Edición 01

PERSPECTIVAS EN CIBERSEGURIDAD

AMENAZAS CIBERNÉTICAS POST COVID

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

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.

ESTEBAN ARIAS

Experto, UNODC Colombia.

FREDY BAUTISTA

Experto en Ciberdelito,
UNODC Colombia.

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

SANTIAGO CASTRO

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.

CONTENIDO

PERSPECTIVAS EN CIBERSEGURIDAD

ASOBANCARIA Y LA OFICINA DE NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO.

Tener una mirada holística, que integre varios puntos de vista, es esencial para comprender cómo las problemáticas afectan a sus diferentes actores. Ya sea desde las medidas de protección en las organizaciones, cambios en el marco legal, hábitos de los usuarios o innovaciones tecnológicas, la seguridad digital no es ajena a este acercamiento, siendo un tema que adquiere mayor importancia en una sociedad que utiliza y depende cada vez más de los servicios digitales.

Desde la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, y la Oficina de Naciones Unidas contra la Droga y el Delito en Colombia, UNODC Colombia, hemos creado esta revista digital, Perspectivas en ciberseguridad, buscando de esta manera compartir, descubrir y comprender los puntos de vista de expertos en un tema tan complejo como es la ciberseguridad, que no puede ser comprendido desde una sola óptica.

La industria financiera es uno de los sectores con mayores índices de digitalización en Colombia. De acuerdo con cifras de la Superintendencia Financiera de Colombia, para el primer semestre de 2020, el 65,77% del monto total de las operaciones se realizaron a través de canales no presenciales [1], un crecimiento del 10,3% frente al mismo período del año pasado. Sin duda, algunas de las principales razones para el mayor uso de estos canales fue la promoción del distanciamiento social y el aislamiento preventivo que fue decretado para hacer frente a la pandemia del COVID-19 en el país.

El uso de canales digitales como internet y banca móvil implica nuevos retos, no solo en materia de gestión de riesgo para reducir los efectos de posibles ataques o vulnerabilidades a organizaciones, sino de protección del usuario y sus hábitos al usar estos mecanismos. De acuerdo con cálculos de Asobancaria, para septiembre de este año, las reclamaciones de fraude en ambiente no presente corresponden al 77,12% del total de reclamaciones, lo que demuestra que es necesario buscar y crear iniciativas que involucren no solo a los bancos para reducir el ciberdelito y el fraude.

Desde Asobancaria y UNODC Colombia, agradecemos a los autores invitados por sus esfuerzos y colaboración para el buen desarrollo de este proyecto. Esperamos que esta primera edición y futuras ediciones de la revista permitan identificar fortalezas, oportunidades de mejora y retos en materia de ciberseguridad y seguridad de la información, entendiendo los puntos de vista de sectores como supervisores, creadores de política pública, expertos en ciberdelito y demás roles que juegan papeles cruciales en la agenda de política en ciberseguridad para nuestro país.

1. *Superintendencia Financiera de Colombia (2020). Informe de Operaciones, primer semestre de 2020.*

INCIDENCIA DEL COVID-19

EN EL CIBERCRIMEN DEL 2020 Y FUTUROS RETOS

POR: CR (RA) FREDY BAUTISTA GARCÍA
Experto en Ciberdelito - UNODC Colombia

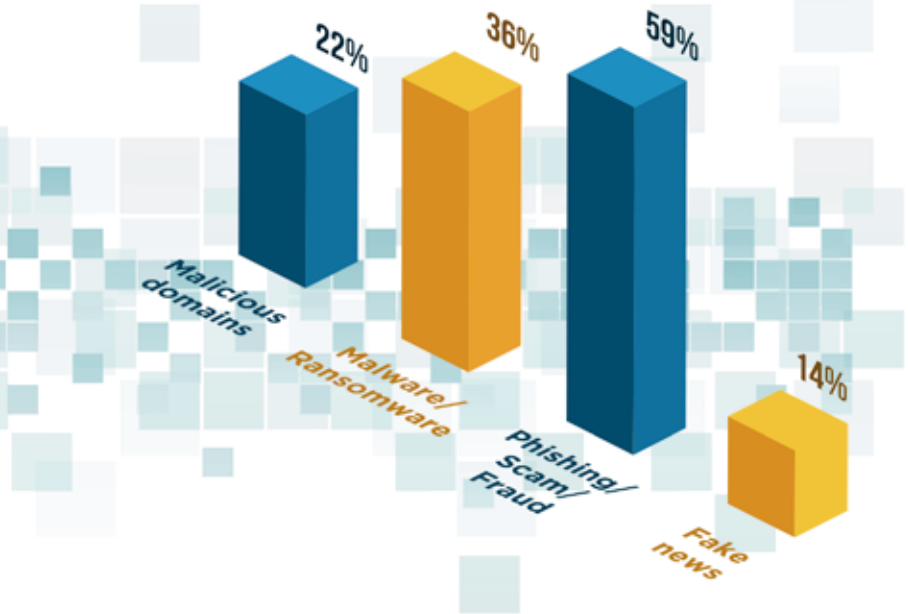
El informe anual 2020 sobre el panorama de amenazas cibernéticas de la Agencia Nacional Europea para la Ciberseguridad (ENISA, 2020) identificó el Top 15 de las Ciberamenazas globales y destacó el incremento de los Ciberataques considerados más sofisticados, dirigidos y difíciles de detectar por los sistemas de seguridad tradicional de los países.

Este panorama de amenazas, valiéndose del miedo e incertidumbre provocados por la inestabilidad de la situación socioeconómica, generada por la pandemia del COVID--19, facilitó el incremento de nuevos ataques basados en la ejecución rápida de estos factores de riesgo.

Esta coyuntura especial ha sido aprovechada por los grupos cibercriminales para acelerar sus campañas de dispersión de malware, el compromiso de data sensible en las organizaciones, facilitar las estafas en Internet y la desinformación, tal como lo aseveró Jürgen Stock, Secretario General de INTERPOL en la presentación del informe: Ciberdelincuencia: Efectos de la Covid-19 (INTERPOL, 2020).

Los principales ciberamenazas descritos en el informe ENISA 2020, incluyen al malware, el ransomware, las brechas de datos, el phishing, los ataques sobre aplicaciones web, ataques DDoS, fugas de información y los robos de identidad.

Fuente: Ciberamenazas 2020 Tomado Sitio Web ENISA



Fuente INTERPOL 2020 Distribución de Ciberamenazas basadas en Covid-19

El informe elaborado por la organización policial internacional a partir de los reportes de los países miembros, indica que las **Estafas por internet** y el **Phishing** con un porcentaje del **59%** fueron las dos modalidades de mayor impacto, pues los ciberdelincuentes suplantando a las autoridades gubernamentales y sanitarias, enviaron a sus víctimas durante los primeros meses de la pandemia, millones de correos electrónicos de phishing con información sobre **COVID--19**, en los que las incitaban a facilitar datos personales y a descargar contenidos maliciosos.

Unos dos tercios de los países miembros que respondieron a la encuesta mundial sobre ciberdelincuencia de INTERPOL informaron de la proliferación del uso de temáticas relacionadas con la **COVID--19** en los delitos de phishing y las estafas por Internet desde el brote de la pandemia. En Colombia las Ciberestafas crecieron un **16.33%** y se registraron más de **45 mil** denuncias entre enero y octubre según cifras de seguimiento al comportamiento delictivo de la Fiscalía General de la Nación.

En un segundo lugar se sitúa el **Malware y el Ransomware** con un **36%** de impacto global de afectación. Al respecto los grupos cibercriminales internacionales incorporaron durante el 2020 un **nuevo mecanismo de presión** a las víctimas, mediante la amenaza de publicación de la información que es **extraída** durante la fase previa a la generación de las llaves de cifrado en el proceso de "secuestro de la información".

Bajo la modalidad de secuestro de información, las organizaciones afectadas además de la gestión propia del ciber incidente y las tareas de restablecimiento del servicio y restauración de la información, deben cuidar que la información de sus clientes o colaboradores no se exponga de manera malintencionada en los foros disponibles tanto en la internet superficial como en la internet profunda DARKNET.

Algunos grupos Cibercriminales vinculados a nuevas familias de malware detectadas en Colombia tras campañas de infección basadas en el ransomware **Sodinokibi/REvil** y **Egregor**, han optado por configurar **"muros de vergüenza"** donde exponen los datos sensibles comprometidos en los sistemas de sus víctimas y presionan de esta manera el pago extorsivo que sigue siendo particularmente a través de Bitcoins y Monero[2].

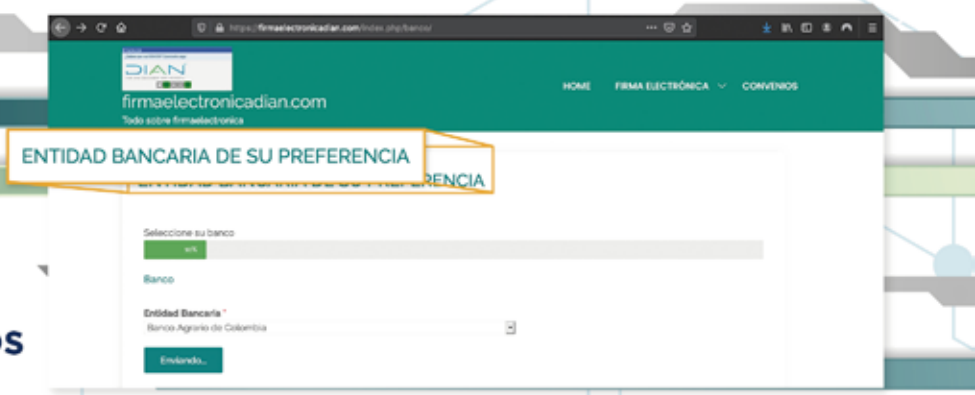
Estos Ciberataques afectaron por igual diferentes sectores productivos del país y empresas prestadoras de servicios, entre ellos el sector de la Salud y aunque los métodos de propagación más utilizados continúan siendo las campañas de phishing que contienen archivos adjuntos maliciosos y que suelen estar en documentos, archivos como ZIP, RAR, ficheros PDF, ejecutables, siguen siendo preponderantes los vectores de infección basados en la suplantación de entidades de gobierno con mayor presencia de trámites en línea

2. *Monero es una criptomoneda de código abierto creada en abril de 2014, que prioriza la privacidad y la descentralización, y se ejecuta en Windows, macOS, Linux, Android y FreeBSD.*

La administración de impuestos y aduanas, la Registraduría Nacional del Estado Civil, la Fiscalía General de la Nación y las autoridades de tránsito en su orden han sido las instituciones mayormente suplantadas, este aspecto debe ser considerado en las estrategias de ciberdefensa de las organizaciones y por tanto la implementación de herramientas de detección de correos maliciosos basados en inteligencia artificial (Deep Learning) IA pueden ser una alternativa para detectar los comportamientos extraños en la cotidianeidad de los correos electrónicos en las organizaciones.

Fuente: Elaboración propia 2020 Muestra de sitio web fraudulento suplantando a DIAN.

En otra tendencia, cibercriminales suplantan página de registro de firma electrónica para capturar datos personales de usuarios



La gestión de permisos para movilidad durante las restricciones y cuarentena, las autorizaciones para trabajo presencial en las sedes de las empresas y el acceso a beneficios y subvenciones del gobierno en torno al **Covid-19**, igualmente han sido utilizados por los Ciberatacante para conseguir engañar a los usuarios e instalar de manera remota códigos de efectos dañinos.

Un **tercer factor** de amenaza durante la pandemia Covid-19 ha sido el auge de dominios maliciosos, su tasa de impacto alcanza un **22%**, y se explica en el registro de sitios web que alojan contenido dañino, útil para la difusión de Malware y Phishing.

Como referencia del crecimiento de esta Ciberamenazas entre febrero y marzo de 2020, un proveedor de Ciberseguridad detectó y comunicó a INTERPOL que los registros maliciosos –malware y phishing incluidos– habían aumentado un **569%**, mientras que los registros de alto riesgo habían subido un **788%.**

Tan solo en la semana doce del año, transcurrida en el mes de marzo, se registraron más de **4.869** dominios asociados a direcciones IP vinculadas a tráfico malicioso, muchos de estas URLs contenían palabras claves como "coronavirus" o "COVID-".

El cuarto factor de ciberamenazas asociadas al COVID-19 tiene relación directa con el incremento de **Fake News** mediante publicaciones de información no contrastada, principalmente asociada a teorías conspirativas entorno a la pandemia, tratamientos médicos, avances de la vacuna, entre otros temas que fomentaron la ansiedad de la población y en algunos casos, facilitó la ejecución de los ciberataques.

Las principales plataformas de tecnología incrementaron los controles para prevenir la utilización de **BOTS** que ayudan a la propagación de estos contenidos falsos con enlaces o vínculos a sitios web con malware.

Durante el mes de marzo por ejemplo Twitter eliminó más de 2.200 tuits con contenido "engañoso y potenpotencialmente dañino" y los sistemas de detección de Fake News identificaron 3,4 millones de cuentas "dirigidas a discusiones sobre COVID--19 con comportamientos de manipulación o spam."

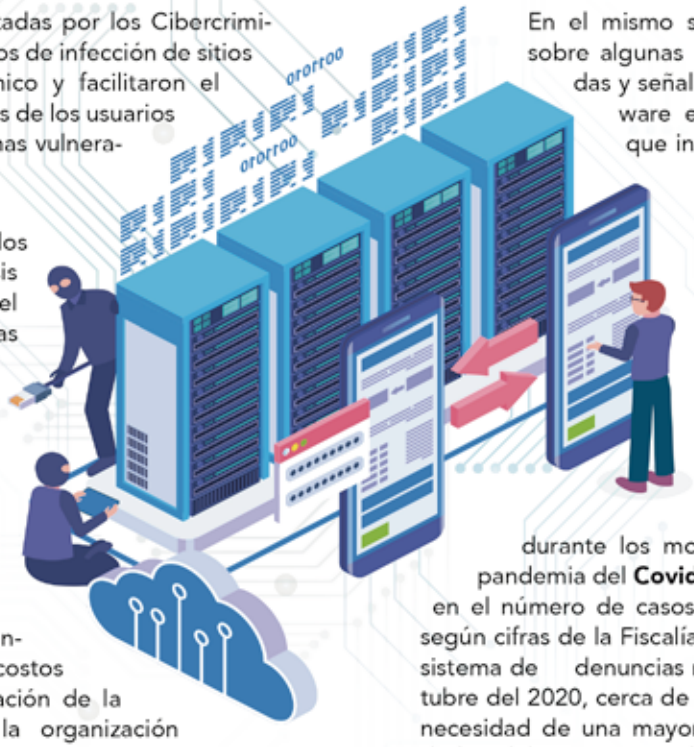
Un bot (aféresis de robot) es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet, cuya realización porparte de una persona seríaimposible o muy tediosa

La misma estrategia fue asumida por Facebook, al generar más de 40 millones de alerta a los usuarios sobre la verificación de contenido considerado como Fake news, y según información suministrada por la misma red social, cerca del 95 % los usuarios notificados no leyeron el contenido.

Por otra parte, la organización policial Europea EUROPOL en su informe de Evaluación de Amenazas del Crimen Organizado en Internet IOCTA 2020, destacó que la pandemia provocó un cambio significativo y una innovación criminal en el ámbito del ciberdelito y que el compromiso de los datos de las tarjetas a través de la modalidad de **e-skimming** (o Skimming digital) aumentó significativamente durante los meses de enero y octubre.

Las ciberamenazas en el sector del **comercio electrónico** tuvieron una importante relevancia durante el 2020, pues muchos de los ciberataques fijaron sus objetivos en los sitios web de establecimientos comerciales y empresas que como medida para mantener activa su operación debieron habilitar sitios en internet y aplicaciones web para la comercialización de sus productos y el relacionamiento con clientes y proveedores.

Las vulnerabilidades explotadas por los Cibercriminales incrementaron los casos de infección de sitios web de comercio electrónico y facilitaron el robo de los datos personales de los usuarios en algunas de las plataformas vulneradas.



La débil conciencia sobre los ciber riesgos y la crisis económica derivada del Covid-19, obligó a muchas organizaciones a priorizar por encima de la ciberseguridad, la comercialización de sus productos, sin valorar adecuadamente el riesgo basado en la evaluación de la probabilidad de ocurrencia de un Ciberataque, el impacto de este en la continuidad del negocio y los costos derivados para la recuperación de la actividad productiva de la organización afectada.

Los grupos cibercriminales dirigieron sus ataques a comerciantes principalmente en **MiPymes**, que no tienen la capacidad de poner en marcha medidas suficientes de protección y suelen ser comprometidos sin que detecten fácilmente la actividad delictiva sobre sus sitios web.

Un ejemplo de esto son los ataques de e-Skimming, los cuales inyectan código JavaScript en los puntos de pago de las páginas de e commerce y así capturan los datos de los clientes.

(EUROPOL IOCTA, 2020)

En el mismo sentido el reporte advierte sobre algunas de las amenazas identificadas y señala algunas variantes del malware en puntos de venta (POS), que incluyen entre otros los siguientes: PwnPOS, AlinaPOS y POSeidon/ Backoff. Más detalles de estas ciberamenazas están disponibles en el informe de EUROPOL.

Todos los anteriores factores de amenazas y riesgos durante el 2020 han impactadoa las organizaciones en Colombia durante los momentos más críticos de la pandemia del **Covid-19**. El incremento del **70%** en el número de casos exitosos de ciberataqzues según cifras de la Fiscalía General de la Nación cuyo sistema de denuncias reportó durante enero y octubre del 2020, cerca de **28.180** casos, demuestra la necesidad de una mayor articulación de las autoridades del ecosistema de Ciberseguridad para enfrentar con éxito a las grupos de cibercriminales; pero también exige de las organizaciones del sector privado asumir mejores posturas de seguridad tales como la asignación de un responsable de la seguridad de la información, una estrategia de respuesta a ciber incidentes , el fortalecimiento en el tratamiento de la evidencia digital y una cooperación interinstitucional que facilite el intercambio de ciber inteligencia a través de equipos especializados en respuesta a incidencias informáticas.

UN SISTEMA FINANCIERO MÁS INCLUSIVO Y CIBERSEGURO

POR: SANTIAGO CASTIBLANCO HERNÁNDEZ
Profesional Junior, Dirección de Gestión Operativa y Seguridad de Asobancaria

Uno de los principales retos que trajo consigo la pandemia en diversos países fue cómo ofrecer los servicios financieros y transaccionales a usuarios sin necesidad que estos se desplacen o reduciendo lo máximo posible la interacción entre personas, para de esta manera permitir el aislamiento social sugerido por las instituciones de salud. Si bien la industria financiera ha experimentado un desarrollo tecnológico brindando a los clientes facilidades electrónicas para sus trámites, esto ha tenido niveles de implementación y de aceptación diferente alrededor del mundo, por lo que aún hay países que mantienen un alto uso del efectivo. Del mismo modo, el uso de canales y servicios digitales también implica garantizar su confiabilidad desde la óptica de ciberseguridad y seguridad de la información.

Las autoridades gubernamentales han incentivado el uso de medios de pago electrónicos en especial en aquellos países en donde el uso del efectivo sigue siendo frecuente. Esto implica ofrecer e implementar mecanismos de pago diferentes al efectivo para la mayoría de su población.

De acuerdo con el **World Cash Report** (G4S, 2018), para 2016, la razón entre moneda en circulación sobre PIB en Sudamérica es del 16%, lo cual hace que la región cuente con el mayor índice al compararla con África, Asia y Norteamérica, en donde el porcentaje es de 10%, 9,6% y 6,13% respectivamente. En Oceanía -la región con relación más baja – la razón es de menos del 4%.

En Europa, con cerca del 9%, países como Suecia, Países Bajos y el Reino Unido han disminuido el uso de efectivo.

Suecia se considera como uno de los principales ejemplos de países que están cerca a ser *cashless*,con un porcentaje de 15% de pagos realizados en efectivos en puntos de venta -POS-, el ciudadano sueco promedio realizó 319 pagos con tarjeta en 2016, mientras el promedio en la Unión Europea es de 116 pagos.

Se considera como factores principales en esta tendencia la baja densidad población que incrementa los costos de distribución de efectivo a lo largo del país, la confianza que tienen los suecos hacia el gobierno, el sistema financiero y la tecnología (G4S, 2018).

Por el contrario, en países como Bélgica, Francia y España, el porcentaje de transacciones con efectivo en POS es de 63%, 68% y 87% respectivamente, aun cuando en estos tres países el número de datáfonos per cápita es superior al promedio global -1.500 terminales POS por cada 100.000 habitantes- (G4S, 2018). Esto demuestra, que la preferencia por pagar con medios de pago diferentes al efectivo va más allá de factores como el desarrollo de los mercados o una infraestructura apropiada.

En Suramérica, en promedio, los países han aumentado el uso de efectivo. A pesar de que la infraestructura para pagos electrónicos ha mejorado en los últimos años, ésta aún se encuentra rezagada. La mayoría de los países de la región se encuentran por debajo del indicador promedio de tarjetas y terminales POS por habitante -el promedio de la región es de 1,5 tarjetas por persona y 1.055 terminales POS por cada 100.000 habitantes, frente al promedio global de 2 tarjetas por persona y 1.500 terminales-. En cuanto al uso de tarjetas en transacciones por habitante por año, es aún bastante bajo al compararlo al promedio global (103 transacciones), siendo Brasil y Colombia los países con promedio más alto, con 31,6 y 18 transacciones por persona en promedio respectivamente (G4S, 2018). En este escenario, agendas gubernamentales que incrementen el acceso a pagos electrónicos permitirán reducir el uso de efectivo, a su vez que grupos poblacionales que no han podido acceder a diferentes instrumentos financieros los puedan conocer, usar y beneficiar de sus características.

Ahora bien, además de los pagos con tarjetas crédito y débito, los establecimientos comerciales y las entidades financieras han innovado con aplicaciones móviles y diferentes medios de pago que reducen el efectivo y contacto físico entre personas. El acceso a telefonía móvil juega un rol primordial en la inclusión financiera.

Un claro ejemplo de esto es África, donde en promedio los habitantes tienen un mayor acceso a celulares (se estiman cerca de 102 subscripciones de telefonía móvil por cada 100 habitantes) que a tarjetas de crédito o débito (G4S, 2018).

A través de diversas aplicaciones de dinero móvil ***-mobile money*** en inglés, producto que permite guardar los fondos en el teléfono móvil y ser transferidos a partir de este- ciudadanos de este continente han podido acceder al sistema financiero, con el 35% de adultos en áreas rurales reportando que han usado los servicios de m-money en Ghana, con 1,7 billeteras móviles por adulto en Kenia, y con 95,1 millones de usuarios en Tanzania (World Bank, 2020).

Por otro lado, el incentivar el mayor uso de pagos electrónicas y herramientas digitales como aplicaciones de banca móvil, implica que el gobierno y el sector financiero diseñen una agenda y mecanismos de seguridad que le brinden y garanticen al usuario seguridad al realizar sus transacciones.

El aumento de campañas de phishing de temática de **COVID-19**, donde ciberdelincuentes se han hecho pasar por instituciones estatales o financieras que buscan engañar a usuarios para que estos entreguen su información personal, junto al incremento de personas desarrollando sus actividades laborales a través de teletrabajo, hicieron que este aspecto adquiriera un mayor protagonismo. De acuerdo con el **Fortinet Thread Intelligence Insider** para América Latina (2020), en Latinoamérica se identificaron en abril de este año más de 4.250 campañas de phishing relacionadas con COVID-19 por correo electrónico. En el caso colombiano, la lucha frente al **phishing** y **smishing** tiene limitaciones desde el marco normativo que dificultan el bloqueo de sitios y el rastreo de los números telefónicos fraudulentos, por lo que cada vez es más imperante el desarrollo de nuevas estrategias para afrontar estos delitos.

Estos engaños y los esfuerzos en prevención no solo se dan en economías en desarrollo como las latinoamericanas.

En Reino Unido, se detectó que a través de correos de phishing de COVID-19 se estafaron cerca de 800.000 libras esterlinas en el mes de febrero, con mensajes de **Action Fraud** (el Centro Nacional de Reporte de Cibercrimen y Fraude) de proteger sus dispositivos y no oprimir en archivos adjuntos o links de correos electrónicos sospechosos (Action Fraud, 2020).

La implementación de estrategias y mecanismos orientado a aumentar la seguridad en pagos electrónicos no es un tema que nazca desde la pandemia de coronavirus.

Una de las principales innovaciones en métodos de pago ha sido la implementación de la opción de pago contactless en tarjetas crédito y débito, la cual fue desarrollada junto a la creación en 1996 del estándar EMV, cuando Europay, MasterCard y Visa crearon el estándar EMV, característico por incluir un chip en el plástico de la tarjeta, lo que permite que el almacenamiento de la información sea más seguro y reduce de gran de gran manera el riesgo de fraude mediante skimming (EMVCo, 2014), este estándar es utilizado en más de 80 países donde se ha reducido de manera significativamente el fraude a través de tarjetas crédito y débito (Mastercard). Si bien las tarjetas con chip existen desde 1996, el que no sean utilizadas aún en la mayoría de los países demuestra en primera medida los retos que presentan varios países al establecer estándares de ciberseguridad en transacciones, en este caso, con tarjetas de crédito y débito.

Por su parte, además de innovaciones tecnológicas que reduzcan el fraude y los ciberataques, organizaciones privadas y entidades públicas y policiales hacen diversos esfuerzos para concientizar a los usuarios financieros de no entregar sus datos personales, no abrir correos sospechosos y en general a tener buenos hábitos de ciberseguridad.

En Colombia, Asobancaria de la mano de Incocrédito y la Policía Nacional realizan campañas de sensibilización dirigidas a clientes de establecimientos bancarias con medidas básicas de seguridad al efectuar transacciones o al no entregar información delicada por teléfono o portales de internet no seguros.

En un mundo post pandemia, que el sistema financiero sea ciberseguro y pueda brindar acceso a todos los ciudadanos es vital para poder asegurar que todos podamos participar de sus productos y ser menos susceptibles ante ciberataques o limitaciones físicas-geográficas que puedan llegar a surgir.

Como se observa, la pandemia actual representa un reto en temas de inclusión y ciberseguridad para las entidades financieras, siendo una prueba de qué tanta profundización tiene los productos financieros electrónicos, qué tan seguros son, qué tanta educación ha recibido los usuarios para un adecuado manejo de estos, y cómo se pueden mejorar estas deficiencias en un mediano plazo.

LA CONFIANZA DIGITAL

EN UN MUNDO POST PANDEMIA

POR: IVÁN MAURICIO DURÁN PABÓN
Director de Desarrollo Digital, Departamento Nacional de Planeación.

En los últimos años el entorno digital ha sido el escenario en el que se han desarrollado todo tipo de actividades socioeconómicas. En el mundo más del 50 % de la población está en línea y cerca de 1 millón de personas cada día comienzan a usar Internet. Específicamente en Colombia, según la Encuesta Nacional de Calidad de Vida (versión 2020), el 65% de personas de 5 años o más usan Internet en cualquier lugar y desde cualquier dispositivo.

También la llegada de la Cuarta Revolución Industrial está impulsando rápidamente la transformación de todos los sectores de la economía. Según estimaciones del (Foro Económico Mundial, 2019), para 2022 se digitalizará más del 60 % del PIB mundial y alrededor del 70 % del nuevo valor creado en la economía durante la próxima década se basará en plataformas digitales. Adicionalmente, según el estudio Securing the Digital Economy, el nivel de dependencia a Internet se ha incrementado de un 23 % en 2008 a un 100 % en 2018, tal como lo reporta el 68 % de los CEOs de las empresas que hicieron parte de este estudio.

Sin embargo, estos mismos CEOs reconocen que el nivel de confianza en Internet es muy bajo, siendo apenas del 30 % en 2018, y se estima que para 2023 caerá al 25 % si nada cambia para mejorarlo. Lo anterior genera grandes retos, ya que se asume que en los próximos cinco años el nivel de dependencia a Internet se mantendrá en el 100 % (Accenture, 2019).

Esta dependencia a Internet, así como la mayor participación y desarrollo de la vida cotidiana de los ciudadanos y las actividades de las empresas en el entorno digital, también implica una mayor exposición a las amenazas y ataques cibernéticos más sofisticados y complejos por parte de delincuentes que aprovechan el creciente intercambio de información y conllevan graves consecuencias de tipo económico o social.

Según estimaciones de Accenture, el costo para los negocios derivado del impacto de los ciberdelitos ha incrementado en un 72 % entre 2014 y 2019 (Accenture, 2019).

Estas proyecciones se realizaron en el contexto previo a la pandemia y en efecto eran magnitudes ya de por sí relevantes que daban paso a grandes desafíos para las diversas acciones de política de los diferentes gobiernos en torno a la seguridad y confianza digital.

Si bien es cierto, la actual situación derivada de la pandemia originada por el COVID-19 ha puesto a prueba la efectividad de las diferentes políticas públicas, y en especial las relacionados con confianza y seguridad digital, pues el uso intensivo del entorno digital ha sido el mecanismo para realizar las actividades socioeconómicas en todos los países, lo que ha incrementado notablemente los desafíos en torno a la seguridad y confianza digital, para que este entorno digital pueda ser aprovechado de manera segura y confiable.

Lo anterior exige establecer medidas para ampliar la confianza digital y mejorar la seguridad digital no sólo durante, sino de manera posterior a esta pandemia, ya que se ha marcado un hito socioeconómico que ha reestructurado el comportamiento entre los usuarios y quiénes deben garantizar la confianza digital, derivado de los esquemas de confinamiento.

Por ejemplo, para abril de 2020, la CRC reportaba un incremento del tráfico de Internet cercano al 38,8%. Esto a la final representa más usuarios, más teletrabajadores, más interacciones digitales y más datos e información que se intercambia y también implica una mayor exposición a las amenazas y ataques cibernéticos que debilitan la confianza digital.

Para Colombia, en relación con la confianza digital, es importante trazar una "línea base" para determinar acciones que permitan, como mínimo, que el estado actual del país en ese tema no se desdibuje. A través del Índice de Evolución Digital 2017 (Chakravorti & Ravi, 2017), se analizan los impulsores que rigen la digitalización de un país, entre ellos, el entorno de confianza digital. Este índice muestra que el país ocupa el puesto 32 entre un total de 42 países con relación a la evolución del entorno de confianza digital, con un desempeño por debajo del promedio global. Este entorno de confianza digital por debajo del promedio no facilita el intercambio efectivo de información, bienes y servicios en línea, que es una situación que se agrava en este momento de pandemia y que muy seguramente continuará una vez se haya superado la misma.

Por eso, el Gobierno nacional considera prioritario atender los nuevos retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital, en pro del desarrollo de una economía digital, y la construcción de un entorno digital seguro, como elemento clave para que sea confiable, y que esté acorde con el aumento y dinamismo de las actividades digitales. (Departamento Nacional de Planeación, 2020).

No sólo durante la pandemia, sino después de ella, la confianza y la seguridad digital se convierten en temas clave para el país y su reactivación económica, al permitir un entorno digital en el que puedan adelantarse las diferentes actividades e interacciones digitales sin que se vean afectadas por amenazas o ataques, generando así estabilidad, promoviendo el desarrollo socioeconómico y facilitando el tránsito socioeconómico hacia la Cuarta Revolución Industrial.

Por tanto, alcanzar el objetivo trazado en el CONPES 3995 Política Nacional de Confianza y Seguridad Digital, cobra una mayor profundidad. La situación post pandemia debe apuntar a implementar medidas para el fortalecimiento continuo de la seguridad, y para la generación de la confianza digital.

Para esto se debe potenciar la anticipación, la gestión de riesgos, la atención oportuna y la defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional fuerte, eficiente y acorde con las necesidades actuales, de manera que se pueda materializar rápidamente la confianza y la seguridad digital ante nuevas situaciones en las que se lleve al máximo el uso del entono digital.

Históricamente, y ahora más que nunca, se requiere que Colombia sea efectivamente una sociedad incluyente y competitiva en el futuro digital.

El mundo se ha reformado y nuestras interacciones cotidianas han cambiado para siempre. La pandemia nos obligó a acercarnos al mundo digital, y el mundo digital nos ofreció soluciones para mantener en funcionamiento la sociedad. Muy seguramente derivado de esto, en el futuro nuestras interacciones se forjarán a través de lo digital.

La confianza digital juega un papel crucial en el desarrollo socioeconómico de los países. Esta pandemia pasará a la historia por muchas cosas, pero con mucha seguridad será recordada como aquella que no sólo fue combatida desde los laboratorios, sino que también fue combatida construyendo una dinámica social sustentada en el entorno digital.

REFERENCIAS

INCIDENCIA DEL COVID-19
EN EL CIBERCRIMEN DEL 2020 Y FUTUROS RETOS

- ENISA. (Octubre de 2020). https://www.enisa.europa.eu/. Obtenido de https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
- EUROPOL IOCTA. (Octubre de 2020). Europol.eu. Obtenido de https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
- INTERPOL. (Agosto de 2020). Interpol.int. Obtenido de https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

UN SISTEMA FINANCIERO MÁS INCLUSIVO Y CIBERSEGURO

- https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month
- https://www.emvco.com/wp-content/uploads/2020/03/COLOR-CORRECT-EMVCo_statistics-20200306.pdf
- https://cashessentials.org/app/uploads/2016/07/2018-world-cash-report.pdf
- http://pubdocs.worldbank.org/en/230281588188110691/Digital-Financial-Services.pdf
- https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122152753.pdf
- https://www.fortinetthreatinsiderist.com/es/current/landing
- https://sea.mastercard.com/en-region-sea/merchants/safety-security/emv-chip.html

LA CONFIANZA DIGITAL
EN UN MUNDO POST PANDEMIA

- Accenture. (2019). Securing the Digital Economy. Reinventing the Internet for Trust. Obtenido de https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf
- Accenture. (2019). The Cost of Cybercrime. Obtenido de https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
- Chakravorti, B., & Ravi, C. (2017). Digital Planet 2017. Obtenido de https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf
- Comisión de Regulación de Comunicaciones (2020). Segundo Reporte de Tráfico de Internet durante el Aislamiento Preventivo. Obtenido de https://www.crcom.gov.co/es/noticia/segundo-reporte-de-trafico-de-internet-durante-el-aislamiento-preventivo
- Departamento Nacional de Planeación (DNP). (2016). POLITICA NACIONAL DE SEGURIDAD DIGITAL . Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- Departamento Nacional de Planeación. (2020). Documento CONPES. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3985.pdf
- Foro Económico Mundial - FEM. (2018). Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Obtenido de http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf
- Foro Económico Mundial. (2019). Shaping the Future of Digital Economy and New Value Creation. Obtenido de https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation