XXXIII
TECMUN

Asamblea General de la Organización Internacional de Policía Criminal

Delegados, jueces, embajadores, ministros, fiscales y compañeros:

Son diversas las acciones que nos llevan a corromper la paz y obstaculizar el crecimiento; sin embargo, hay dos actitudes que considero las más perjudiciales para nuestro progreso: la ignorancia y la indiferencia. A mi parecer, una más grave que la otra. La primera se resume en la falta de información y conocimientos sobre conceptos, que sin importar el nivel de dificultad, son vitales para el desarrollo del ser humano, así como la negligencia de las personas de adquirir estos conocimientos inclusive cuando tienen un deber moral o legal. La segunda, y la más grave, se basa en el comportamiento indistinto ante las situaciones que nos afectan tanto individualmente como colectivamente, sin importar el conocimiento adquirido acerca de éstas. Se puede tener la información, pero predomina la inactividad. Ambas representan el mayor peligro para nuestro futuro y lamentablemente están cada vez más presentes, en todos los sectores y en todas las edades.

Todos somos un engrane, que sin importar el tamaño, es fundamental para el funcionamiento de un reloj. En este caso, de una sociedad. Si un engrane falla, el sistema completo cae. Las acciones que decidas llevar a cabo, o la falta de éstas, van a dictar tu porvenir y el de tus alrededores. No se trata de esperar a que alguien tome riendas en el asunto con la convicción de que la decisión que tome, sea la más apta para un futuro del cual eres protagonista. No se trata de estar a la espera de tiempos mejores con la ilusión de que en algún momento llegarán. Se trata de crear y trabajar por un futuro en el que el diálogo y el intercambio de ideas está presente en todos los sectores y en todas las edades; en el que la gente quiera estar informada para poder ser partícipe en la toma de decisiones.

Debemos dejar de ser espectadores del cambio si realmente queremos ver un progreso y empezar a ser intérpretes de nuestro propio futuro. Aprovecha la oportunidad que se te presenta el día de hoy y las herramientas que te brinda TECMUN para trabajar por un futuro en el que la participación ciudadana y la responsabilidad social son los actores principales que van a dictaminar las decisiones que va a llevar a esta sociedad, a este gran reloj, a trabajar de la manera más efectiva posible.

_____

Gisela Anahí Lima Castillo
Subsecretaria General de la Asamblea General
XXXIII TECMUN

Delegado:

Ya he estado aquí antes. Recuerdo que tenía 13 años, y sí, estaba aterrada. Nunca había estado tan aterrada en mi vida. Yo sé que es difícil pararse enfrente de otros sólo para dar a conocer tu punto de vista, sintiendo que tus ideas son erróneas, que no eres lo suficientemente bueno. Pero delegado, te aseguro que lo eres. Tus ideas valen la pena ser escuchadas, tu forma de ver el mundo no está mal sólo por el hecho de ser diferente y te aseguro que eres más fuerte de lo que crees. Espero que puedas recordar estas palabras por los siguientes tres días de debate, pero también espero tener la fortuna de que conserves mi mensaje por el resto de tu vida. El mundo ha cambiado demasiado desde que yo me senté ahí por primera vez, con una placa de la delegación de China. Desafortunadamente, no ha cambiado para bien y en la actualidad ustedes tienen más retos con los que lidiar que los que yo tuve cuando era más joven. La sociedad está perdiendo sus valores, la corrupción está tomando control de los más vulnerables, la discriminación es un problema con el cual debemos de lidiar día con día y estamos destruyendo nuestro planeta como si no hubiera un mañana. El día de hoy les pediré que me hagan el favor más grande que alguna vez haya pedido: Sean la diferencia. En un mundo rodeado de monotonía, sean la diferencia. El mundo es inmenso, no hay fronteras para los soñadores. Sé un alma libre cada día de tu vida y deja un pedazo de ti en las vidas de los que te rodean. Ten ideas locas que nadie pensaría, sé original, sé curioso. En un mundo lleno de inseguridades, sé la diferencia. Sé feliz, comparte tu sonrisa con cada persona con la que tengas oportunidad, porque nunca se sabe quién podría necesitarla. Quizá tú podrías necesitar la de ellos. Sé leal a quién eres en realidad, sé leal a lo que crees, entonces nada ni nadie será lo suficientemente fuerte para tirarte. Ayuda con cualquier cosa que puedas si hay alguien que te necesite. Ayuda a tu familia, amigos, e incluso a extraños. Todos comenzamos siendo extraños. En un mundo alimentado por demonios, sé humano, sé la diferencia. Sé respetuoso con los que amas, con los que te han lastimado y con los que puedas odiar. Ten empatía, sé amable y sé honesto. Por favor, salva los valores que nos hacen virtuosos. Cambia el mundo siendo la diferencia. He crecido con el sueño de dejar un mundo mejor a las generaciones que vienen, pero no seremos capaces de hacerlo solos. Aún sigo aterrada, temerosa de que nada de lo que pueda llegar a decir logre enriquecer el modo en el que vives tu vida, que esto no se quede guardado en tu memoria, en tu corazón. Temo que el mundo siga cayéndose a pedazos y que no logre ser la diferencia que me propuse ser. A pesar de todo tengo esperanza, y la esperanza es la única cosa más fuerte que el miedo. Ahora más que nunca alza tu voz por lo que es injusto, esparce tus palabras en cada rincón de todo corazón latiente, sé lo suficientemente valiente para expresarte, porque no importa lo que cualquiera pueda decirte, las palabras y las ideas pueden cambiar al mundo. Hazte escuchar.

Ivana Naomi Millán Flores
Asamblea General de la Organización Internacional de Policía Criminal
XXXIII TECMUN

Antecedentes de la Asamblea General de la Organización Internacional de Policía Criminal

La Organización Internacional de Policía Criminal (INTERPOL) se creó en 1923 con la visión principal de convertirse en la organización responsable de facilitar la cooperación policial internacional, a fin de hacer del mundo un lugar más seguro. Tiene su Secretaría General con sede en Lyon, Francia, y se ha convertido en la organización policial internacional más grande del mundo, contando actualmente con ciento noventa países miembros con la única misión de prevenir y combatir el crimen a través de la innovación y la cooperación en asuntos policiales y de seguridad. La Asamblea General es el órgano supremo de la organización y se reúne anualmente para tomar decisiones cruciales en torno a sus políticas, recursos, métodos de trabajo, finanzas, actividades y programas. El principal objetivo de la organización es abordar crímenes de impacto internacional, tales como terrorismo, ciberdelitos, genocidios, trata de personas, tráfico de drogas o crimen organizado. INTERPOL cuenta con equipos de respuesta especializados, análisis de inteligencia criminal, gestión de fronteras, avisos de color, intercambio de datos y análisis forenses para garantizar el éxito de las operaciones policiales, y a su vez la captura del mayor número de criminales posible.

Tópico A

Medidas para erradicar la ciberdelincuencia en América Latina y el aumento del *Phishing* en la región

Por: Ivana Naomi Millán Flores
Sofía Mitre de Jacobis

Durante el monzón de agosto de 1947, el Imperio británico debilitado por la Segunda Guerra

Introducción

En América Latina ha habido un gran aumento de la ciberdelincuencia en los últimos años. Según la cadena de noticias británica BBC, se estima que durante el 2017 han habido hasta doce ataques cibernéticos por segundo a lo largo del mundo. Dichos ataques abarcan todo tipo de software que haya sido diseñado con el propósito de dañar los aparatos electrónicos conectados a la Web y realizar el robo de datos de identidad. Dentro de esta última categoría se encuentra uno de los crímenes más comunes a nivel global, y que está afectando a la economía de varios países latinoamericanos. El *phishing* es una estrategia que utilizan las personas para extraer información ya sea personal o bancaria de una o varias personas por medio de estafas, como por ejemplo al hacerse pasar por un banco o alguna otra compañía en la cual tengan que dar sus datos para registrarse. Este tipo de ataque constituye hasta el 40% de los ataques cibernéticos y se estima que a países tales como México les ha llegado a costar hasta 150 millones de pesos (El Financiero, 2017). Dentro de América Latina, de acuerdo a un estudio realizado por él Anti-Phishing Working Group (APWG), Argentina, Brasil, México, Chile y Perú son los países más afectados por hackeos de esta índole, juntos conformando el 95% de los casos de malware y *phishing*, pero con aún más importancia, Brasil, Perú y México son los países de esta región con mayor desarrollo de malware dentro de sus fronteras, siendo blancos fáciles para los hackers que practican el *phishing* como primera herramienta de estafa.

Antecedentes de los países involucrados

En América Latina un gran número de empresas y organismos gubernamentales reciben constantes amenazas de *phishing*, provocando que aproximadamente el 60% de ellos considere que su información corre el riesgo de ser robada y extraída para propósitos ilícitos (Tendencias de Seguridad Cibernética en América Latina y el Caribe, 2014). Solo durante el último año se estima que un 30% del total de empresas latinoamericanas han sido atacadas por este fenómeno, siendo entre los casos más comunes la extracción de datos sobre cuentas corporativas y el fraude (Montalvo, 2017). Respecto a la región, alrededor de 667 millones de amenazas han sido bloqueadas por la compañía de seguridad informática Kaspersky durante el 2017, lo cual representa un aumento con respecto al 2016 de 59%, desglosado en un promedio de 117 ataques por hora, 33 por segundo. (Kaspersky Lab, 2017). Las cifras han alarmado a la comunidad internacional, y diversas investigaciones y estudios han sido requeridos en la región para la evaluación de la situación actual.

Según las declaraciones de la unidad de negocio *Westcon-Comstor*, en Latinoamérica la ciberseguridad representa un mercado multimillonario a partir de las grandes cantidades de capital que se invierten en ella. Durante 2017, la inversión total en ciberseguridad constó de aproximadamente 120 billones de dólares, de los cuales 12 billones pertenecen a lo invertido sólo en América Latina. A pesar de esto, el capital no basta para prevenir los daños causados por los hackers y cibercriminales. Un estudio realizado a 32 países latinoamericanos por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) reveló que cuatro de cada cinco países no cuentan con un centro de comando y control de seguridad cibernética, mismos que no cuentan con proteccion anti *phishing*, a la vez que demostró la inneficiencia de los protocolos Concluyendo en que la gran mayoría de estos países para perseguir los delitos cibernéticos.

La Unión Internacional de Telecomunicaciones lanza anualmente el estudio *Global Cyber Security Index*, cuyo ejemplar del 2017 coloca a México en la primera posición de su lista de países de América Latina y el Caribe con mayor compromiso hacia la ciberseguridad. Por otro lado, el estudio indica que los países con más usuarios que han registrado ataques de malware durante el 2017 son Brasil, México y Colombia. A su vez, Brasil fue considerado el país más peligroso en Latinoamérica respecto a amenazas cibernéticas per cápita de usuarios, de entre los cuales el 30% salió afectado por los ataques.

En Argentina, el 19 de septiembre de 2011 fue presentado un proyecto para sancionar el *phishing*, mejor conocido como Proyecto de Ley para tipificar el *Phishing* o Captación Ilegítima de Datos en el Senado de la Nación. Mediante este proyecto se busca combatir las diferentes técnicas de obtención ilegítima de información personal. Por otro lado, dentro de Chile no existe en el Código Penal un artículo que sancione el phishing, sin embargo, los tribunales recurren a la figura de la estafa tradicional para castigar estas conductas.

Antecedentes sobre el crimen

Phishing

El *phishing* es un término que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando

también llamadas telefónica o *pharming*. Esta última técnica se caracteriza por explotar una vulnerabilidad de los servidores DNS al permitir que el atacante redireccione un nombre de dominio a otra máquina distinta. El objetivo principal de este tipo de criminales es robar la información personal de distintos usuarios para usarla a su favor. Dado el creciente número de denuncias de incidentes relacionados con el *phishing* y *pharming*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas, sin embargo no todos los países han logrado aplicarlas.

Los intentos más recientes de *phishing* han tomado como objetivo a clientes de bancos y servicios de pago en línea, siendo estos seleccionados aleatoriamente. Sin embargo, se ha demostrado que los *phishers* son capaces de establecer conexiones con el banco o servicio de una posible víctima de su preferencia, y de este modo enviar el correo electrónico apropiado. Esta variante hacia objetivos específicos en el *phishing* se ha denominado *spear phishing*. Pero los usuarios de bancos no son los únicos en riesgo de vivir un ataque tipo *phishing*. A finales de 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace, redireccionando los enlaces de modo que dirigieran a una página web falsa diseñada para robar información de ingreso de los usuarios. A partir de ese momento, se empezaron a tomar acciones para comprender la vulnerabilidad de las redes sociales frente a este tipo de crímenes. Algunos experimentos han otorgado una tasa de éxito de hasta 90% en ataques *phishing* en redes sociales, alertando así a la comunidad internacional (Kaspersky Lab, 2014).

La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. Los URLs manipulados, o el uso de subdominios, son trucos comunes utilizados por *phishers*. Otro método popular de *phishing* es conocido como *Cross Site Scripting*, donde el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. El criminal dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. Los usuarios verifican sus cuentas en esta página fraudulenta, y en seguida acceden a la pagina oficial por medio de un enlace que se les proporciona para continuar con las operaciones que el cliente desee realizar.

El *Addline Pishing* es otro tipo de técnica en el que se hace referencia a una doble suplantación de identidad, donde el criminal es capaz de acceder de forma fraudulenta al

computador o dispositivo móvil de la víctima, y robar información de más de una cuenta personal. La técnica nació en Estados Unidos a mediados del año 2013, y desde entonces se ha hecho famosa alrededor del mundo por su eficacia. El atacante usualmente roba de tres a cuatro cuentas que estén disponibles dentro del ordenador o móvil al que este tenga acceso, robando así la información de diversas aplicaciones con el propósito de realizar operaciones fraudulentas a nombre de otra persona. Los servicios más afectados por el robo de datos son cuentas bancarias, correos electrónicos, PayPal, Amazon, entre otros. Los fraudes son casi imposible de rastrear ya que las operaciones fraudulentas se realizan desde cuentas con permisos, y usualmente utilizan aplicaciones para ocultar la dirección de la computadora hackeada desde un inicio.

Los daños causados por el *phishing* oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Los negocios en los Estados Unidos pierde cerca de dos mil millones de dólares al año mientras sus clientes eran víctimas de este tipo de delitos, mientras que el Reino Unido pierde aproximadamente doce millones de libras esterlinas. Sin embargo, este tipo de estafas no sólo afectan a grandes corporaciones, sino también a la población en general, siendo el robo de identidad uno de los delitos más comunes. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los *phishers*, incluyendo números de tarjetas de crédito y números de seguridad social. Con la información obtenida del robo de identidad, los criminales pueden realizar numerosas actividades fraudulentas dentro de las cuentas bancarias de las víctimas, tales como la creación de nuevas cuentas para compras ilícitas, sustracciones económicas o incluso total acceso y control de redes sociales, correos electrónicos y teléfonos móviles, poniendo en riesgo no sólo a la víctima del fraude, sino también a quienes la rodean. Esto convierte a este tipo de fraude cibernético en un peligro no solamente económico, sino que logra tener un impacto social y de seguridad nacional.

Desde 2001, la Unión Europea cuenta con el marco legal necesario para tratar adecuadamente crímenes de este índole, siendo una de las primeras regiones en tomar acciones legales en contra de los crímenes cibernéticos. La Decisión Marco del Consejo de Ministros de la Unión Europea dispone en su art. 3º que cada estado miembro debe adoptar las medidas necesarias para castigar, prevenir y erradicar la realización de transferencias de dinero, ya sea mediante la alteración y robo de datos informáticos o datos de identidad. El *phishing* o fraude cibernético también tiene sus repercusiones legales que varían dependiendo de los sistemas de justicia de cada país, siendo el promedio de condena entre diez y doce años de prisión, a pesar

de que en países como Turquía esta sentencia puede llegar hasta los 300 años. Por otro lado, aún existen ciertas regiones del mundo donde no se tiene una sentencia establecida, por lo que en la actualidad se busca establecer parámetros claros para poder desarrollar un mejor sistema de condena en materia de ciberseguridad.

El "Phishing" en América Latina.

Durante Septiembre de 2017, un informe realizado por la compañía de desarrollo de software de ciberseguridad VU informó que el *phishing* es la modalidad de cibercrimen más frecuente en América Latina. El estudio, en el que participaron seiscientas organizaciones de dieciocho países, entre los que se encuentran Colombia, Argentina, Chile, Bolivia, Nicaragua, Perú, Venezuela y Ecuador, referencia los problemas más comunes de seguridad informática a nivel corporativo, señalando que el 41% de los casos de *phishing* se confirmaban dentro de estas organizaciones. Por otro lado, las agencias gubernamentales quedaron en el segundo lugar, teniendo 29% de los casos de *phishing* en América Latina.

Durante la primera mitad de 2017 se registraron 677 millones de ataques cibernéticos en América Latina, lo que implica un alza del 59% comparado con las cifras de 2016 (CNN, 2017). Los ataques son dirigidos principalmente al sector salud, así como a pequeñas y medianas empresas, siendo el *phishing* la amenaza con mayor impacto en América Latina. Según Kaspersky, Brasil, México y Colombia son los países que más ataques cibernéticos han sufrido durante 2017, siendo los dispositivos móviles el nuevo objetivo de preferencia para los fraudes informáticos. Las pérdidas del sector financiero latinoamericano a causa de las deficiencias relacionadas con la ciberseguridad alcanzan los mil millones de dólares anuales. A pesar de esto, en muchos países de la región el marco legal para erradicar la ciberdelincuencia se ve entorpecido por la ineficacia de las normativas nacionales.

Casos recientes

Los registros realizados por el Banco de México (Banxico) posicionan a México en la posición número ocho entre los países donde más se presenta el robo de identidades mediante el *phising*. Solo en los primeros tres meses del 2017 se cometieron 18 mil fraudes cada día en el país, siendo el comercio electrónico la vía a través de la cual ocurren el 91% de los fraudes cibernéticos. A su vez, solo durante el mes de marzo de ese mismo año se registraron 3,682 casos, cifra histórica para este tipo de delito. Esto provocó fuertes acusaciones hacia las compañías bancarias, tales como Santander, Citibanamex, BBVA Bancomer, HSBC y Banco

Azteca, principalmente por situaciones de robo de identidad o de datos confidenciales, consumo de recursos de redes corporativas, pérdidas económicas y fraudes.

A mediados del año 2017 la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) alertó a los usuarios sobre un caso identificado de *phishing* por parte de la empresa Apple. Por medio de la aplicación iCloud los delincuentes estaban teniendo acceso a los datos financieros de las tarjetas que se encontraban registradas por los usuarios, advirtiendo a la población sobre los peligros que traía consigo el use de esta aplicación sin el debido cuidado. Sin embargo, este no es el caso más sonado de *phishing* dentro del país. Un ataque de *phishing* masivo afectó al banco mexicano Santander cuando un correo falso fue enviado a los usuarios informándoles que se había bloqueado su número de cliente, y para activarlo debían solicitarlo en un enlace adjunto. La página a la que se les dirigía les pedía llenar datos personales y confidenciales como su nombre, domicilio, número de identificación personal (NIP), número de cuenta, tarjetas y contraseñas, los cuales se utilizaron posteriormente para realizar el fraude. Otro caso de fraude en los sistemas bancarios mexicanos llamó la atención de los usuarios. Ese mismo año, el *phising* se presentó en BBVA Bancomer por medio de llamadas en las que una operadora falsa llamaba a clientes sobre la cancelación de un seguro médico, a través de las cuales se obtenían de ellos datos sobre su cuenta bancaria.

En Chile durante el 2017 los ataques informáticos ocurridos aumentaron en un 40%, comparados con el 2016, año en el que el *phising* fue también el ataque informático que más afectó a Chile y a otros países como Brasil (Pizarro, 2017). En uno de los casos más sonados de la región, el ataque afectó a una estudiante, robándole un total de $1,9 millones de pesos chilenos a través de giros en su tarjeta de crédito. A partir del incidente, la Corte de Apelaciones de Santiago acogió un recurso de protección contra el Banco de Chile, siendo un paso histórico en el país en materia de crímenes cibernéticos.

Por otra parte, el estudio realizado durante el tercer trimestre de 2017 situó a Argentina como el séptimo país con mayor número de ataques recibidos durante el año en cuestión. Durante Noviembre de 2016 se llevaron a cabo 24 falsas transferencias hacia proveedores, robando 3,5 millones de pesos. La Policía Federal Argentina detuvo a las personas que aparentemente comprometieron las cuentas bancarias en el municipio 25 de mayo, en las afueras de Buenos Aires. Se creía que el suceso se debió a que las computadoras de la Tesorería se vieron infectadas por un virus, sin embargo las investigaciones continuaron en abril del 2017. Durante el mes de agosto de ese mismo año se dio a conocer que el fraude bancario se

realizó gracias a la creación de una réplica de la página *Home* Banking, de la Banca Internet Provincia (BIP), hecha a partir de un ataque homográfico, en el cual se modificó un sólo caracter de la liga original del sitio web, mandando al usuario automáticamente a una página señuelo con el fin de robar información y llevar a cabo las transacciones ilegales.

La Organización Internacional de la Policía Criminal y los crímenes cibernéticos.

La tecnología está evolucionando, y con el tiempo, cada vez más delincuentes aprovechan el anonimato y la velocidad de Internet para usarlo a su favor, con el fin de cometer delitos sin ninguna barrera física o virtual. Complejos ataques contra sistemas informáticos están en constante evolución convirtiéndose en una amenaza real para la población, dejando a miles de víctimas en todo el mundo y afectando a la economía mundial. La Organización Internacional de Policía (en lo sucesivo denominada INTERPOL), con la ayuda de la cooperación bilateral con agencias de aplicación de la ley y la industria privada, tiene el deber de investigar y encontrar a los responsables de estos ciberdelitos. INTERPOL se encuentra en una posición privilegiada para avanzar en la lucha contra el delito cibernético a escala mundial mediante la investigación proactiva de delitos emergentes, las últimas técnicas de capacitación y el desarrollo de nuevas herramientas policiales innovadoras.

Acciones previas

Durante 2015, INTERPOL desplegó la operación *First Light* en veintitrés países alrededor de Asia. La operación se enfocó en ubicar y rastrear teléfonos y correos electrónicos infectados por cibercriminales, teniendo como resultado el arresto de 500 personas y el desmantelamiento de 15 centros de operación. La primera fase de la operación empezó en 2014, y resultó en el arresto de 20 individuos dentro del territorio de Tailandia, quienes fueron identificados como las cabezas de sindicatos que generaban ilegalmente aproximadamente diez millones de dólares resultados de crímenes cibernéticos. Entre otros resultados de la operación, se destaca la reducción de un cuarenta por ciento en fraudes de telecomunicaciones.

Durante 2016, dentro de los cuarteles generales de INTERPOL en Francia, se celebró la reunión anual contra la ciberdelincuencia, tocando temas de inteligencia contra delitos de ingeniería social y tácticas contra el fraude. Considerando el incremento de criminales utilizando técnicas avanzadas para realizar fraudes en internet, el evento se enfocó en paneles de expertos, tendencias y retos en investigar este tipo de crímenes.

Referencias

1. Panda Security. (s.f.). Phishing. Recuperado el 14 de diciembre del 2017, de *Panda Security*.Web.<https://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/>

2. Ruy Alonso R. (2017). Phishing y otros 5 casos de fraudes bancarios en el 2017. Recuperado el 14 de diciembre del 2017, de *El Economista*. Web. <https://www.eleconomista.com.mx/finanzaspersonales/Phishing-y-otros-5-casos-de-fraudes-bancarios-en-el-2017-20170815-0130.html>

3. PANDAID. (2014). Se descubre un caso de ciberespionaje en América Latina en los últimos 4 años. Recuperado el 14 de diciembre del 2017, *PANDAID*. Web. <http://www.pandaid.com/se-descubre-un-caso-de-ciberespionaje-en-america-latina-en-los-ultimos-4-anos/>

4. Sabrina Pagnotta. (2017). Confirman que fue phishing lo que permitió el robo de $3,5 millones en Argentina. Recuperado el 15 de diciembre del 2017, *We Live Security*. Web. <https://www.welivesecurity.com/la-es/2017/08/07/confirman-phishing-robo- argentina/>

5. Rebolledo, R. A. (2017, August 15). Phishing y otros 5 casos de fraudes bancarios en el 2017. Recuperado el 15 de diciembre del 2017, *El Economista*. Web. <https://www.eleconomista.com.mx/finanzaspersonales/Phishing-y-otros-5-casos-de-fraudes-bancarios-en-el-2017-20170815-0130.html>

6. Político, R. A. (2017, July 19). Cada día se cometen 18 mil fraudes cibernéticos en México. Recuperado el 15 de diciembre del 2017, *Animal Político*. Web. <http://www.animalpolitico.com/2017/07/fraudes-ciberneticos-mexico/>

Glosario

A

***Addline Phishing*:** Doble suplantación de identidad, donde el victimario es capaz de acceder de forma fraudulenta al equipo de la víctima, y robas más de una cuenta personal.

Antivirus: Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

C

Cibernética: Ciencia que estudia la construcción de sistemas electrónicos y mecánicos a partir de su comparación con los sistemas de comunicación.

Ciberseguridad: Conjunto de herramientas que pueden utilizarse para proteger los activos de una organización y los usuarios en el ciberentorno.

Cross Site Scripting: Tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web.

D

DNS: Por sus siglas en inglés, *Domain Name System*, sistema de nomenclatura jerárquico a redes IP como Internet o una red privada.

I

Ingreso Per Cápita: indicador económico que mide la relación existente entre el nivel de renta de un país y su población.

M

***Malware*:** Abreviatura de *Malicious Software* y engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Marco Legal: Parámetros bajo los que se regiran todos y cada uno de los delitos o faltas previstas.

P

***Phishing*:** Fraude en línea con el propósito de robar datos y credenciales mediante un señuelo.

S

***Spear Phishing*:** Estafa de correo electrónico dirigida que obtiene acceso no autorizado a los datos confidenciales de las personas.

U

URL: Ruta que se encuentra en la caja de texto ubicada en la barra de navegación del navegador, sirve para ubicar de manera precisa en un servidor, cualquier recurso: una imagen, un video o una página web.

V

VU: Compañía especialista en el desarrollo de software de Ciberseguridad, con foco en la prevención del fraude y el robo de identidad..

Preguntas Guía

---

1. ¿Cómo está relacionada mi delegación con la INTERPOL?

2. ¿Cuáles son las estrategias de ciberseguridad de mi delegación?

3. ¿Cómo se ve afectada mi delegación por los crímenes tipo *phishing*?

Tópico B

Medidas para la prevención de tráfico de personas en Asia tras el desmantelamiento de organización criminal transnacional en Tailandia

Por: Ivana Naomi Millán Flores
Sofía Mitre de Jacobis

Introducción

Durante los últimos años alrededor de Asia los casos de tráfico de personas han ido en aumento. Según el reporte de la Biblioteca del Congreso Nacional de Chile (BCN), Asia tiene a los países con mayores índices de tráfico de personas en el mundo, siendo inmigrantes y mujeres los más afectados (2016). Los estudios del Índice de Esclavitud Global (IEG) dictan que 44 de cada 100 habitantes son esclavos, incluyendo mujeres y niños, los cuales son traficados de diferentes maneras: explotación sexual, laboral y el tráfico de sus órganos (2017). Sin embargo, Tailandia es el lugar en donde se concentra la mayor cantidad de tráfico de personas, y se destaca por una amenaza común e insistente: el crimen organizado transnacional. Por otro lado, el sudeste asiático no es el único pasando por una crisis debido a este crimen. Se estima que hay 45,8 millones de personas en condiciones de esclavitud en el mundo, de las cuales 58 por ciento se concentran en India, China, Pakistán, Bangladesh y Uzbekistán.

Antecedentes de los países involucrados

A inicios de 2017, la Oficina Central de Investigación reveló el caso de ocho mil niñas provenientes de la India quienes fueron llevadas a Dubai como esclavas, junto con otros cinco mil menores indígenas del estado de Jharkhand. Se estima que 130 mil menores caen en las redes de trata de personas todos los años en la India, y las estadísticas empeoran año con año. Esta es la realidad de aproximadamente 1.4% de los habitantes de la India, siendo este país asiático uno de los más problemáticos en el mundo con respecto a este delito (La Nación, 2016).

En noviembre de 2017, el Departamento de Estado en Estados Unidos modificó el nivel de Tailandia dentro del informe anual sobre el tráfico de personas, desplazando al país del nivel tres al dos, en donde se encuentran los países que no cumplen con los estándares establecidos internacionalmente en contra de la trata de personas. Durante años, Tailandia ha sido señalada como uno de los principales centros de la trata de personas en Asia. Según el Departamento de Estado de Estados Unidos, al menos decenas de miles de personas son víctimas cada año de las redes de venta de personas en el país, recibiendo en el último informe del gobierno estadounidense la peor calificación posible por ser fuente, destino y país de tránsito para hombres, mujeres y niños sometidos a trabajos forzados y tráfico sexual. Hoy en día, los labores

de respuesta a este tipo de crímenes que azotan al país se ven retrasados, tanto por el golpe de estado ocurrido durante 2016 como por los problemas sociopolíticos generados por la imposición de un gobierno militar en la región.

Durante el 2016, Malasia se encontraba en la última categoría de la lista que categoriza a las naciones que no cumplen con los estándares mínimos en el combate a la esclavitud moderna. En el mismo año, las autoridades encontraron cuatro campamentos abandonados por traficantes y fosas comunes con decenas de cuerpos. En mayo de 2017 se encontraron más de cien tumbas en campos clandestinos administrados por mafias que se encontraban en una operación en contra de la trata de personas, este hecho desencadenó una crisis de refugiados en la región. Cerca del lugar las autoridades Malagueñas notificaron el descubrimiento de diecinueve fosas en la selva que hace frontera con Tailandia que se encontraban con los restos de al menos veinticuatro personas identificadas como víctimas de la trata de personas (EFE, 2017).

El tráfico de menores y mujeres es un problema concurrente en China, y aunque actualmente las cifras oficiales concernientes a esta situación sean inexactas debido a que solo se registran los casos resueltos por la policía. De acuerdo a las últimas estadísticas oficiales dadas a conocer en abril de 2009, los registros policiales muestran que hasta 3.455 niños y 7.365 mujeres fueron rescatados de las redes de tráfico de personas en las que estaban (El Universal, 2017). Como solución a este problema, el gobierno chino puso en marcha en 2008 un plan destinado a combatir a las mafias que se dedican al tráfico de personas, a concientizar a la población y de esta manera prevenir posibles víctimas de estas redes. A diferencia de otros países, China adoptó la estrategia de visibilización y denuncia en lugar de negar la existencia del problema, ante lo cual se espera que lo lleve a convertirse en uno de los países más activamente implicados en la lucha contra el tráfico de personas.

Una de las provincias más afectadas de China es la provincia de Yunnan debido a su localización fronteriza, además de la pobreza material y el bajo nivel educativo en el que vive la mayor parte de su población. Otro factor que no solo ha afectado a la provincia de Yunnan es el factor étnico. El hecho de que algunas comunidades vivan aisladas contribuye a la inseguridad y a su indefensión, estas incluyen también a las provincias como Sichuan, Yunnan y Guizhou, las cuales coinciden en dos elementos: un bajo nivel de desarrollo y una importante presencia de comunidades étnicas minoritarias. Para finalizar, Estados Unidos incluyó en el reporte sobre Trata de Personas a China en él mismo rango que Siria, Rusia, Corea del Norte o

Venezuela. Esto se debe a que de acuerdo al Departamento de Estado de Estados Unidos, China no ha tomado medidas serias para poner fin a su complicidad en el tráfico de seres humanos.

Antecedentes sobre el crimen

Las Naciones Unidas define la trata de personas como el transporte de seres humanos utilizando la fuerza u otras formas de coerción, tales como rapto, fraude, decepción, abuso de poder o posición de vulnerabilidad con el objetivo de explotar a las víctimas, utilizando en provecho propio y de modo abusivo las cualidades de estas. Dentro de los tipos de abuso más comunes en el tráfico de personas se encuentra la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas, la servidumbre o la extracción de órganos. Sin embargo, el tráfico de personas está conformado por todo un proceso en el cual se ven involucrados más personas además de los tratantes y las víctimas. Para que el proceso pueda ser completado los tratantes deben recurrir a la captación, el transporte, el traslado, la acogida o la recepción de personas.

La trata y el tráfico de personas son delitos que se han incrementado en forma alarmante en los últimos años debido a las difíciles condiciones de vida en los países menos desarrollados, al endurecimiento de las políticas migratorias en los países industrializados y al hecho de que por mucho tiempo estos fenómenos no fueron considerados como un problema estructural sino como una serie de episodios aislados. La Fundación Thomson Reuters reveló en 2017 que existen alrededor de 46 millones de esclavos en el mundo, a la vez que aseguró que la trata de personas se extiende a lo largo de 167 países, siendo Asia la región donde este crimen genera 1.8 millones de euros al año y se puede encontrar a un 60% de los esclavos a nivel mundial (2017). La respuesta mundial frente al crecimiento de esta forma de criminalidad fue la Convención contra la delincuencia organizada transnacional firmada en Palermo en el 2000 y los dos protocolos del mismo año: Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire y Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños.

De acuerdo a la coordinación general de la asociación Hotline Human Rights Trust, la alza en la presencia de este crimen a lo largo de Asia no es producto de hechos aleatorios, sino de una correlación entre diversos hechos sociales y económicos que actualmente se están suscitando en la región, siendo el motivo más común la pobreza y la mentalidad machista y sexista dentro de las comunidades rurales. Es común encontrarse con casos en los que los

hombres de familia venden a tratantes a sus respectivas hijas o esposas a cambio de saldar deudas o elevar sus expectativas económicas. De igual modo, se han reportado casos en los que los ciudadanos padeciendo de dificultades económicas extremas aceptan tratos con los traficantes, que por medio de engaños convencen a la población de someterse a sus negocios sin saber de qué se tratan realmente ni a dónde los están llevando.

Actualmente más de la mitad de la población mundial vive en Asia, cifra que se ve relacionada con los fenómenos migratorios en la región. A comienzos de 1990, Asia ya contaba con el mayor número de emigrantes a nivel global con un total de 49,8 millones de personas (INEDIM, 2017). Debido a su número y vulnerabilidad la mayor parte de los tratantes en Asia oriental y el Pacífico están en busca de emigrantes para relizar sus crímenes, sin embargo mujeres y niños también son blancos fáciles para este tipo de organizaciones. Los métodos que usan los traficantes para tomar a su víctima son variados y pueden ir desde el engaño hasta el secuestro.

Desmantelamiento de organización criminal transnacional en Tailandia

Según la agencia de noticias Internacional EFE, en julio de 2017 un total de 62 personas; militares, policías y empresarios, fueron condenadas a penas de entre 4 y 94 años de prisión en un juicio que se llevó a cabo en Bangkok contra una red que traficaba inmigrantes indocumentados a Malasia (2017). Entre los condenados se encuentran dos de los líderes de esta red; el General del Ejército: Manas Kongpan, y el hombre de negocios y ex alto funcionario de la provincia meridional de Satun: Patchuban Angchotipan. Según las investigaciones los criminales fueron acusados de tráfico, trata de personas, tenencia de armas, secuestro y homicidio. De los 103 acusados iniciales, uno murió durante el juicio y otros 40 han sido absueltos por el tribunal del país, quien ha impuesto una compensación de más de 130 mil dólares para las víctimas (EFE, 2017).

Alrededor de 200 testigos han comparecido en este proceso judicial, que comenzó en 2015 tras el hallazgo en el sur de Tailandia de varios campamentos clandestinos por los que habían pasado refugiados de la minoría musulmana rohinyá e inmigrantes bangladesíes, mismos que terminaron siendo vendidos como esclavos a barcos de pesca. A la par del campamentos, los investigadores encontraron tumbas con un total de 36 cadáveres. Los traficantes, incluidos varios birmanos y al menos un rohinyá, torturaban y abusaban de los

inmigrantes, incluidos mujeres y niños, para exigir el pago de hasta 3.000 dólares a los familiares (El Cofidencial, 2017). La polémica del caso yace no sólo en los crímenes realizados por los altos funcionarios y miembros del ejército, sino en las constantes amenazas propiciadas a los testigos y la falta de protección policial a los mismos durante el proceso de condena, llevando incluso al policía tailandés que lideró la operación a pedir asilo en Australia a finales del 2015.

Los campos encontrados existían desde 2013, después de que el gobierno de Tailandia desarrollaran una política a favor de las minorías de la región. Los emigrantes llegaban en botes a las costas tailandesas para ser redirigidos a Malasia y poder otorgarles provisiones. Sin embargo, tanto servidores públicos como la policía local encontraron en el proyecto la posibilidad de generar ganancias económicas con la ayuda de las redes de tráfico de personas, revelando que la corrupción es uno de los principales aliados de la trata en el país. Sólo unos días después de hallar las fosas comunes y los campos, el alcalde de uno de los pueblos cercanos y su ayudante fueron arrestados junto con otros 50 oficiales de la policía por sus conexiones con las redes de trata locales. El reciente descubrimiento del uso de los campos clandestinos interrumpió el flujo habitual de esta red de tráfico humano, orillando a las mafias a abandonar a miles de indocumentados en embarcaciones que navegaron durante días a la deriva en los mares de Tailandia, Malasia e Indonesia, creando la peor crisis de refugiados que ha padecido la región en décadas.

Por otro lado, Tailandia carece de claridad dentro de sus legislaciones al hablar sobre el tráfico de personas. Durante 2008, con el propósito de evitar sanciones por el gobierno estadounidense relacionadas al tráfico de personas, se creó apresuradamente un intento de ley que cubriera los aspectos generales del crimen. La acción impidió la imposición de sanciones internacionales, sin embargo a partir de entonces la ley nacional contra la trata sería utilizada a favor de los criminales, aprovechando algunas lagunas dejadas por la ley para escaparse de las condenas. Uno de los problemas más grandes que trajo consigo la ley fueron los criterios para considerar a una persona como víctima, ya que estos no están estandarizados y a menudo se acusa a la víctima de ser culpable de la situación.

La Organización Internacional de la Policía Criminal y la trata de personas

La trata de seres humanos es un crimen bajo el derecho internacional, además de muchos sistemas jurídicos nacionales y regionales. Debido a las complejidades del problema, ya que

que el crimen organizado está cambiando, modificando sus modelos de trabajo en función de la demanda, incentivos, oportunidades y rentabilidad, se necesitan multitud de estrategias de variados niveles para reducir el problema.

El rol de la Organización Internacional de la Policía Criminal (en lo sucesivo denominada INTERPOL) es esencial en la resolución de la situación que concierne la trata de personas en Asia, ya que gracias al alcance que tiene esta organización resulta plausible utilizar las herramientas técnicas y los sistemas al alcance para compartir información de forma global. Estas incluyen las asociaciones, las cuales fortalecen el enfoque ya que trabajan en todos los sectores; los eventos y conferencias que hacen posible la reunión de expertos que conciernen al tema a resolver de todo el mundo; y la serie de recursos que se han recopilado a través del tiempo que incluyen información general, legislación internacional, guías y manuales de aplicación de la ley.

Además de lo previamente mencionado, en INTERPOL se apoya a la policía nacional en despliegues tácticos sobre el terreno, los cuales están hechos con el propósito de romper las redes de delincuencia detrás de la trata y el tráfico de personas. Esto se logra a través de talleres de capacitación para garantizar que los oficiales sobre el terreno estén capacitados en una variedad de habilidades. Estas incluyen las técnicas de entrevista especializada y el uso de equipos especializados. Los despliegues combinan de manera eficiente la acción policial con los aportes de diversos sectores, como los administradores de aduanas y del medio ambiente, las organizaciones no gubernamentales, los funcionarios de los Ministerios de Salud y Asuntos Sociales y los fiscales.

Acciones previas

A mediados de 2014, alrededor de 170 agentes de las fuerzas del orden público de Côte d'Ivoire participaron en la Operación Nawa, en la que gendarmes, policías y agentes forestales se concentraron en campos de cacao y minas de oro ilegales en cinco áreas de la región de Soubré (INTERPOL, 2014). Con la mayoría de las víctimas sospechosas de trata de niños procedentes de Burkina Faso y Malí, la operación condujo al arresto y la condena de ocho traficantes, resultando en el rescate de 76 niños víctimas de la explotación infantil y tráfico de personas alrededor de África occidental.

Durante 2015 se inició dentro de los territorios de Ghana y Costa de Marfil la Operación Akoma, resultando en el rescate de más de 150 niños de la región víctimas de la trata y explotación. En asociación con la Organización Internacional para las Migraciones, la operación en curso se ha enfocado en los sectores agrícolas y comerciales, conduciendo hasta el momento al arresto de 25 personas involucradas en la trata de personas. Más de 250 funcionarios que representaban a servicios policiales, gubernamentales, de inmigración, forestales, sociales y médicos, fueron entrenados antes de llegar a la operación, con el propósito de guiar a los elementos en la identificación de los casos y para asegurar que los niños rescatados recibieran la atención necesaria antes de regresar a un lugar seguro.

En 2017, cerca de 500 víctimas de la trata de personas, entre ellas 236 menores, fueron rescatadas luego de una operación de INTERPOL realizada simultáneamente en Chad, Malí, Mauritania, Níger y Senegal. En total, 40 presuntos traficantes fueron arrestados y serán procesados por delitos como la trata de personas, el trabajo forzoso y la explotación infantil. Los delincuentes obligaban a las víctimas a participar en actividades que van desde la mendicidad hasta la prostitución, con poco o ningún respeto por las condiciones laborales o la vida humana. Durante los días posteriores a los arrestos, se requirió la colaboración de la Organización Internacional para las Migraciones y otras organizaciones no gubernamentales en orden de garantizar el cuidado adecuado hacia las víctimas después de las labores de rescate.

Referencias

1. Internacional Criminal Police Org. (2017). INTERPOL-led operation rescues 500 victims

of human traficking, leads to 40 arrests. Recuperado el (28 de diciembre de 2017), de Internacional Criminal Police Org. Web. <https://www.interpol.int/News- and-media/News/ 2017/N2017-162>

2. Asia News. (2015). Trata de mujeres en Bangladesh: víctimas de la pobreza, la ignorancia y de una mentalidad machista. Recuperado el (28 de diciembre de 2017), de Asia News. Web. <http://m.asianews.it/index.php?art=35414&l=es>

3. Charles Parkinson. (2013). Bolivia desmantela red de trata de personas de Bangladesh a Brasil. Recuperado el (28 de diciembre de 2017), de InSight Crime. Web. <https:// es.insightcrime.org/noticias/noticias-del-dia/bolivia-desmantela-red-de-trata-de-personas-de-bangladesh-a-brasil/>

4. Quanbao Jiang y Jesús Javier Sánchez Barricarte. (2011). Trafficking in Women in China Recuperado el (28 de diciembre de 2017), de Universidad Carlos III de Madrid. Web. <http://portal.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/ trafico_mujeres_china>

5. Víctor Sancho. (2017). EU incluye a China en la lista negra de tráfico de personas. Recuperado el (29 de diciembre), de EL UNIVERSAL. Web. <https://www.google. com.mx/amp/amp.eluniversal.com.mx/amp/note/amp/eluniversal/905946>

Glosario

C

Clandestino: Que se hace de forma oculta o secreta para burlar la ley.

Concurrente: Que se junta o coincide con otro u otros en el mismo sitio y/o momento.

Complicidad: Complicidad de una persona junto con otras en la comisión de un delito o colaboración en él sin tomar parte en su ejecución material.

D

Desmantelamiento: Destrucción de las fortificaciones.

E

Emigrantes: Persona que vive en un país o región que no es el suyo propio de origen.

Esclavos: Persona que carece de libertad y derechos propios por estar sometido de manera absoluta a la voluntad y el dominio de otra persona.

F

Funcionarios: Persona que ocupa un cargo jerárquico de confianza en la administración pública y para el cual ha sido designada por las autoridades competentes en forma directa.

I

Inmigrantes: Persona que llega a un país o región diferente de su lugar de origen para establecerse en él temporal o definitivamente.

L

Legislaciones: Conjunto de leyes por las cuales se regula un Estado o una actividad determinada.

M

Mafia: Organización clandestina de criminales que intenta conseguir el monopolio de sus actividades delictivas en una zona.

O

Organización No Gubernamental: Institución sin fines de lucro que no depende de la administración del Estado y realiza actividades de interés social.

T

Transnacional: De varias naciones.

Preguntas Guía

---

1. ¿Cómo se ve afectada mi delegación por el tráfico de personas en Asia?
2. ¿Cuáles son las medidas de seguridad que tiene mi delegación con respecto al tráfico de personas?
3. ¿Cuál es la relación que tiene mi delegación con los programas de la INTERPOL para contrarrestar el tráfico de personas?