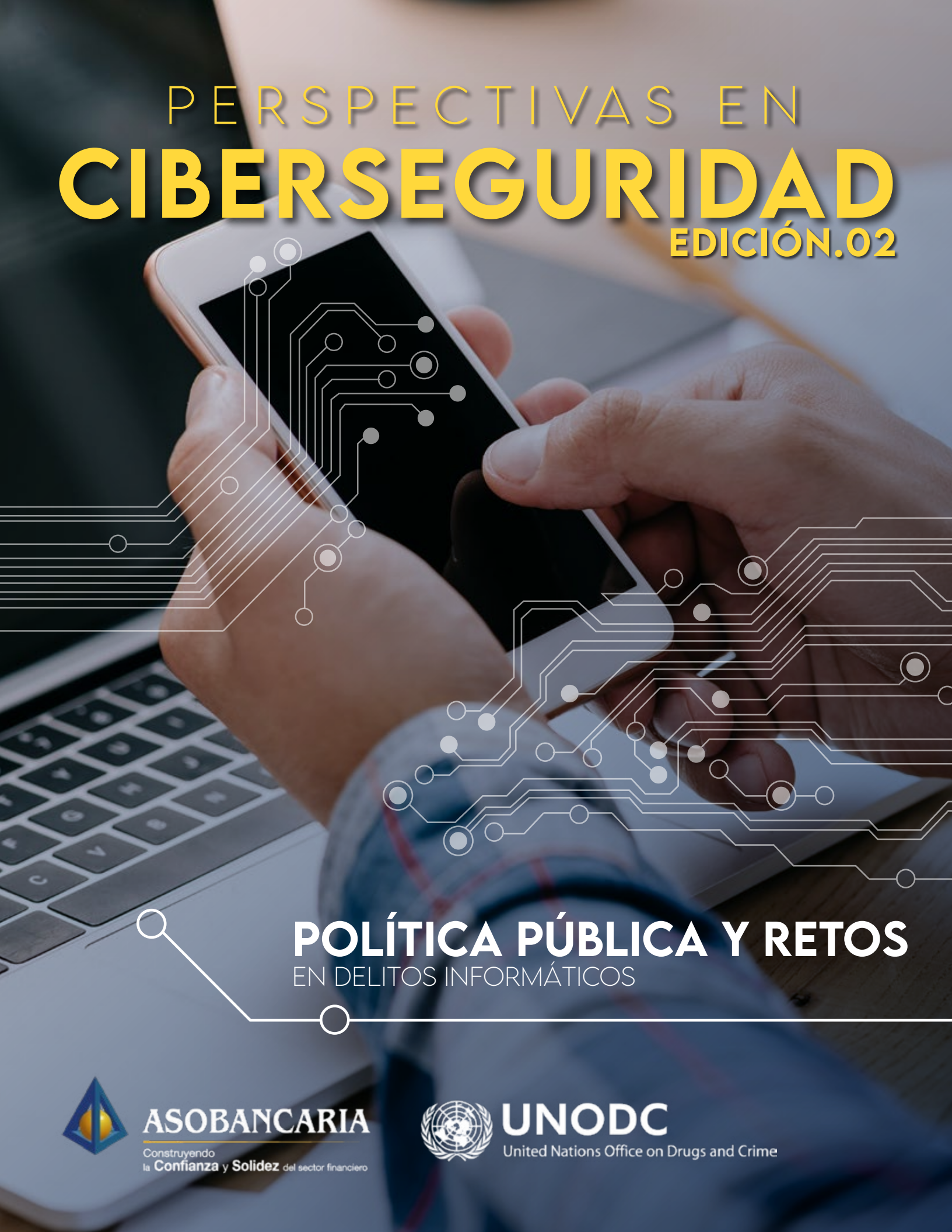


PERSPECTIVAS EN CIBERSEGURIDAD

EDICIÓN.02

POLÍTICA PÚBLICA Y RETOS
EN DELITOS INFORMÁTICOS

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

UNODC
United Nations Office on Drugs and Crime

Pierre Lapaque
Representante en Colombia
Oficina de las Naciones Unidas Contra la Droga y el Delito

Andrea Agudelo
Coordinadora de Delitos Económicos y Drogas Ilícitas
Prevención del Delito y Justicia (PROJUST)
Oficina de las Naciones Unidas Contra la Droga y el Delito

Hernando José Goméz
Presidente
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Alejandro Vera
Vicepresidente técnico
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Jaime Rincón
Director Gestión Operativa y Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Santiago Castiblanco
Profesional Junior
ASOBANCARIA

Babel Group
Diseñadora Editorial:
Adriana Villegas

CONTENIDO

ANÁLISIS Y PERSPECTIVA DE POLÍTICAS PÚBLICAS EN EL ÁREA DE DELITOS INFORMÁTICOS

POR:

IRMA ENCARNACIÓN LLANO PEREIRA,
Fiscal Delegada Nacional de Delitos Informáticos de la República del Paraguay

Nos encontramos en pleno siglo XXI, donde en nuestra vida diaria y en los diferentes ámbitos, interactuamos con el uso de la tecnología de la información y la comunicación. Cada día, este proceso se complejiza y su análisis se consolida en una cuestión de especialistas formados.

Hoy nuestra jornada diaria es inconcebible sin que estemos conectados a internet, en el uso de diferentes apps, para el desenvolvimiento en cuestiones elementales como para poder llegar a un lugar, comunicarnos, estudiar, trabajar, es decir, en todos los ámbitos de nuestras vidas. Más aún en estos tiempos de pandemia, que se ha potencializado y hemos migrado en el desenvolvimiento diario, en el uso de la tecnología y así también como consecuencia la multiplicación de ciberdelitos. Así, con el uso de la tecnología, han surgido nuevas modalidades delictivas de las cuales somos víctimas diariamente.

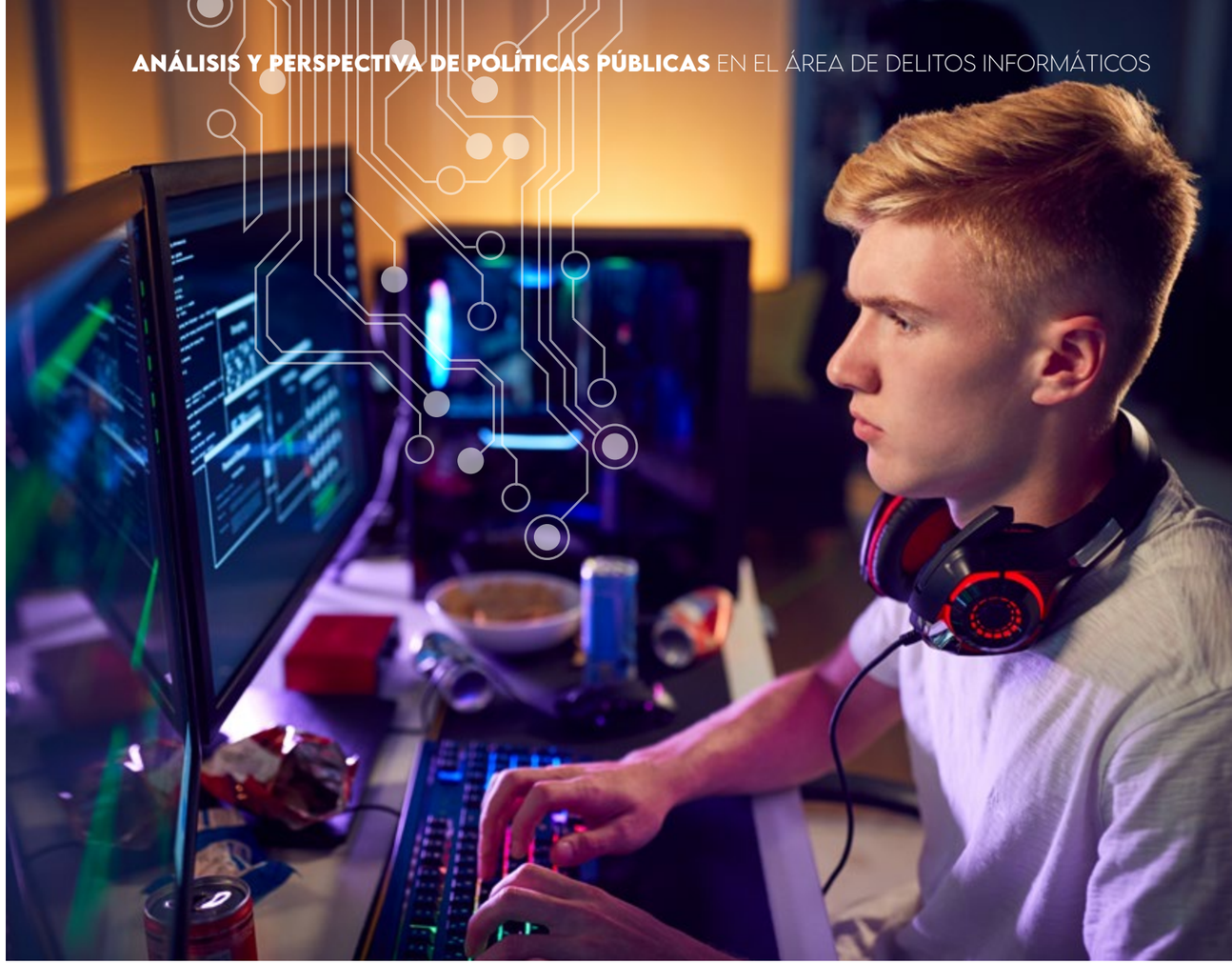
Es muy importante resaltar que, con el avance de internet, se destacan 2 pilares fundamentales que cada día los Estados a través de sus diferentes políticas públicas tratan de fortalecer que son la ciberdefensa y ciberseguridad (al referirnos a la ciberdefensa, hablamos de las herramientas para defender la ciberseguridad del propio Estado en el ciberespacio).

Haciendo un análisis de los tiempos en que vivimos, de cómo ha aumentado el cibercrimen, de la forma burda en que caen las víctimas en la mayoría de los casos a través de ingeniería social y las afectaciones que tiene este delito en la sociedad, hemos decidido hablar y analizar las políticas públicas a fin de poder atajar y atacar al cibercrimen.

Se ha identificado que los adultos a través de ingeniería social caen con facilidad, siendo engañados y entregando ellos mismos sus claves de acceso de sus perfiles en diferentes plataformas, dándose en los últimos tiempos un aumento considerable de casos de acceso indebido a sistemas informáticos, que son modalidades propias que se están dando como el robo a cuentas de WhatsApp y cuentas bancarias.

De igual manera, hoy en día, con las medidas sanitarias a nivel mundial consecuencia de la pandemia en donde los niños y adolescentes, a fin de no perder sus

HAY QUE RECONOCER QUE EN MUCHOS CASOS LOS PADRES SON ANALFABETOS DIGITALES, CON DESCONOCIMIENTO TOTAL DE LAS MEDIDAS DE SEGURIDAD,



clases en escuelas y colegios las realizan de manera virtual, esto ha conllevado a que accedan a internet sin limites en la mayoría de los casos, dando posibilidad a que sean víctimas de casos de explotación o abuso sexual infantil en línea, aumentando considerablemente estos hechos y más aún porque en la mayoría de los casos los padres desconocen las plataformas donde están navegando y con quienes están interactuando, siendo presas fáciles de personas inescrupulosas. Hay que reconocer que en muchos casos los padres son analfabetos digitales, con desconocimiento total de las medidas de seguridad, como por ejemplo de los controles parentales.

Los jóvenes son nativos digitales, en donde su identidad digital y su socialización lo es todo a través de las redes sociales, pero desconocen de los peligros que existen y para eso debemos prepararlos y educarlos, a fin de que no sean víctimas de cibercriminales.

No obstante, al hablar de educación en el ámbito de la era digital, no solo debe ser enfocado a los niños y adolescentes, sino a los adultos que en muchos casos tienen casi total desconocimiento sobre mecanismos de ciberseguridad en el uso de internet.

La ciberseguridad es elemental y debe ser parte de la agenda de cada ciudadano, empresa y gobierno, siendo el responsable de ponerlo en la agenda los propios Estados. Es así que gobiernos, sector público y sector privado, así como ciudadanos particulares, están utilizando software a fin de fortalecerla, más en estos tiempos

que todos estamos interconectados, los cual han dado oportunidades a la población, pero del que a su vez surgen retos, desafíos y nuevas maneras delictivas potenciadas, ya que los cibercriminales tienen alcance mundial.

Al referirnos a las nuevas maneras delictivas hablamos de las diferentes variantes de malware maliciosos, significando diferentes tipos de amenazas informáticas, como lo son virus informáticos o ransonwares que están causando estragos a nivel mundial. También estas los troyanos bancarios, que suplantan nuestras identidades y hacen transferencias fraudulentas de nuestras cuentas en línea, utilizando apps para violar nuestras privacidades y vender nuestra información.

¿Qué se busca con todo esto?, lucrar ilegalmente en muchos casos, mientras que en otros se quiere obtener información de cada uno de nosotros, por ejemplo, para crear tendencia mundial sobre la manipulación en elecciones, y en otros casos satisfacer la depravación sexual.

La mayoría de estas modalidades delictivas en años anteriores no existían, sin embargo, hoy con la globalización, no estamos ajenos a sufrir estos desmanes, en donde los límites fronterizos en el ciberespacio han desaparecido y en muchos casos en una investigación criminal están involucrados varios países, a fin de poder llegar a los responsables.

La conclusión de esta Delegada Nacional de la Unidad Especializa de Delitos Informáticos del Ministerio Público de la República del Paraguay, es que con base en todo lo referido, es de fundamental importancia que cada país desarrolle su plan estratégico en el ámbito de la ciberseguridad, basándose los mismos en los siguientes ejes elementales a fin de poder hacer frente a las nuevas amenazas que surgen:

La educación del usuario de internet, debe ser el eje fundamental de toda estrategia, con campañas de concientización, enfocado a todas las edades a fin de que se familiaricen con el uso de la tecnología y la ciberseguridad.

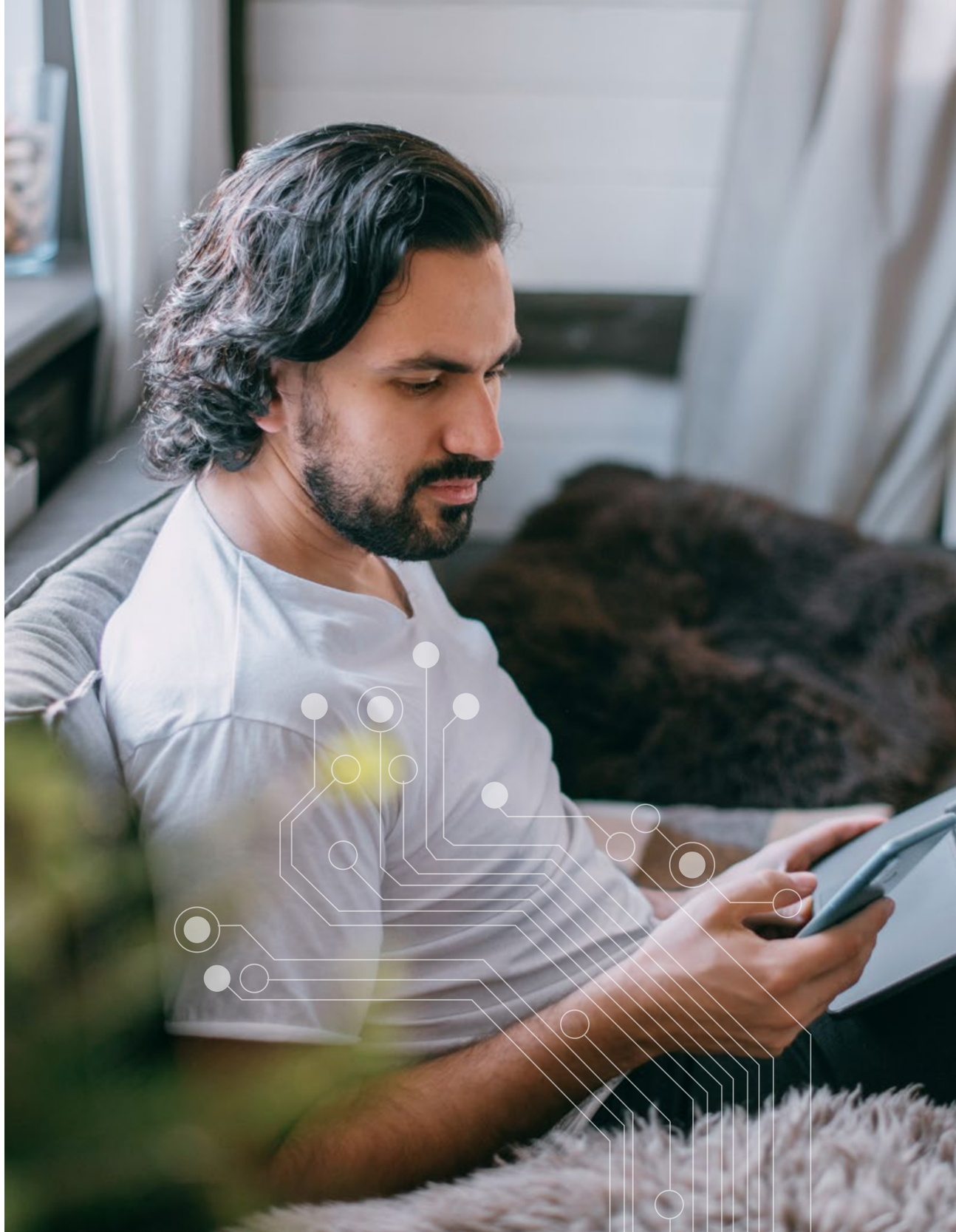
La formación de capacidades en el área de la ciberseguridad, el fortalecimiento del área en las investigaciones de las unidades especializadas en la lucha contra el cibercrimen, con herramientas forenses y capacitación constante, a fin de poder identificar a los cibercriminales y fortalecer el enlace de los puntos de contactos a nivel internaciones a fin de trabajar en equipo en la lucha contra estos tipos de delitos que no conocen fronteras, la cibercriminalidad.

Se deben buscar buenas prácticas, manuales de protocolos en el manejo de la información de cada ciudadano, en la ciberseguridad de las infraestructuras tanto para el sector público y sector privado. Es decir, una regulación en la protección de datos personales, con políticas comunes a nivel mundial, teniendo en cuenta que tenemos en frente a multinacionales que hoy tienen más poder que el propio Estado.

La creación de agencias especialistas en la protección y la reacción ante incidentes cibernéticos, especialmente teniendo en cuenta las infraestructuras críticas.

Se deben crear planes estratégicos nacionales, con análisis constante a fin de ir mejorándolos constantemente, teniendo en cuenta que al hablar del uso de la tecnología y su evolución esta es dinámica, no para, evoluciona a pasos gigantes y para poder hacer frente y estar preparados como Estados, se debe prever en las políticas de los planes nacionales estratégicos de gobiernos y de buenas prácticas en el ámbito de la tecnología que estos sean tan dinámicos como la propia tecnología y los cibercriminales, es decir dejar de lado la burocracia gubernamental.

Finalmente, quiero expresar que el punto central de las instituciones responsables del área de ciberseguridad, ciberdefensa y cibercrimen debe estar focalizado en **fortalecer la educación de la ciudadanía, sector público y privado en el uso de la tecnología de la información, para evitar así ser analfabetos digitales**.



LA CIBERDELINCUENCIA, UN ASUNTO DE ESTADO

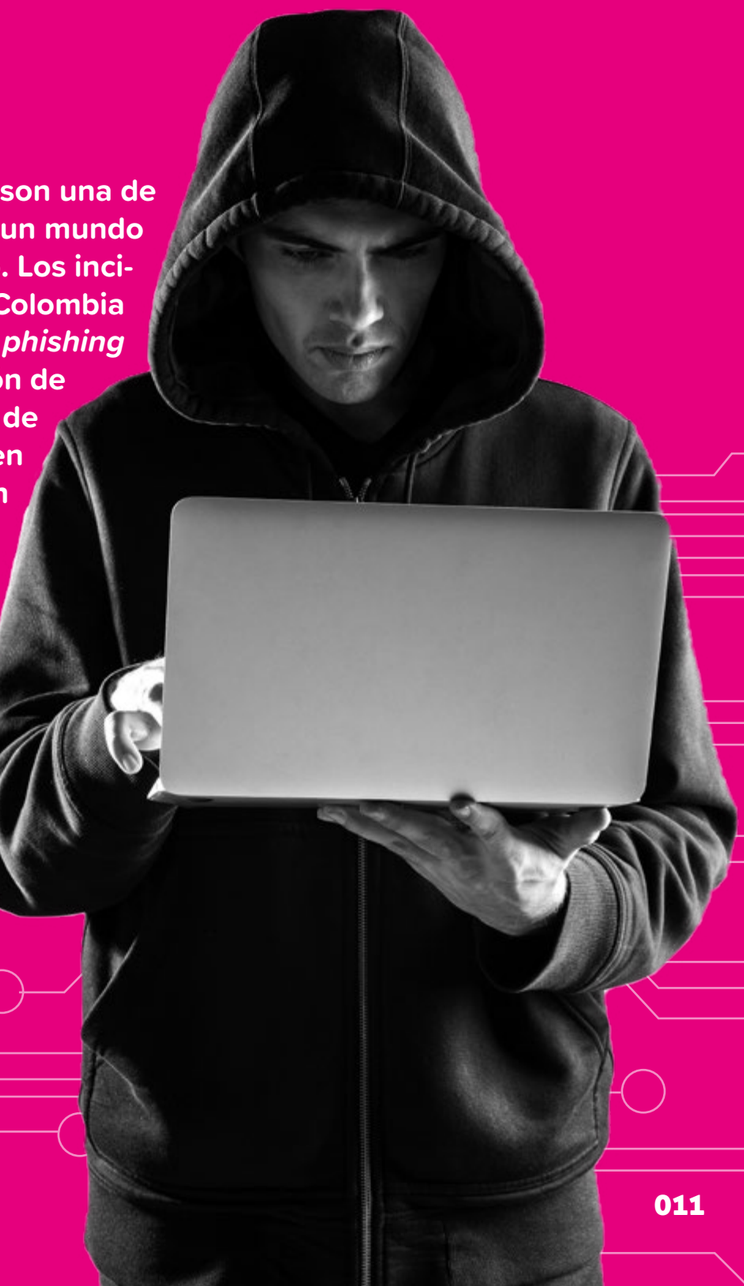
POR:

HÉCTOR JOSÉ GARCÍA,
director del Observatorio de Gobierno y TIC de la Universidad Javeriana. Presidente de Camerfirma Colombia

RESUMEN:
La delincuencia informática es uno de los principales problemas del siglo XXI y también una de las grandes preocupaciones del Estado colombiano. El siguiente artículo de investigación resalta el Modelo de Madurez de la Capacidad de Ciberseguridad liderado por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID). Se mencionan los avances de Colombia en su lucha contra la ciberdelincuencia y se reiteran las dificultades que se tienen a la fecha para hacer frente a este flagelo, al tiempo que se brindan algunas recomendaciones.

PALABRAS CLAVE:
Ciberdelitos, Cooperación, Ciberserguridad, Capacidad.

Los delitos informáticos son una de grandes preocupaciones en un mundo cada vez más digitalizado. Los incidentes más reportados en Colombia siguen siendo los casos de *phishing* con un 42%, la suplantación de identidad 28%, el envío de *malware* 14% y los fraudes en medios de pago en línea con 16%. (Cámara Colombiana de Informática y Telecomuciones -CCIT, 2020)



LA CIBERSEGURIDAD Y LA COOPERACIÓN INTERNACIONAL

EL derecho penal y el derecho procesal penal clásicos fueron desarrollados sobre la base de un modelo de criminalidad física, marginal e individual. Sin embargo, en la actual "Era de la Información", en donde se hace referencia a la creación de "una nueva estructura social dominante, la sociedad red; una nueva economía, la economía informacional/global; y una nueva cultura, la cultura de la virtualidad real" (Castells, 1998, p. 370), la revolución 4.0 que agrupa estas realidades, ha traído consigo grandes retos y dificultades para la represión de este tipo de delitos, con ocasión de la dificultad en la detección y persecución de los mismos, entre otras razones, por el anonimato, la falta de coordinación y la escasa cooperación internacional. (Fernández Teruelo, 2011).

El Informe de *Cibercrimen ThreatMetrix* identificó a América Latina como un foco para el fraude en la creación de cuentas bancarias, con alrededor del 20% del volumen total frente a un promedio de la industria del 12,2%. Las creaciones de nuevas cuentas son atacadas *constantemente*, lo que representa una oportunidad de

explotar, aumentar y monetizar robos y credenciales falsificadas. Aproximadamente uno de cada siete intentos de creación de cuenta nueva se identifica como un posible ataque. (LexisNexi, Risk Solutions, 2020).

Las cifras sobre fraudes informáticos vienen en aumento. A través de los canales que pone a disposición la Policía Nacional, se registraron 30.410 en el 2019. De acuerdo con el reciente estudio sobre "Tendencias del Cibrecrimen 2019-2020", de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), las modalidades de fraude más recurrentes son el *phishing* con 42%, la suplantación de identidad con 28%, el *malware* 14% y los medios de pago digitales con 16%. En Colombia, el tipo penal "hurto por medios informáticos", es el delito más denunciado con un total de 31.058 casos. En segundo lugar, se encuentra la violación de datos personales con 8.037 casos. El tercer delito más denunciado es el acceso abusivo a sistemas informáticos con 7.994 casos.

Esta estadística revela que en Colombia el *phishing* y sus distintas tipologías como el *smishing*, son las modalidades preferidas para obtener los datos personales de una persona natural o jurídica y suplantar su identidad, principalmente, para realizar hurtos por medios informáticos, lo que en últimas se traduce en un uso indebido y una violación de los datos personales. (CCIT, 2020).

Para hacer frente a este flagelo de la ciberdelincuencia se requieren esfuerzos internos y de cooperación internacional. En el derecho interno se han introducido una serie de tipos penales con la creación, incluso, de un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos". No obstante, a pesar de las quejas, las denuncias recibidas por la Policía no llegan a conocimiento de los fiscales y no se judicializan dichas conductas. De acuerdo con cifras del estudio sobre ciberdelincuencia de la CCIT, más del 40% de los casos denunciados no llegan presentarse como una denuncia formal ante la Fiscalía, por lo que se puede concluir que en la actualidad casi un 50% de los delitos informáticos en Colombia quedan en la impunidad, ante una clara deficiencia en la judicialización de los mismos.

DE ACUERDO CON CIFRAS DEL ESTUDIO SOBRE CIBERDELINCUENCIA DE LA CCIT, MÁS DEL 40% DE LOS CASOS DENUNCIADOS NO LLEGAN PRESENTARSE COMO UNA DENUNCIA FORMAL ANTE LA FISCALÍA.

Colombia ha tenido avances importantes en el marco internacional en la lucha contra este flagelo. Además de pertenecer a la Europol y a Interpol, en 2015, el país suscribió el Convenio de Budapest sobre ciberdelincuencia. Adicionalmente, Colombia adoptó una estrategia nacional de ciberseguridad (NCS, por sus siglas en inglés) lo que se ve reflejado en el nuevo CONPES de seguridad digital y ciberseguridad. En la región, no son pocos los países que ya cuentan con una estrategia nacional de ciberseguridad que ha sido una de las recomendaciones de la OEA.

A nivel internacional, existe otro importante referente que es el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés), que es la base de los estudios regionales de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) en 2016 y 2020. Este modelo tiene cinco etapas de madurez: 1) Inicial, 2) Formativa, 3) Consolidada, 4) Estratégica, 5) Dinámica y se divide a su vez en cinco dimensiones: (i) política y estrategia de ciberseguridad; (ii) cultura cibernética y sociedad; (iii) educación, capacitación y habilidades en ciberseguridad; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías. Cada una de estas dimensiones se subdividen en un conjunto de factores que describen y definen lo que significa poseer capacidad de seguridad cibernética en cada factor e indican cómo mejorar la madurez. Este modelo es la hoja de ruta para avanzar ordenada y coordinadamente en la lucha contra la ciberdelincuencia a nivel internacional. (Creese, 2020)

Colombia tuvo un buen desempeño en el CMM 2020. La nueva política de seguridad digital (CONPES 3995/2020) apunta a fortalecer aún más las capacidades de todas las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. Asimismo, Colombia creó el Comité de Seguridad Digital, liderado por el Coordinador Nacional de Seguridad Digital como ente máximo para tratar temas intersectoriales de seguridad digital y ya cuenta con Equipos de Respuesta a Incidentes de Seguridad Cibernética, en concordancia con la iniciativa CSIRT Américas.

INCONVENIENTES MÁS RELEVANTES PARA JUDICIALIZAR Y ENFRENTAR LA CIBERDELINCUENCIA

No es una verdad oculta que las infracciones informáticas son difícilmente descubiertas o perseguidas. Esta realidad se presenta por diversas razones, la mayoría de ellas universales y que se exponen a continuación:

Capacidad y anonimato del sujeto activo de la conducta punible. Los sujetos activos del delito proceden sigilosamente y poseen alta capacidad tecnológica, logrando actuar anónimamente y borrar toda huella digital que los vinculen con el delito. Ese ocultamiento es una eficiente forma de evadir su responsabilidad, ya que éste puede valerse de sistemas de terceros o utilizar programas de enmascaramiento que no permiten ver la verdadera dirección electrónica, ya sea de correo electrónico o la misma IP.

Capacidad de acción y reacción. Otra problemática es la capacidad de acción y reacción de los prestadores de servicios digitales, de la policía, fiscalía y jueces, por lo que se debe velar por la capacitación y trabajo coordinado de estos actores.

Entidad especializada y Ministerio Público experto. No contar con un área experta en el Ministerio Público que pueda trazar las directrices para la correcta indagación de este tipo de infracciones, así como investigar y perseguir estas conductas, dificulta la sanción del delito. (Acurio del Pino, 2016).

La concepción tradicional de tiempo y espacio. Dado que los delitos informáticos se consuman en su mayoría en el ciberespacio, esto es, en un lugar donde no existen fronteras territoriales, se hace compleja la persecución y judicialización de los mismos, en virtud del principio de territorialidad de la ley penal. Un ejemplo es el virus *I LOVE YOU*, que se perpetró desde Filipinas y causó daños a nivel global. Otro de los ejemplos que afectan la concepción de tiempo y espacio del delito digital son las *logic bomb* o bombas lógicas que son programadas para "explotar" tiempo después de haber implantado la bomba en el sistema informático, lo que hace complejo el rastreo de la persona que cometió el delito. (Acurio del Pino, 2016).

Escasez de fuerza laboral calificada. La escasez de profesionales calificados en ciberseguridad es un desafío casi universal. Esta circunstancia generalizada resalta la necesidad e importancia de equilibrar las inversiones enfocadas en la persecución de estos delitos y poder fomentar habilidades y educación que contribuyan de manera sustancial y auto sostenible a las posturas nacionales de ciberseguridad. (Creese, 2020).

RECOMENDACIONES

De acuerdo con lo expuesto se proponen las siguientes recomendaciones:

1 Construir e implementar adecuadamente las políticas públicas de seguridad digital y ciberseguridad, las cuales son fundamentales para asegurar los derechos y la seguridad informática.

2 Contar con una legislación avanzada y específica para el tratamiento de los delitos informáticos.

3 Fortalecer la cooperación regional e internacional, dado que es un factor indispensable para reaccionar ante el crimen informático organizado y detener los ataques cibernéticos antes de que lleguen a niveles incontrolables. (Mikser, 2020).

4 Educación cibernética. Entre otros objetivos estratégicos, la tercera estrategia de seguridad cibernética de Estonia (2019-2021) ha abordado la educación cibernética como parte de las áreas futuras donde se deberán realizar más inversiones. (Mikser 2020).

5 Elaborar un Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, dado que es un elemento clave para que los líderes empresariales y las juntas corporativas comprendan mejor los riesgos cibernéticos de su modelo operativo comercial y logren el equilibrio adecuado entre proteger la seguridad de sus activos, mitigar las pérdidas y mantener la rentabilidad en un ambiente competitivo. (Barmpaliou 2020).

6 Aplicar el principio de equivalencia, universalidad y justicia mundial. Este principio es muy útil en el campo de los delitos informáticos y consiste en la aplicación de la ley penal si el delito es cometido en otro país donde también se encuentra tipificado, permitiendo que pueda seguirse el proceso penal por el cometimiento de dicho delito, pero en nuestro país.

REFERENCIAS BIBLIOGRÁFICAS

Acurio del Pino, S. (2016). Delitos Informáticos: Generalidades. Publicado en Internet: **https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf**

Barmpaliou, N. (2020). Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe. En: Banco Interamericano de Desarrollo. Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. 2020. Disponible en: **https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf**

Cámara Colombiana De Informática y Telecomunicaciones –CCIT (2020). Tendencias Cibercrimen 2019-2020. Disponible en: **https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf**

Castells, M. (1998). La era de la información. Sociedad, Economia y Cultura (Vol. 3: Fin de milenio). Madrid: Alianza editorial.

Creese, S. (2020). Tendencias regionales en el estado de preparación en ciberseguridad, 2016-2020. En: Banco Interamericano de Desarrollo. Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Disponible en: **https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf**

LexisNexi, Risk Solutions. (2020). Cybercrime. Report January-June 2020. Disponible en: **https://risk.lexisnexis.com/insights-resources/research/cybercrime-report**

Mikser, S. (2020). La necesidad de una respuesta armonizada a las amenazas de ciberseguridad. En: Banco Interamericano de Desarrollo. Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Disponible en: **https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf**

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

UNODC
United Nations Office on Drugs and Crime

¿CÓMO IMPLEMENTAR POLÍTICAS EFICIENTES PARA CONTENER LOS DELITOS INFORMÁTICOS?

POR:

CESAR MÉRIDA,
Expresidente del comité de seguridad Bancaria en Guatemala, formador para la Asociación Bancaria de Guatemala (ABG) en temas de seguridad y prevención de fraudes e investigaciones.

No cabe duda, el Convenio de Budapest el 23 de noviembre del año 2001 marcó el rumbo que deberían seguir muchas organizaciones a nivel mundial en relación al tema de ciberseguridad; la evolución de las Nuevas Tecnologías de la Información y la Comunicación (NTICS) trajeron consigo recursos, procesos e infraestructura que abriría la puerta a la mutación de delitos existentes, como el robo y fraude, o el nacimiento de otros, adaptándose de esta forma a las nuevas tendencias digitales; lo cual es inevitable. Este tratado internacional elaborado por el Consejo de Europa busca la cooperación de la industria privada, para la lucha contra la cibercriminalidad y la necesidad de proteger los derechos legítimos de este tipo de ataques y la unificación de criterios penales destinados a la prevención de estos delitos, adoptando medidas legislativas apropiadas para castigarlos y perseguirlos. En Colombia, por ejemplo, ya se tiene una política pública relacionada con el tema.

Entonces ¿cómo hacer más eficiente la política pública en delitos informáticos? Inicialmente debe entenderse, cuál es la razón y principio de una política pública: "las políticas públicas son actividades que un Estado diseña y gestiona a través de un gobierno electo y una administración pública con fines de satisfacer las necesidades de una sociedad" (Graglia, 2012).

Toda política pública tiene un ciclo de vida o momentos para su creación, desarrollada por etapas: la primera etapa, de gestación, que hace referencia al surgimiento de problemas públicos y responde a una agenda de gobierno basada y enfocada desde tres perspectivas: la agenda pública, la agenda de política y la agenda de gobierno; la segunda etapa, llamada de diseño y formulación, se analiza el problema y se buscan soluciones respondiendo a dos interrogantes ¿cuál es el mejor resultado? y ¿cuál genera mejores beneficios?; y en la tercera etapa, llamada de implementación o ejecución, se traza el plan de acción respondiendo a tres interrogantes, ¿cuál es la mejor forma de ejecutar una política pública?, ¿cómo planear la administración de los recursos para su ejecución? y ¿cómo comunicársela a la población?, por último, la etapa de evaluación de impacto, que consiste en valorar los efectos para medir como ha cambiado una condición o una situación.

No debe perderse de vista que la instrumentación de una política pública cumple con tres principios esenciales: de forma directa, que se lleva a cabo a través del aparato gobierno con sus recursos y su personal; de forma indirecta realizada por medio de organizaciones no gubernamentales o empresas privadas y por último cuando hay una intervención público-privada, partiendo de lo antes dichos podemos decir que los retos para hacer más eficientes las políticas públicas no dependen de una agenda de gobierno sino del involucramiento de las entidades afectas, sin importar que estas sean entidades gubernamentales o entidades civiles.

Por otra parte, los incidentes y las amenazas a la seguridad de la información traen consecuencias adversas para las empresas dedicadas a esta actividad, por los riesgos el acceso indebido de información privilegiada de la organización, trabajadores, clientes y proveedores, por lo que frente a estas ciberamenazas latentes

LOS INCIDENTES Y LAS AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN TRAEN CONSECUENCIAS ADVERSAS PARA LAS EMPRESAS DEDICADAS A ESTA ACTIVIDAD, POR LOS RIESGOS EL ACCESO INDEBIDO DE INFORMACIÓN PRIVILEGIADA

debemos estar preparados mediante un plan de prevención que accione los protocolos necesarios ofreciendo una solución adecuada al tipo de ataque.

De acuerdo con un informe de Enjoy Safer Techonology [ESET] (2020), el 60% de las organizaciones encuestadas manifiestan que su principal preocupación es el acceso indebido a la información, seguido de la sustracción de información (55%) y la infección con códigos maliciosos 53%. Asimismo, para 2019, los incidentes más reportados en Colombia son: phishing (42% de los incidentes), suplantación de identidad (28%), envío de malware (14%) y fraude en medios de pago en línea (16%) (Banca&Economía, 2020). Al respecto, no se puede dejar de mencionar que en el 2019 un error de configuración de bases de datos expuso información de millones de habitantes en Colombia, la cual contenía “datos sensibles que aluden a relaciones personales, situación financiera, salarios e incluso puestos de trabajo” (ESET, 2020).

Asimismo, las organizaciones financieras en Colombia han identificado algún tipo de evento de seguridad digital, detectando, entre los casos de mayor afectación: el empleo de códigos maliciosos o malware (75% del total de entidades), Phishing, Vishing o Smishing (75% del total de entidades) y violación de políticas de escritorio limpio (clear desk) (70% del total de entidades), el 19% de las entidades financieras identifican ocurrencia de eventos de malware diariamente” (Asobancaria-OEA, 2020).

Sin temor a equivocación podría asegurarse, que el ser humano juega un papel importante a lo interno de las organizaciones financieras, cuando se trata de ciberseguridad. Es decir, es la parte más vulnerable en cualquier sistema de seguridad. Con base en lo anterior, es importante recordar que, dentro de la digitalización de los servicios financieros y su ecosistema, existe un eslabón altamente vulnerable dentro del flujo informático, como lo es el usuario, no solamente por su poca habilidad y conocimiento de los sistemas informáticos, sino por los medios para conectarse.

Las vulnerabilidades se reducen en parte gracias a que las empresas tienen una gran cantidad de recursos económicos y expertos en temas informáticos que ayudan en determinado momento a mitigar cualquier amenaza que vaya en contra de las operaciones diarias de las entidades financieras. Sin embargo, puede existir que entre las entidades financieras las áreas de seguridad

informática y seguridad de la información que, si bien tienen una estrecha relación, no coordinen sus actividades en el ecosistema.

Esta diferencia radica en que la seguridad de la información, integra toda la información independientemente del estado en el que se encuentre, es decir, protegiendo la confidencialidad, la integridad y la disponibilidad de los datos. Concretamente se enfoca en los riesgos, analiza escenarios, mantiene observancia de buenas prácticas, esquematiza normas y exige niveles para asegurar procesos, tecnología para su utilización, almacenaje, transmisión, recuperación y disposición final de la información; entretanto la seguridad informática se centra en la protección de infraestructura critica para el resguardo de esa información, como redes, sistemas operativos, ordenadores, entre otros, esta última tiene como objetivo la implementación de medidas para proteger estos activos físicos y la comunicaciones soportando las operaciones en sus totalidad. Además de estos riesgos, el usuario o internauta se ve en ocasiones en la necesidad de conectarse en computadores externos fuera de una red de confianza, teléfonos móviles o APP's no seguras, lo cual posibilita la oportunidad de que se originen ciberdelitos.

Colombia es uno de los países latinoamericanos con mayor desarrollo en seguridad cibernética, pero estos avances deben de ir de la mano de la recuperación de la confianza en las entidades financieras. Es evidente que aún hay un tema olvidado tras la estructuración de estas políticas, que se aclaran con las respuestas a las siguientes interrogantes: ¿cómo se siente el usuario respecto al almacenamiento de su información? o ¿cómo se filtrará mi información?

La sustracción de información del 2019 fue una llamada de atención, si bien propicia nuevos avances e implementaciones tecnológicas como reconocimiento facial, de voz, uso de contraseñas o huellas dactilares que generan confort para tener acceso a las plataformas digitales bancarias para validación de saldos, transferencias pagos o gestiones internas; en definitiva, no resuelven ese sentimiento de inseguridad en el usuario.

A pesar de que los avances tecnológicos logrados a la fecha son importantes; queda pendiente desarrollar campañas de concientización hacia el usuario -algunos bancos ya la tiene-, para alertarlo acerca del riesgo las redes sociales, páginas web y blocks específicos y plataformas, medios ideales para engañarlo e incidir en la desconfían y reputación de grupos financieros.

Los retos en política pública que tiene el sistema financiero colombiano ante los delitos informáticos deben ir encaminados a la recuperación de la confianza del usuario, es decir, no solo envío de correos, interacciones mediante una página web, mensajes de texto o un call center. Los riesgos relacionados con la operación son cruciales, se vulneran y se expanden con el comportamiento humano y los juicios subjetivos de las personas, potencializan las amenazas y las vulnerabilidades tomando en cuenta que estás se encuentran ligadas, la seguridad de los sistemas informáticos desde la política pública tiene un alto impacto puesto que sin seguridad no hay privacidad y mucho menos confianza en los sistemas que administran la información.

Los responsables de la comunicación hacia los usuarios y al personal que labora en el sistema bancario, deben tener presente que el tiempo de vida de la política y los cambios que pueda sufrir a futuro, están ligados a los cambios en la administración pública. Lo temas relacionados con la ciberseguridad deben ir más allá de un "shut down" del sistema para dar cumplimiento a lo trazado dentro de los planes de continuidad de negocios y debe de encaminarse a estructurar de forma consensuada estrategias no solo preventivas, sino que también aquellas relacionadas con apoyar la transformación cultural de los usuarios, si bien las nuevas generaciones manejan de mejor forma los cambios tecnológicos, hay un conglomerado de clientes que se han tenido que ir adaptando a las exigencias de estos cambios y este debe de ser el focus group a consolidar.

BIBLIOGRAFÍA

Asobancaria-OEA. (2020). Estado de la Ciberseguridad en sistema Financiero Colombiano. Colombia: N/A.

Banca&Economia. (2020). Alianzas del sector público y privado para combatir el Crimen Financiero en tiempos del Covid-19. Colombia: Banca&Economia.

ESET – Enjoy Safer Technology, (2020). Security Report, Latinoamérica 2020.

Graglia, J. E. (2012). En la búsqueda del bien común. Manual de Políticas Públicas. Argentina: Asociación Civil Estudios Populares (ACEP) / Fundación Konrad Adenauer (KAS) Argentina.

RETOS Y ESTRATEGIAS DEL SECTOR FINANCIERO PARA AFRONTAR AMENAZAS EMERGENTES

POR:
JORGE MARIO RODRÍGUEZ,
Director de Seguridad de la Información
de la Fundación Grupo Social

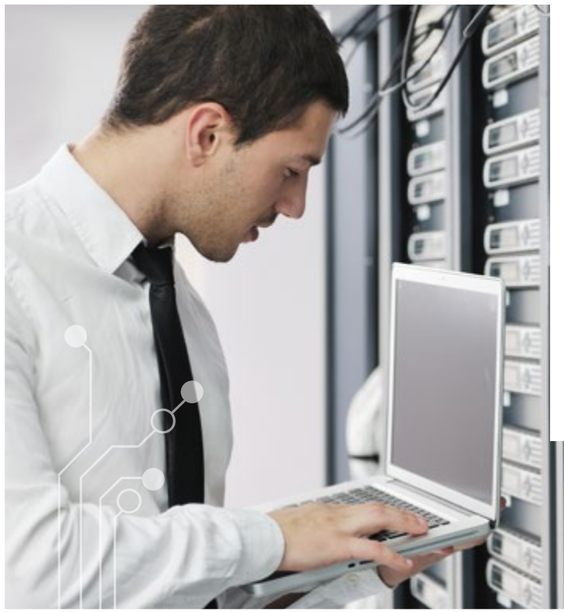
Desde la antigüedad la forma en que los hombres han manejado la información les ha valido para su propia supervivencia. El hecho de saber dónde podían conseguir presas para cazar, peces o fuentes de agua y no revelarlo a otros miembros de las tribus pueden ser ejemplos de los primeros inicios de la importancia de la confidencialidad, en ese mismo sentido se puede comparar como ingeniería social la forma en que la serpiente convenció a Eva para que le diera la manzana a Adán o cuando el caballo entró a Troya haciéndose pasar por un regalo de los dioses.

En fin, hay muchas comparaciones que nos indican la existencia milenaria e intangible de los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad.

En la actualidad preservar esos principios, como parte de la función de la Seguridad de la Información, se ha vuelto muy complejo. En especial por la gran amplitud de tecnologías emergentes acompañadas de grandes innovaciones. Si a esa situación le sumamos un mundo sumergido en estrategias de ciberguerra entre estados y afectado por una pandemia, el escenario se convierte en algo aterrador, no solo por las implicaciones financieras sino por las que se pueden tener sobre la supervivencia de las personas.

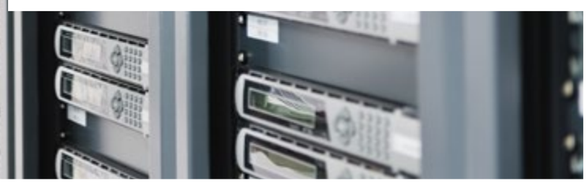
Para mencionar algunos de los eventos a los que nos referimos, tenemos:

- Robos de monedas virtuales
- Pornografía Infantil
- Ciberataques entre potencias que involucran a Israel, Irán, China, Rusia, Estados Unidos, Corea del Norte entre otros.
- Grandes fugas de datos personales.
- Ransomware a hospitales en pleno pico de pandemia.
- Transferencias Interbancarias no autorizadas a través el sistema SWIFT
- Ciberataques a plantas nucleares, oleoductos y sistemas de energía eléctrica
- Espionaje en el hogar a través de ataques a cámaras de vídeo y otros dispositivos de uso doméstico o personal.



Afortunadamente los seres humanos tenemos siempre la oportunidad de poder defendernos ante la incertidumbre y amenazas, la palabra clave para afrontar situaciones como estas es la “Resiliencia”, el concepto de resiliencia, en mi opinión, es seguir avanzando y siendo operativo pase lo que pase, requiere de un gran esfuerzo y compromiso de las organizaciones, principalmente por la gran diversidad de situaciones a las que se ven afrontadas.

Cuando hablamos del sector financiero, encontramos diferentes escenarios de amenazas reales y de incertidumbre que deben ser afrontados para garantizar esa resiliencia, estas son algunas consideraciones importantes para garantizar la supervivencia y afrontar los retos que implican los delitos informáticos.



CONTINUIDAD DE NEGOCIO:

En el caso de los planes de continuidad de negocio, para que garanticen la resiliencia, es muy importante realizar pruebas e incluir en ellos escenarios adicionales a la tecnología, como pandemias por ejemplo y considerar un incremento de la severidad de la situación mientras se tiene activo el plan: terremotos, infección con ransomware, asonadas, entre otros escenarios que pudiesen agravar la situación mientras se está ejecutando la estrategia de continuidad.

ATENCIÓN DE INCIDENTES:

Los incidentes que afronta el sector financiero son muchos, desde ciberataques hasta el robo a mano armada de una oficina. Teniendo en cuenta el escenario hostil que enfrenta el mundo interconectado, se debe asumir que la red corporativa ya está comprometida o que dentro de poco se será víctima de un ciberataque, es por ello que la caza de amenazas (threat hunting) para determinar si en la actualidad existe un compromiso en la red, la implementación de sistemas de EDR/XDR, para reaccionar oportunamente y la implementación de un centro de operaciones de seguridad (SOC), para tener una visibilidad confiable, son claves en el modelo de prevención.

Por su parte, los delitos comunes como fraude en cheques, intrusiones a ATM, cambiazo, entre otros, vienen teniendo un gran componente tecnológico que invita a fortalecer y unificar el mundo ciber con el físico a través de la implementación de capacidades de informática forense.

En cuanto al clásico Phishing, Smishing y suplantación de marcas en redes sociales o sitios web, el establecimiento de protocolos y responsables para la definición de contactos con las compañías de hosting o redes sociales sustentados en un argumento jurídico sólido y predefinido juega un papel importante una vez la entidad ha identificado la acción delincuencial a través de un monitoreo robusto de la red.

Adicionalmente, es importante fortalecer las medidas frente al robo de efectivo y en especial de dispositivos en oficinas tales como computadores y discos de ATM frente asonadas, situación que podría comprometer la seguridad informática de las Entidades frente a un análisis de la postura de seguridad de los Banco por parte de los delincuentes con base en el estudio de esos dispositivos.

GRAN AMPLITUD DE TECNOLOGÍAS EMERGENTES ACOMPAÑADAS DE GRANDES INNOVACIONES.

SEGUIR EN EL JUEGO:

Claramente las entidades financieras deben involucrarse en el escenario competitivo propuesto por las Fintech, incluyendo la necesidad de evaluar la emisión en el futuro de sus propias criptomonedas o usar tecnologías de blockchain en sus procesos de innovación, el cual se ve amenazado por los delitos informáticos y donde la validación de la identidad del usuario/cliente toma una gran relevancia. Es por ello que se deben crear hubs de innovación en ciberseguridad e inclusión de la ciberseguridad en el diseño de productos y servicios en todas las fases de creación y a través del uso de metodologías agiles.

GESTIONAR EL RECURSO HUMANO:

Otro gran reto es capacitar al recurso humano frente a las amenazas derivadas de la ingeniería social, las incomodidades de la automatización y la inteligencia artificial, sumando los riesgos de gestión de cambio, derivados de adoptar nuevos modelos con componentes de ciberseguridad como parte del diseño de productos y servicios.

Una gran estrategia es la prueba y entrenamiento permanente del recurso humano en relación con las nuevas formas de ataque y su rol en los nuevos esquemas de innovación en ciberseguridad.

ANALÍTICA UNIFICADA DE INFORMACIÓN:

La analítica de datos no solo debe verse desde la óptica de negocio, son capacidades que pueden implementar modelos predictivos y reactivos para fortalecer la seguridad en un entorno donde la seguridad física, la seguridad electrónica, el monitoreo de vídeo y el monitoreo informático se unifiquen para afrontar rápidamente amenazas o indicios de estas.

Unificando y haciendo correlación de información de todas las fuentes de seguridad disponibles, físicas y lógicas, se pueden lograr mejores resultados para atender eventos que afronte una Entidad Financiera.

TRABAJO REMOTO.

El acceso a información de clientes de las Entidades de manera remota por parte de los empleados y de terceros, cuando el tercero accede de manera directa a los sistemas de la Entidad o cuando lo hace sobre la información que le ha sido confiada por la Entidad Financiera, genera una serie de riesgos de seguridad de la información, legales y regulatorios. La definición de estándares que incluyan el monitoreo y restricciones sobre el personal y la clara identificación de los riesgos que se aceptarán hacen que el modelo funcione. Adicionalmente la limitación en el uso de los dispositivos se convierte en un reto para los empleadores que deben buscar el punto de equilibrio entre las libertades a permitírsele al empleado en el dispositivo y las que no.

COMPUTACIÓN EN LA NUBE

La dependencia de modelos preconcebidos por terceros para la seguridad de la información y la continuidad de las operaciones genera incertidumbre acerca de la adopción de modelos interesantes basados en computación en la nube. La definición de estándares, aprobación del apetito de riesgo, dosificación de la información entregada, estrategias de continuidad y la revisión seria de las amenazas y sus consecuencias podrán permitirles a las entidades financieras dar sus primeros pasos a los modelos de computación en la nube. También el control de las terceras partes que tienen información de las Entidades y que sustentan su operación en la nube es relevante.

AGILIDAD Y CULTURA

La rapidez con la que se lleven al mercado los nuevos productos y servicios invita a las Entidades financieras a adoptar modelos de gestión de proyectos agiles y de metodologías de iteración como Lean Startup, Desing Thinking u otras similares. Aunque no es suficiente con la adopción de estos modelos. Se hace necesario crear un ambiente de innovación y crear un mix de la cultura innovadora con la cultura actual de cada organización para mantener los valores culturales preexistentes y abrirse a los cambios. Esto aplica en el campo de la mejora de procesos de seguridad de la información, implementación de mecanismos innovadores de ciberseguridad y la seguridad electrónica y física, principalmente por la necesidad de vincular las nuevas iniciativas innovadoras con el campo de la seguridad.

LA FUGA DE DATOS.

Las constantes fugas de datos de terceras partes como el caso reciente de Facebook afectan directamente a los clientes del Sector Financiero ya que esa información será utilizada para la realización de diferentes ataques sustentados en ingeniería social. El reto está en combatir ese contacto no autorizado de los delincuentes que compite con el legítimo y necesario por parte de las Entidades Financieras. Una opción puede ser la realización de pruebas controladas de ingeniería social que busque educar a los clientes del sector y que les permita encontrar y cuestionar las diferencias cuando se ven enfrentados a la duda.

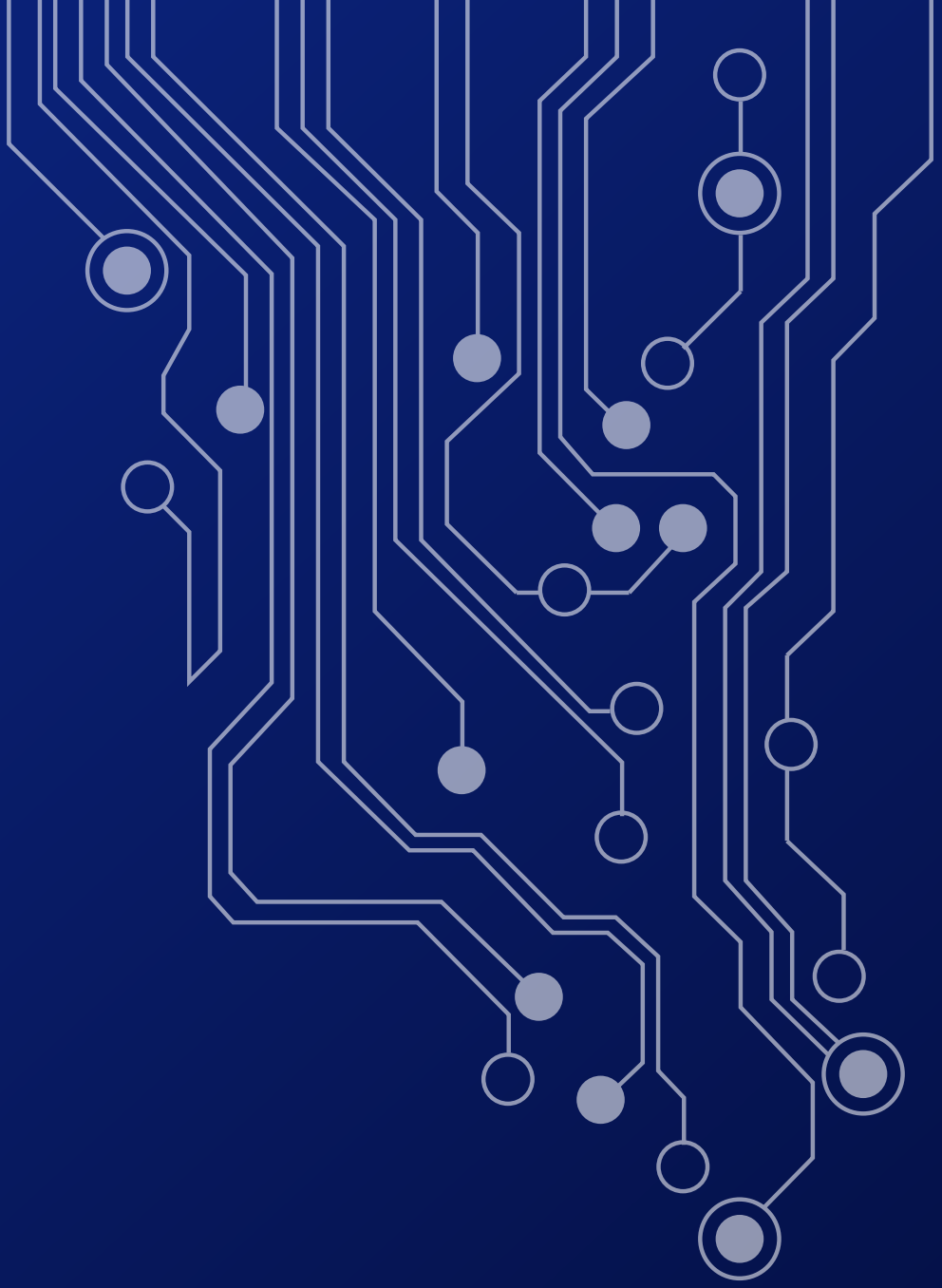
MIX TECNOLÓGICO

El mix tecnológico entre integraciones de terceras partes con aplicaciones de las entidades y conexiones entre sistemas, así como la inclusión de nuevas funcionalidades a las aplicaciones existentes o sitios web genera la incertidumbre de brechas de seguridad que llaman a un proceso serio de ejecución del ciclo de desarrollo seguro de software (SDLC) y a la revisión de la interacción del código fuente de esas aplicaciones para garantizar que es seguro y que no deja fallas fácilmente explotables.

FORTALECIMIENTO E INTEGRACIÓN CON LAS CAPACIDADES DEL ESTADO.

Las entidades financieras y el estado deben integrarse más allá del simple reporte de eventos y empezar a simular de manera más frecuente escenarios de ciberataques en los que se involucren los centros especializados de operación del gobierno, de tal manera que se pueda reaccionar de manera contundente ante un actor malicioso independiente o patrocinado por un estado. En ese mismo sentido, se debe fortalecer a los prosecutores del delito, con formación directa en foros, donde los bancos expongan las modalidades delincuenciales y los prosecutores las formas de persecución para lograr mayor efectividad en los criterios de investigación y rapidez en las respuestas.

Finalmente, ante los constantes cambios y la variedad de amenazas, las entidades financieras deben leer su entorno unificando los componentes de la ciberinteligencia, nuevas tecnología y tendencias en ciberseguridad con los componentes que hoy ya analizan como la geopolítica, los cambios en los mercados de capitales, entre otros, para la toma de decisiones que les permitan ser competitivas y resilientes.



ASOBANCARIA

Construyendo
la **Confianza** y **Solidez** del sector financiero

UNODC

United Nations Office on Drugs and Crime