N° 11/2018**.

Declaro que hago pública mi responsabilidad en torno al contenido de la obra y autorizo su reproducción. El artículo representa un trabajo original, que no ha sido publicado y no está siendo considerado para publicación en otro periódico, impreso o electrónico, tanto en parte o en su totalidad.

Declaro que el artículo cumple las normas para publicación, las cuales fueron leídas y acatadas por el autor. En caso de aceptación del artículo para publicación en la **Revista MERCOPOL - Año XI N ° 11/2018**, estoy de acuerdo con posibles modificaciones de forma que tengan el objetivo de adecuar el texto, al patrón editorial / diagramación de la revista y con la realización de revisiones complementarias, desde que, en ambos casos, se resguarden el contenido y las ideas del texto original.

En el caso de la publicación del artículo en la **Revista MERCOPOL - Año XI N ° 11/2018**, los derechos de autor a él referentes serán de propiedad exclusiva de la revista, siendo a mí vedada su reproducción, total o parcial, en cualquier otra parte o medio de divulgación, impresa o electrónica, sin la previa autorización de los editores de la Revista MERCOPOL.

Por ser expresión de la verdad, firmo el presente término.

Ciudad, fecha/mes/año

F I R M A

Nombre Completo

MERCOSUR

CIBERCRIMEN
Y CIBER SEGURIDAD