MODALIDADES DE CIBERCRIMEN EN TIEMPOS DE PANDEMIA COVID-19 EN BOGOTÁ (COLOMBIA).

Ensayo presentado por:

CARLOS JACINTO CASTELLANOS VEGA

Tutor Temático: LUIS EDUARDO GÓMEZ HERNÁNDEZ

Tutor Metodológico: Cr(r) JORGE ALONSO ISAZA QUEBRADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGÍA Y SEGURIDAD.

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ D.C. JUNIO DE 2.020

Resumen

El siguiente ensayo se realizó con el fin de evidenciar la afectación que han tenido los ciudadanos por el uso de sus dispositivos o equipos de cómputo por parte de los ciberdelincuentes quienes usando distintas modalidades de Cibercrimen han aprovechado estos tiempos de Pandemia COVID-19 en Bogotá D.C.

La Información analizada permitió realizar un comparativo de las diferentes modalidades de Cibercrimen denunciadas por la ciudadanía en las 20 localidades de Bogotá y demuestra a partir de 10 variables la dinámica que ha impactado en la población el tener que hacer uso de sus equipos o dispositivos cumpliendo la medida de aislamiento preventivo obligatorio abriendo una ventana de oportunidad para los ciberdelincuentes.

Se concluyó que una vez se aumentaron las tareas en casa producto del confinamiento la ciudadanía en general quedo expuesta a los diferentes ataques cibernéticos, estas actividades delictivas pasaron de 33 modalidades de Cibercrimen (1.025 denuncias en el periodo 2.019) a 41 modalidades (2.016 denuncias en el periodo 2.020).

Palabras claves: cibercrimen, ciudadanía, COVID-19, equipos de cómputo, modalidades, seguridad informática, teletrabajo.

Abstrac

The following trial was carried out in order to demonstrate the affectation that citizens have had due to the use of their devices or computer equipment by cybercriminals who, using different modalities of Cybercrime, have taken advantage of these times of Pandemic COVID-19 in Bogotá D.C.

The analyzed information allowed a comparison of the different forms of Cybercrime denounced by citizens in the 20 localities of Bogotá and demonstrates from 10 variables the dynamics that have impacted the population having to use their equipment or devices in compliance with the mandatory preventive isolation measure opening a window of opportunity for cybercriminals.

It was concluded that once the tasks at home were increased as a result of confinement, the general public was exposed to different cyber-attacks, these criminal activities went from 33 forms of Cybercrime (1.025 complaints in the period 2.019) to 41 modalities (2.016 complaints in the period 2.020).

Key words: cybercrime, citizenship, COVID-19, computer equipment, modalities, computer security, telework.

Introducción

Este ensayo pretende reflejar, la evolución dinámica que han tenido las modalidades de Cibercrimen en Bogotá en tiempos de la pandemia COVID-19, a partir de la emergencia sanitaria decretada por el Gobierno en Bogotá mediante la Resolución número 385 del 12 de marzo del 2.020. Con base a lo anterior se focalizará en las denuncias reportadas por la ciudadanía en las 20 localidades de Bogotá, evaluando el impacto de las modalidades de cibercrimen en los denunciantes, a partir de diez variables: tipo de denuncia interpuesta por la ciudadanía, localidad más afectada, días de la semana, rango de horas, género, rango de edad, grado de escolaridad, estado civil, profesión de los denunciantes, sitios de mayor afectación y comportamiento de las modalidades asociadas a los hechos punibles denunciados con infracción a la Ley 1273 del 2.009. La muestra objeto de estudio, permitirá realizar un comparativo para los períodos 12 de marzo al 12 de mayo de los años 2.019 y 2.020 y lograr realizar el análisis y evaluación de las variables antes mencionadas.

Así mismo, se pretende establecer si se cuenta con el desarrollo tecnológico en la ciudad para enfrentar estas modalidades denunciadas y verificar que capacidades técnicas y humanas tienen actualmente las autoridades en cabeza del Órgano Investigativo en Colombia que es la Fiscalía General de la Nación y otras entidades que cumplen o coadyuvan en la Investigación de hechos punibles como la Policía Nacional de Colombia a través del Grupo de Delitos Informáticos de la Dirección de Investigación Criminal e INTERPOL.

Por último y consecuente con este aspecto, impactar con algunas recomendaciones de expertos en materia de Ciberseguridad, a fin de que los lectores conozcan y sirvan de multiplicadores ante la comunidad en general, de manera que sirva como espacio preventivo para no ser victima de los ciberdelincuentes.

Desarrollo

Definición de Cibercrimen

De acuerdo con la entrevista otorgada en la página web a la empresa proveedora de información y capacitación Infolaft, sin fecha de publicación, el Mayor Félix Daniel Miranda, jefe del Grupo Investigativo contra el Ciberterrorismo de la Dirección de Investigación Criminal e Interpol (Dijin), definió el cibercrimen como ¨aquel conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones (TIC) que atentan contra esos tres conceptos del ciberespacio que son la confidencialidad, la integralidad y la disponibilidad de la información. (Infolaft, s.f.). Según Armando Colmenares Duque, Fiscal del CTI, experto en delitos informáticos, resaltó que el robo de las cuentas bancarias a través de plataformas, es la conducta delictiva que crece masivamente en la red. (Fiscalia.gov.co, 2.018). Por su parte el CAI virtual del centro cibernético policial define las primeras ocho modalidades de cibercrimen en su mural (Caivirtual.policia.gov.co, 2.020) como 8 categorías así:

Phishing

Es un delito conocido como suplantación de identidad, esta modalidad se caracteriza por intentar adquirir información confidencial de forma fraudulenta como contraseñas, información sobre tarjetas de crédito o información bancaria, esta trampa llega por correo electrónico o falsos websites que se muestran como páginas de facebook o bancos para obtener la información.

Skimming

El fraude o robo de información de tarjetas de crédito se toma como un delito cibernético debido a que es usual en cajeros automáticos, restaurantes y bares. Consiste en el copiado de la banda magnética de la tarjeta con el objetivo de desocupar las cuentas bancarias o pedir avances.

Estafa Cibernética

Se da por publicidad que ofrece grandes descuentos, esta generalmente es un enlace que conduce a una pagina que pide su información personal, con el objetivo de hackear el dispositivo y obtener beneficio.

Carta Nigeriana

Esta modalidad se lleva a cabo principalmente por correo electrónico, generalmente es una carta ofreciendo una fortuna inexistente a cambio de pagar un dinero por adelantado.

Malware

Este funciona a través de un mail que puede ser de cobranza de alguna entidad bancaria o reportando que tiene una investigación por parte de la fiscalía o una multa por exceder la fecha limite de pago, con el objetivo de que usted de click; esto hace que automáticamente se descargue un virus a su computador, generando daño en el equipo y robando la información.

Smishing

Se da principalmente por mensajes de texto al móvil o incluso llamadas, que intentaran suplantar la identidad de alguna persona entre los contactos del usuario del teléfono o intentando que acceda a un link para reclamar un premio, con el fin de solicitar dinero a un conocido suyo por medio de un mensaje o hackear el celular.

Ramsomware

Es un programa de software malicioso que infecta un equipo de cómputo y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. Esta modalidad tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos

importantes predeterminados con una contraseña. Principalmente han sido detectados cinco tipos de clases: 1.Ramsomware de cifrado que cifra archivos personales y documentos hojas de cálculo, imágenes y video; 2.Lock Screen Ramsomware Winlocker bloquea la pantalla del PC y solicita el pago; 3.Masterd Boot Record (MBR) Ransomwa-realware es la parte del disco duro del PC que permite iniciar el sistema operativo; 4.Ransomware de cifrado de servidores web, su objetivo son los servidores web y cifrar sus archivos; 5.Ransomware de dispositivos móviles principalmente Android pueden infectarse mediante descargas no oficiales. (Kaspersky, 2.020).

Vishing

Mediante esta modalidad los ciberdelincuentes hacen uso del protocolo voz sobre IP (VoIP), y la ingeniería social para engañar a las personas y obtener información financiera sensible o útil para el robo de identidad, esta modalidad opera mediante llamadas telefónicas utilizando mensajes pregrabados o de una persona que llama para solicitar información financiera personal. (Reporte Digital, 2.019).

Para luchar contra estas modalidades cibercriminales, una de las herramientas legales que el Congreso dicto fue la Ley 1273 del 2.009, ¨De la Protección de la Información y los datos¨ (Secretariasenado, 2.019) la cual brinda un soporte institucional a las autoridades encargadas de combatir este flagelo, a continuación se presenta un resumen donde se establece el artículo Penal creado, cuando se vulnera y que pena estableció el legislador en cada uno de los artículos siguientes (llámese prisión o multa).

Figura No. 1 Legislación Penal Colombiana frente a los delitos informáticos Art. 1, Ley 1273

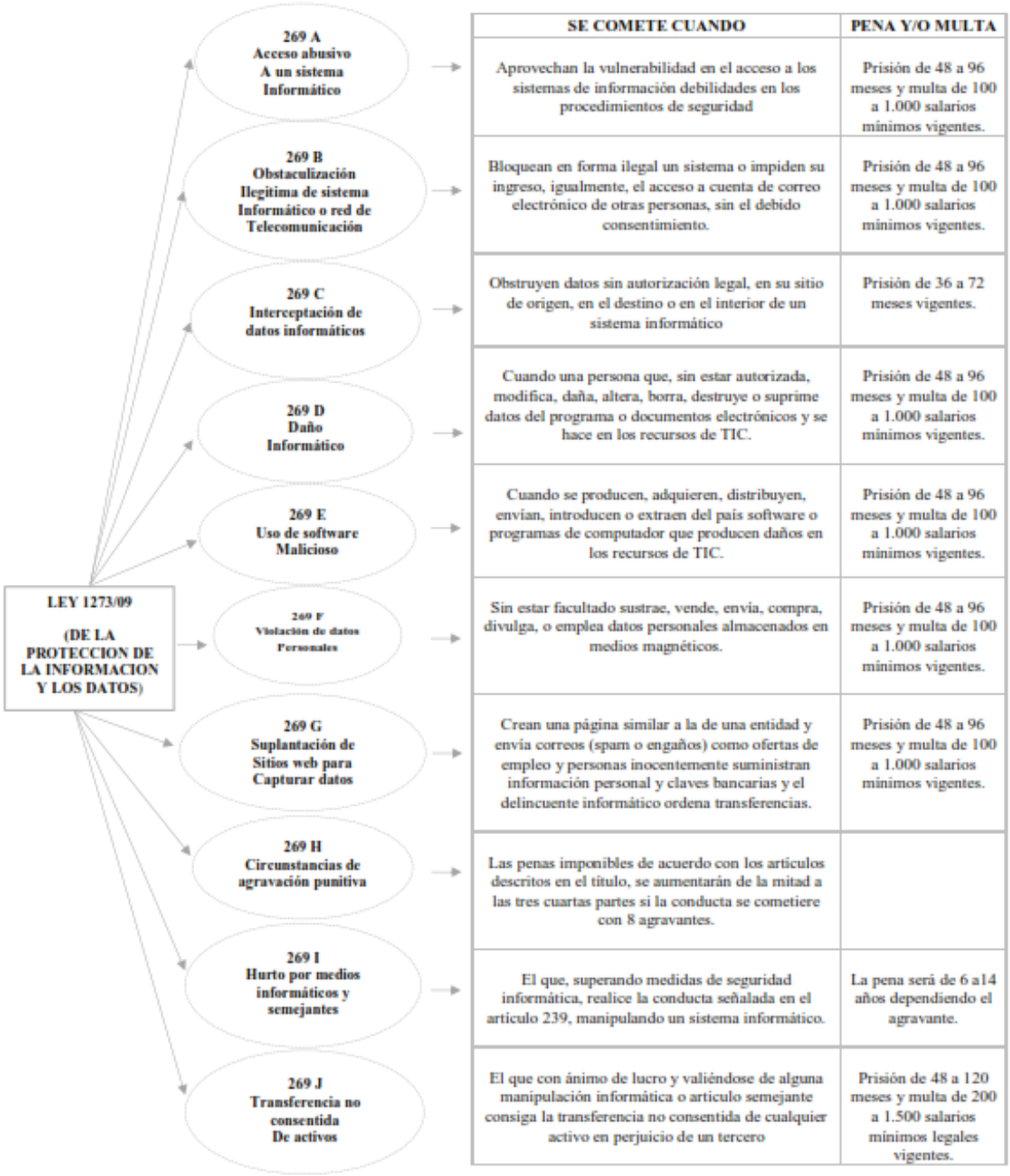


Figura No. 1. Legislación penal colombiana frente a los delitos informáticos. (Art. 1 de la Ley 1273/09)
Fuente: Elaboración del autor con base en la Ley 1273 de 2.009. (Congreso de la Republica (2.009)

Fuente: Elaboración con base en la Ley 1273 de 2.009 (Congreso de la República).

El Teletrabajo la Puerta Hacia los Ciberataques

El teletrabajo se encuentra definido en la Ley 1221 de 2.008 como: “Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo” (mintic.gov.co, 2.008). Sin embargo, una de las consecuencias de la crisis del COVID-19 es la improvisación y adaptación de los ecosistemas informáticos de las empresas y de sus sistemas de gestión al teletrabajo. La necesidad de cerrar los centros físicos de trabajo, como oficinas o coworkings, ha precipitado esta modalidad productiva con todos los riesgos que esto supone en cuanto a seguridad informática. (Directivos y Empresas, 2.020).

El Ministerio de Tecnologías de la Información y las Comunicaciones realizó conjuntamente con Nubelo, la plataforma número uno de habla hispana de trabajo 3.0, el primer estudio en Colombia que tiene como objetivo la identificación de las necesidades de la comunidad de Teletrabajo autónomo del país, haciendo un especial énfasis en la capital de la Republica (45%) de los encuestados, el estudio indico que para este año 2.020 el 50% de la fuerza laboral sería digital (Teletrabajo.gov.co, 2.015, p. 3). Según la última encuesta realizada por el Ministerio de Tecnologías de la Información y Comunicaciones, hasta el 2.018 existían 122 mil teletrabajadores en Colombia, siendo Bogotá la ciudad que concentra el mayor número con 63.995. (Secretaria.gov.co, 2.019). De acuerdo a estimativos de la Federación de Aseguradores Colombianos (Fasecolda) y las Administradoras de Riesgos Laborales (ARL) de 10,4 millones de trabajadores registrados se estima que entre 2 y 3 millones se encuentran trabajando en casa. (ElTiempo, 2.020).

A partir del cruce de información de las últimas dos fuentes se calcularía en cerca de más de 2.500.000 personas que aproximadamente en Bogotá tienen un empleo formal, si se reducen quinientos mil empleos que se perdieron en el último mes (Revista Semana, 2.020) nos queda un aproximado de 2.000.000 de empleos formales que divididos en el 25% que corresponden al dato de las Administradoras de Riesgos Profesionales, actualmente en Bogotá se encuentran en teletrabajo más de 480.769 personas, esto comparado a la ultima cifra oficial de 63.995, destaca un incremento de más del 751%, todo esto para significar que el cibercriminal hoy en dia tiene multiplicadas sus opciones de ataques cibernéticos con una gran posibilidad de éxito.

La ciberseguridad es una tarea pendiente en muchas empresas, especialmente en el caso de pymes y autónomos. Los hackers o ciberdelincuentes saben que la coyuntura económica y sanitaria es una puerta abierta a numerosos dispositivos y sistemas informáticos que contienen importantes cantidades de información y que en estos momentos no se están custodiando de forma apropiada. Ahora bien, la información de las empresas está siendo tratada por trabajadores que utilizan sus propios dispositivos y redes de conexión a internet, lo que supone una enorme debilidad en seguridad y una llamada perfecta de acción para los ciberdelincuentes.

Un primer riesgo que corren las empresas es la falta de computadores propios para abastecer a todos sus empleados. Por lo anterior es importante contar con una VPN (Red Privada Virtual) que permita el acceso remoto a programas, archivos y que además permita cifrar el contenido y contar con actualizaciones de seguridad. (Yeshica, 2.020)

Cecilia Pastorino, especialista en Seguridad Informática de Eset Latinoamerica, cree que hay dos riesgos principales: 1. La confidencialidad de la información y 2. La disponibilidad de los servicios. En el primer riesgo explica que los hábitos inseguros en las comunicaciones remotas pueden habilitar que los atacantes tengan un camino adicional para acceder a la información confidencial de la empresa. En el segundo riesgo señala que ¨cuando muchos trabajadores se conectan en remoto al mismo tiempo, se provoca que el sistema de red privado colapse y que después nadie pueda hacer su trabajo de manera oportuna ¨. (Ona Systems, 2020)

A la hora de trabajar desde casa, es usual que los equipos (propios del trabajador o de la empresa) tengan acceso a sistemas a través de una red VPN, que cifra el tráfico desde el origen, es decir, desde la computadora del empleado hasta la computadora de la empresa, la información esta protegida por un firewall que bloquea el acceso no autorizado, y con protocolos IDS o IPS que permiten a los equipos técnicos el detectar y prevenir intrusos.

Según Alexander Ramírez, Gerente de la firma Seguridad Informática Frontech, otro riesgo es que ¨el trabajador puede acceder desde su computador a archivos maliciosos enviados por correo electrónico o redes sociales, los malware roban todo tipo de información, como las contraseñas, tanto del empleado como del empleador.¨ También es de considerar que en la mayoría de casos, los servicios de internet que no son lo suficientemente robustos para lidiar con las exigencias de las redes laborales, que tampoco están aseguradas. Por eso el colaborador debe garantizar que la conexión a internet se haga directamente al router de su casa y no a través de una red wifi desconocida o de redes públicas ¨ los usuarios no saben que los routers deben actualizarse no solo

para dificultar el acceso a los delincuentes, también para garantizar mayor rendimiento afirma el experto Ramírez.

David Pereira, experto en Ciberseguridad y CEO de la firma SecPro, señala que la VPN no es suficiente, ¨no basta con eso, hay que colocar otros mecanismos de seguridad adicionales; por ejemplo, herramientas de privacidad, de borrado seguro y de autentificación para mejorar la conexión¨ (El Tiempo, 2020). El atacante también puede bloquear la conexión para evitar que el usuario la use o crea un punto de acceso falso, que duplica el nombre de la red inalámbrica y desactiva la original. Así logra que los dispositivos se conecten a la nueva señal mientras tiene acceso a todo el trafico generado, totalmente visible si no está encriptado. Pereira expresa que ¨la protección de la red equivale a que el usuario tenga un equipo Wips (sistema de prevención de intrusión inalámbrica). Sin embargo, puede que lo tenga en la oficina, pero no en la casa, lo que hace a ese usuario más vulnerable¨. (Yeshica, 2.020).

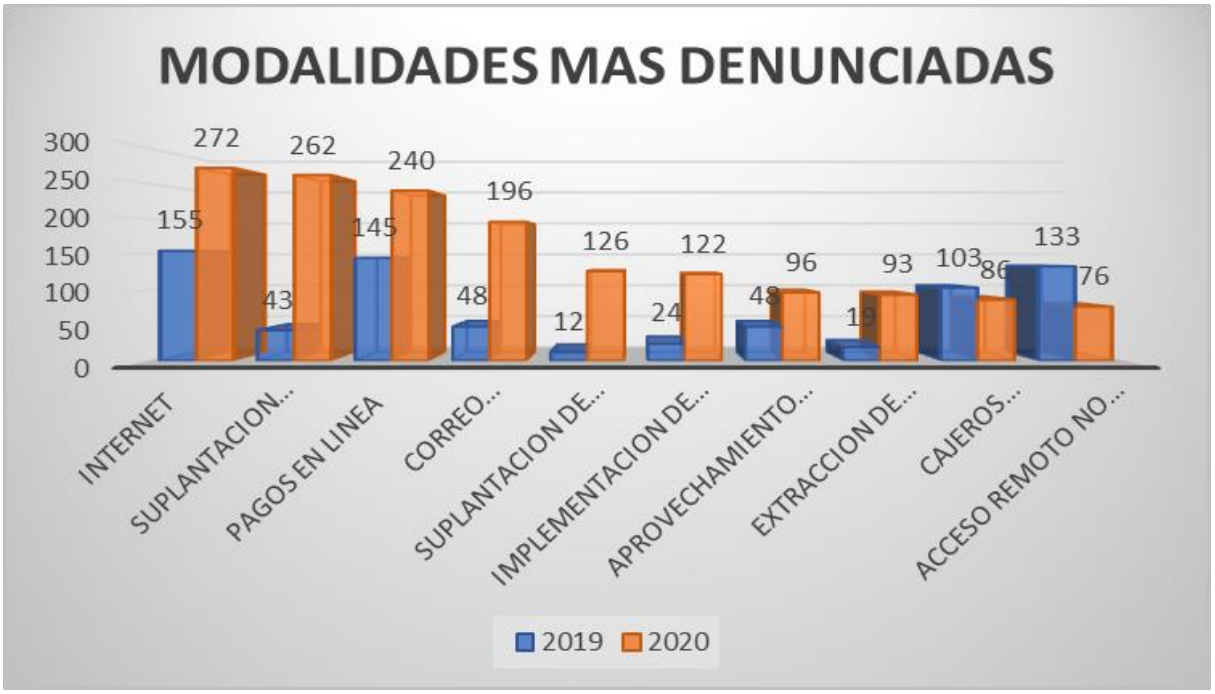
A continuación, la idea es establecer una mirada basada en números donde el objetivo es verificar cual fue el nivel de denuncias durante los dos períodos de tiempo estudiados en las 20 localidades de Bogotá, logrando establecer de la más a la menos afectada, así mismo poder aterrizar las variables enunciadas en el ensayo primordialmente las modalidades, es de recordar que la muestra objeto de estudio, permitirá realizar un comparativo para los períodos del 12 de marzo al 12 de mayo de los años 2.019 y 2.020, analizarlo y evaluarlo para tener cifras concretas frente a las 10 variables objeto de estudio.

Cuadro No. 1 Denuncias por modalidades en las 20 localidades de Bogotá

NUMERO DE LOCALIDADES Y PUESTO POR INCREMENTO DE DENUNCIAS					
LOCALIDAD	**PUESTO POR DENUNCIA**	**PERÍODO 2.019**	**PERÍODO 2.020**	**INCREMENTO**	**POBLACIÓN**
18	RAFAEL URIBE	23	64	178%	341.886
19	CIUDAD BOLIVAR	26	68	162%	776.351
11	SUBA	130	333	156%	1.381.597
10	ENGATIVA	97	236	143%	892.169
5	USME	15	35	133%	348.332
1	USAQUEN	115	265	130%	476.931
9	FONTIBON	57	116	104%	444.951
8	KENEDDY	121	227	88%	1.273.390
13	TEUSAQUILLO	61	109	79%	139.369
4	SAN CRISTOBAL	26	45	73%	387.560
7	BOSA	39	61	56%	799.660
6	TUNJUELITO	18	27	50%	183.067
12	BARRIOS UNIDOS	43	62	44%	276.453
16	PUENTE ARANDA	57	75	32%	211.802
15	ANTONIO NARIÑO	23	30	30%	108.976
14	MARTIRES	21	27	29%	92.234
3	SANTAFE	37	46	24%	91.111
2	CHAPINERO	90	111	23%	125.294
17	CANDELARIA	12	8	-33%	21.830
20	SUMAPAZ	0	0	-	7.838
	CUADRANTE X ASIGNAR	13	70		N. A
	VACIAS	1	1		N. A
	TOTAL	1.025	2.016		8.380.801

Fuente: Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional SIEDCO – Policía Metropolitana de Bogotá.

Figura No.2 Modalidades más denunciadas



Fuente: Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional –SIEDCO – Policía Metropolitana de Bogotá.

Al analizar la Figura No. 2 Modalidades más denunciadas y realizar el comparativo de los dos meses tomados como muestra académica (12 de marzo al 12 de mayo de los años 2.019 y 2.020) se toman las más denunciadas, pero el estudio evidenció que los delitos informáticos aumentaron (evolucionaron) un 97% y la dinámica reflejada en las diferentes modalidades de cibercrimen paso de 33 en el periodo 2.019 a 41modalidades en el período 2.020 en la ciudad de Bogotá, con 991 denuncias de más en el año 2.020 reportadas en el Sistema Estadístico Delincuencial Contravencional y Operativo (SIEDCO) de la Policía Metropolitana de Bogotá, (ver variables de Modalidades de Cibercrimen períodos 2.019 y 2.020 completas en los anexos A y B).

Cuadro No.2 Denuncias por infracciones a la Ley Penal, consagrada en la Ley 1273 del 2.009.

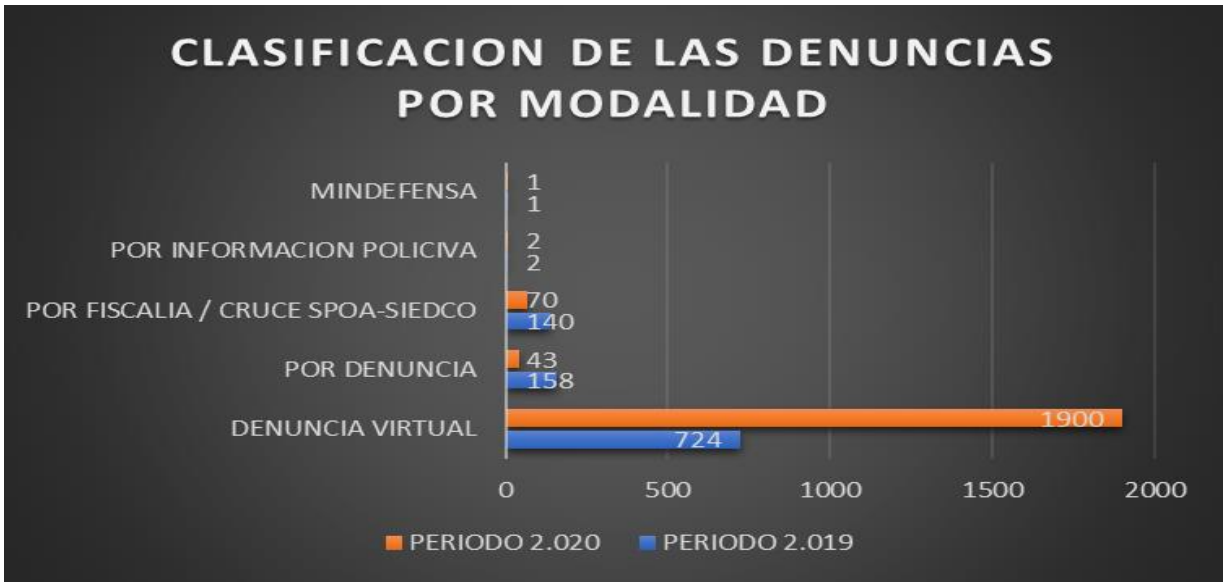
DENUNCIAS POR INFRACCIONES A LA LEY 1273 DEL AÑO 2.009			
PUESTO	**TIPO PENAL**	**PERIODO 2.019**	**PERIODO 2.020**
1	Artículo 269I. hurto por medios informáticos y semejantes.	466	670
2	Artículo 269A. acceso abusivo a un sistema informático.	159	433
3	Artículo 269F. violación de datos personales.	183	314
4	Artículo 269G. suplantación de sitios web para capturar datos personales.	51	308
5	Artículo 269J. transferencia no consentida de activos.	90	120
6	Artículo 269C. interceptación de datos informáticos.	27	92
7	Artículo 269E. uso de software malicioso.	39	47
8	Artículo 269D. daño informático.	7	27
9	Artículo 269B. obstaculización ilegítima de sistema informático o red de telecomunicación.	3	5
	TOTAL	1.025	2.016

Fuente: Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional –SIEDCO – MEBOG.

El Cuadro No. 1 denuncias por modalidades en las 20 localidades de Bogotá, representa la muestra tomada en espacio para este ensayo, donde se muestran las 20 localidades que corresponden a la División Político Administrativa de Bogotá, se evidencia que todas las localidades tuvieron un alza en las modalidades denunciadas a excepción de la localidad de Candelaria así mismo 9 localidades muestran tendencias por encima del 100% de aumento en sus denuncias. El cuadro No. 2 denuncias por infracciones a la ley penal, consagrada en la Ley 1273 del 2.009 realiza el comparativo donde se observa que para el período 2.019 se produjeron 1.025 modalidades denunciadas que comparándolas con las 2.016 modalidades denunciadas en el

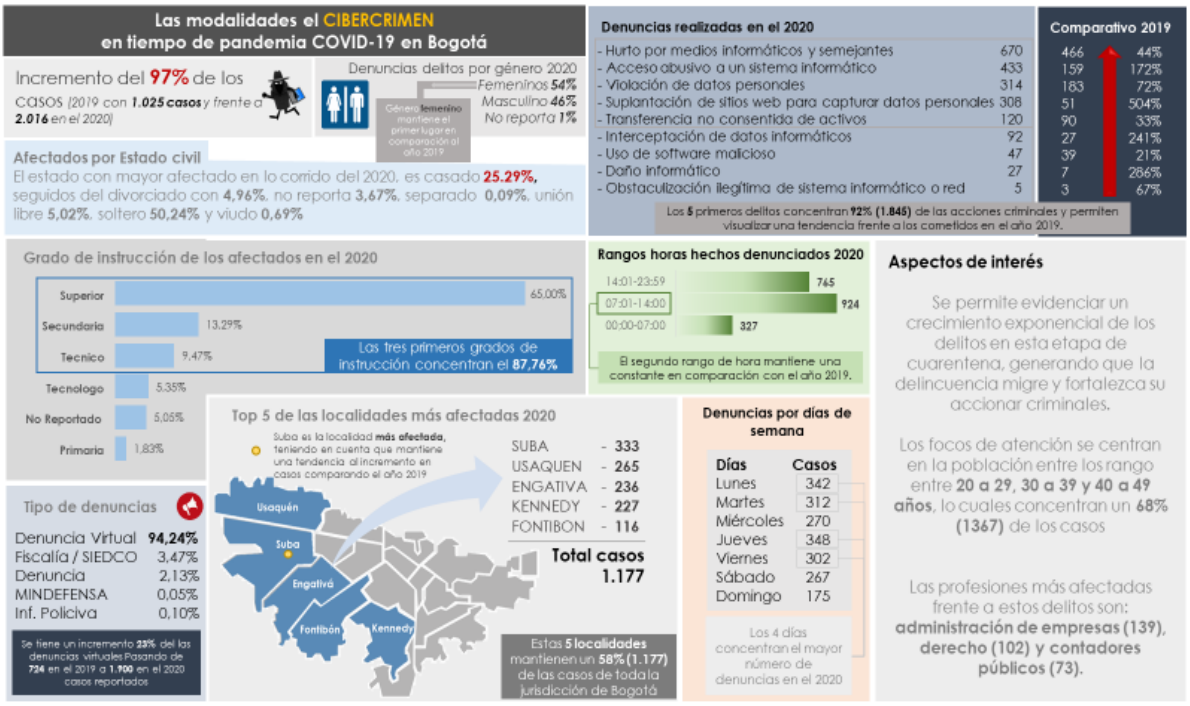
período 2.020 se refleja para este periodo de pandemia COVID-19 en Bogotá un aumento en las modalidades del 97%.

Figura No.3 Clasificación de las denuncias por modalidad.



La Figura No. 3 Clasificación de las denuncias por modalidad evidencia la manera en que la ciudadanía interpuso la denuncia, del total de las 2.016 denuncias instauradas por modalidades en tiempos de pandemia COVID-19 en Bogotá (periodo 2.020) se puede observar que 1.900 se realizaron de manera virtual (94,24%), por cruce de Sistemas entre Instituciones (Fiscalía-SPOA – Policía SIEDCO) 70 denuncias (3,47%), por denuncia interpuesta personalizada 43 (2,13%), por información Policiva 2 denuncias (0,09%) y 01 denuncia reportada por el Ministerio de la Defensa Nacional de Colombia (0,04%).

Infografía No. 1 Dinámica de las 10 variables, objeto de estudio.



Fuente: infografía elaborada con datos aportados por el Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Metropolitana de Bogotá.

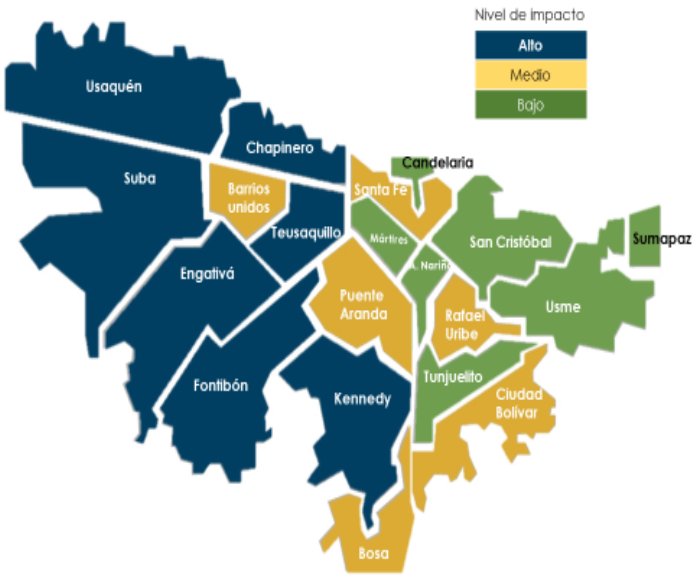
La infografía No.1 dinámica de las 10 variables objeto de estudio, refleja la evolución o dinámica presentada por las modalidades de Cibercrimen durante el período evaluado, mostrando el incremento en cada una de las variables analizadas en tiempos de pandemia COVID-19 en la Capital de la Republica.

De allí se desprende el aumento del 97% de modalidades de cibercrimen al encontrar después del comparativo que en el periodo 2.019 las modalidades denunciadas fueron 1.025, entre tanto para el periodo 2.020 el aumento paso a 2.016 modalidades denunciadas.

Mapa No.1 Georreferenciación de las modalidades de Cibercrimen.

Georreferenciación de las modalidades del CIBERCRIMEN en tiempo de pandemia COVID-19 en Bogotá

No.	Localidad	2019	2020	Población
1	Usaquén	115	265	476.931
2	Chapinero	90	111	125.294
3	Santafé	37	46	91.111
4	San Cristóbal	26	45	387.560
5	Usme	15	35	348.332
6	Tunjuelito	18	27	183.067
7	Bosa	39	61	799.660
8	Kennedy	121	227	1.273.390
9	Fontibón	57	116	444.951
10	Engativá	97	236	892.169
11	Suba	130	333	1.381.597
12	Barrios Unidos	43	62	276.453
13	Teusaquillo	61	109	139.369
14	Mártires	21	27	92.234
15	Antonio Nariño	23	30	108.976
16	Puente Aranda	57	75	211.802
17	Candelaria	12	8	21.830
18	Rafael Uribe	23	64	341.886
19	Ciudad Bolivar	26	68	776.351
20	Sumapaz	0	0	7.838



Fuente: Mapa No. 1 elaborado con datos aportados por el Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Metropolitana de Bogotá.

En el mapa No. 1 Georreferenciación de las modalidades denunciadas se demuestra que en el período 2.019 sumaron un total de 1.025 denuncias y que en el período 2.020 sumaron un total de 2.016 denuncias, en las 20 localidades de Bogotá, (con su respectiva población), evidenciándose un aumento en tiempos de pandemia COVID-19 del 97% y otorgando un color azul, (7 localidades que sobrepasan alzas de más del 100%) café (6 localidades que reportan alzas de más del 50% y verde (7 localidades con baja afectación en comparación a las primeras, más sin embargo reportan alzas entre el 23 y el 44%). De resaltar las localidades de La Candelaria que tuvo una disminución del -33% y la localidad de Sumapaz que no reporto denuncias para ningún período evaluado.

Análisis demás Variables en Tiempos de Pandemia COVID-19

En tiempos de Pandemia y durante el período señalado se registraron en promedio 33,6 denuncias diarias, los días de la semana por mayor grado de denuncias interpuestas son el jueves (348) 17,26%, lunes (342) 16,96%, martes (312) 15,47%, viernes (302) 14,98%, miércoles (270)13,34%, sábado (267) 13,24% y el día que menos denuncias se realizan es el Domingo (175) 8,68%.

Se realizaron tres grupos de horas en tiempos de pandemia a seguir: 0:00 y 6:59 horas se registraron 327 denuncias, (16,22%) el de mayor afectación oscilo entre las 07:00 y las 14:00 horas con 924 denuncias (45,83%) y entre las 14:01 y 23:59 765 denuncias (37,94%).

En tiempo de pandemia el género femenino fue el más afectado instaurando un total de 1.073 denuncias (53,22%) mientras que el Género Masculino denuncio 924 (45,83%), no reportan genero un total de 19 personas con igual número de denuncias (0,94%).

En rangos de edad la generación que esta entre los 30 y 39 años han sido los más afectados por delitos informáticos con 613 denuncias (30,40%), le sigue la generación entre los 20 y 29 años con 517 denuncias (25,64%), la generación entre los 40 y 49 años es el tercer renglón más afectado con 406 denuncias (20,13%), entre los 50 y 59 años 222 denuncias (11,01%), entre los 60 y 69 años 106 denuncias (5,25%), la generación entre los 11 y 19 años 58 denuncias (2,38%), entre los 70 y 79 años, 38 denuncias (1,88%) y entre los 80 y 94 años se formularon 08 denuncias (0,39%), no reportan edad 48 personas (2,38%).

Por grado de escolaridad se concluye que el 65% de los denunciantes tiene escolaridad Superior (1.310), el 13,29% Secundaria (268), el 9,47% es Técnico (191), el 5,35% es Tecnólogo (108) y el 1,83% Primaria (37), el 5,05 % no reporto escolaridad (102 denunciantes).

Por estado civil los solteros instauraron 1.013 denuncias (50,24%), los casados 510 denuncias (25,29%), unión libre 303 denuncias (15,02%), divorciados 100 denuncias (4,96%), viudos 14 denuncias (0,69%) y separados 02 denuncias (0,09%), no reportan estado civil 74 denunciantes (3,67%).

En tiempos de pandemia el 4,80% (817 denuncias) corresponde a las 20 profesiones más afectadas, las tres primeras de este grupo son Administración de Empresas con 139 denuncias, Derecho con 102 denuncias y Contaduría Pública con 73; las restantes profesiones (396) reportan el 95,19%. (1.205 denuncias). Es pertinente aclarar que para el período 2.019 se registraron en total 261 profesiones afectadas y para el período 2.020 un total de 416 profesiones.

Los denunciantes expresaron que las clases de sitio más afectadas son la red virtual (582), apartamento (368), casas de habitación (225), apartamento en conjunto cerrado (135), casa en conjunto cerrado (105), vía pública (85) y bancos (69). Estos 07 sitios (10%) recopilan 1.569 denuncias, (77,82%) los restantes 62 sitios sumaron 447 denuncias (90%).

Desarrollo Tecnológico Institucional en Materia de Ciberseguridad

Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, en el 2011, el Gobierno Nacional expidió el Documento CONPES 3701 Lineamiento de política para Ciberseguridad y Ciberdefensa. (Departamento Nacional de Planeacion, 2.011), cuya función principal en Colombia es ser la hoja de ruta en materia económica y social (Consejo Nacional de Política Económica y Social Conpes).

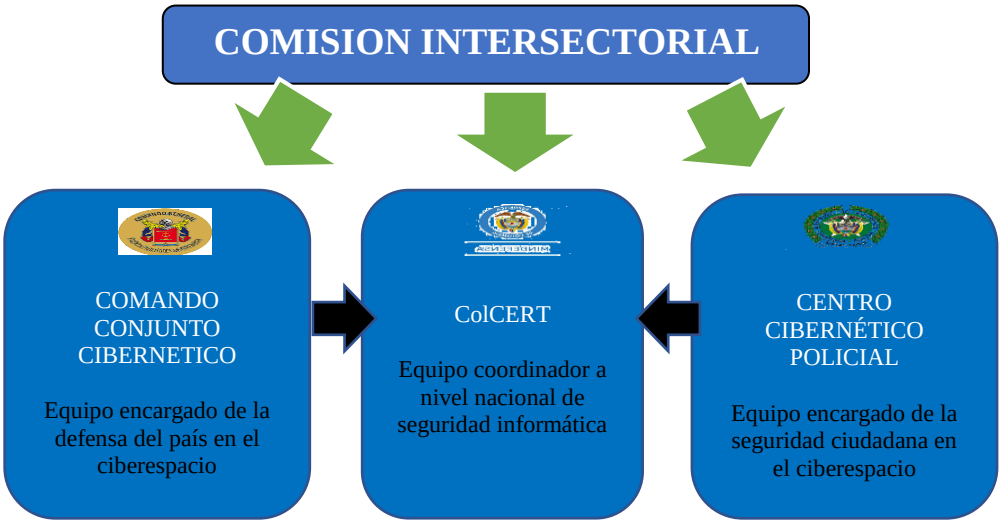
El principal logro alcanzado por la política de Ciberseguridad y Ciberdefensa, fue el fortalecimiento de la Institucionalidad en el tema. Lo anterior, fue posible por medio de la creación de nuevas instancias tales como el grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y las unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

En 2013, a través del Ministerio de Relaciones Exteriores, el país solicitó formalmente la adhesión a la Convención de Europa sobre cibercriminalidad, también conocido como Convenio de Budapest. Este Convenio establece los principios de un acuerdo internacional sobre seguridad cibernética y la sanción de delitos cibernéticos. En el mismo año, se estableció un convenio

multilateral con el Foro Económico Mundial, para identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, cada vez mayor, entre personas, procesos y objetos. A través del Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), se ha logrado trabajar con varios equipos de respuesta ante incidencias de seguridad (CSIRT) en la región. Colombia es parte de una red de alerta que proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernética, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente.

En este mismo frente, el país ha suscrito acuerdos con organizaciones internacionales como el Antiphishing Working Group. Lo anterior, con el fin de acceder a recursos y programas específicos en ciberseguridad y ciberdefensa, y hacer parte de esta coalición con empresas de la industria, autoridades legales y entidades de gobierno, que colaboran en función de contar con mejores mecanismos de alarma y respuesta frente a ataques. (Departamento Nacional de Planeacion, 2.016).

Figura No.4: Lineamientos de Política para Ciberseguridad y Ciberdefensa, establecidos en el CONPES 3701 del 2.011.



Fuente: Ministerio de Defensa Nacional

Con base al CONPES 3701 nació el CONPES 3854 el 11 de abril del 2016, la política nacional de seguridad digital, el cual cambia el enfoque tradicional al incluir la gestión de hacer bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas, principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Para lograrlo, se implementaron acciones en torno a cinco ejes de trabajo. (Dnp.gov.co, 2016)

Por su parte, la Policía Nacional, a través del Centro Cibernético Policial, sostiene mecanismos de cooperación con homólogos en otros países y agencias de ley a nivel mundial, tales como: la Organización Internacional de Policía Criminal (INTERPOL), la Oficina Federal de Investigaciones de los Estados Unidos (FBI), la Administración para el Control de Drogas de los Estados Unidos (DEA), el Centro Europeo contra el cibercrimen (EC3), la Comunidad de Policías de América (AMERIPOL), la Agencia Internacional de Cooperación Coreana (KOICA), la Agencia Nacional contra el crimen del Reino Unido (NCA), el Grupo de Trabajo Americano de delitos Tecnológicos del INTERPOL (GLDTA) y el Programa de Asistencia Antiterrorismo de Estados Unidos (ATA). Esto, con el fin de combatir el cibercrimen desde diferentes flancos. Otro aspecto a resaltar, es que Colombia cuenta con ocho CSIRT con membresía en el Foro de equipos de seguridad y respuesta de incidentes, llamado FIRST14 por sus siglas en inglés. Esto les permite responder de manera más eficaz a incidentes de seguridad, al tener acceso a información acerca de

las mejores prácticas, ser invitados a eventos y a capacitaciones y cursos relacionados con la seguridad digital.

Actualmente está en vigencia el CONPES 3975 del 2.019, (Mintic.gov.co, 2.019) allí se presenta una breve síntesis de la Política de Transformación Digital e Inteligencia Artificial (IA), esta nueva estrategia pretende enfrentar los requerimientos que ha impuesto la OCDE (Organización para la Cooperación y el Desarrollo Económico). Así las cosas, se busca también, disminuir las brechas de incorporación de tecnológicas digitales en el sector público y privado. En resumen, este CONPES 3975 prevé líneas de acción con diversos propósitos, dentro de los cuales resaltan los siguientes: 1. Disminuir barreras relacionadas con la falta de cultura y el desconocimiento. 2. Desarrollar ajustes normativos e institucionales para favorecer la adopción de la transformación digital en componentes clave. 3. Mejorar el desempeño de la política de gobierno digital y 4. Generar las condiciones habilitantes para impulsar el desarrollo de la Inteligencia Artificial (IA).

Actualmente y de acuerdo a conversación telefónica con el Teniente Coronel Luis Fernando Atuesta Zarate Jefe del Centro Cibernético Policial, Bogotá cuenta con un aproximado de 160 investigadores en la DIJIN, que en conjunto con un aproximado de 70 investigadores del Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, cada entidad con su respectivo laboratorio de informática forense y bajo el liderazgo de 35 fiscales que están actualmente comprometidos en luchar contra este flagelo que en época de pandemia COVID-19 han visto sus capacidades limitadas, producto del aislamiento, el oficial reconoce que es todo el andamiaje investigativo el que está limitado ¨no se están realizando audiencias, no están recibiendo

capturados ¨todo esto genera que el trabajo se represe, igualmente en limitamientos en temas de ciber, que hace referencia a solicitudes a otras empresas, (redes sociales, todo lo que tiene que ver con Facebook, Google, Twitter, WhatsApp), siempre van a ser indispensables realizarlas y es pertinente dejar claro que las políticas de uso de estas empresas antes mencionadas son diferentes a nuestra legislación penal, (lo que en nuestro país es delito pueda que en otro donde se está consultando no sea delito), esto finalmente limita a que las respuestas a las solicitudes tenga más que ver con las políticas mismas de las redes sociales. Finalmente, al pedir una calificación porcentual de esta limitación operativa, responde que sería muy subjetivo ¨quizás un 30% pero es decir cualquier cosa¨.

Lo expuesto por el Coronel Atuesta cobre vigencia cuando se escuchan las limitaciones del órgano rector de investigación, la Fiscalía General de la Nación y encontrando que por pandemia no se ha podido acceder a información confidencial, por tomar un ejemplo de actividad investigativa ¨Búsqueda selectiva en base de datos¨ herramienta indispensable para un funcionario que cumpla labores de policía judicial, porque permite por ejemplo acceder a información de los números celulares a nombre de una persona y tener registro de las llamadas realizadas y recibidas, todo lo anterior como consecuencia de las medidas que se han adoptado en la rama judicial ya que por causa de la reducción de la actividad de los juzgados y la realización solo de audiencias urgentes o con preso, estas audiencias no se han podido llevar a cabo, ya que estas deben ser legalizadas dentro de las 36 horas siguientes a su recolección. El propio fiscal general Francisco Barbosa reconoció que esa herramienta se ha visto afectada y que se están buscando alternativas para normalizar esas labores de policía judicial. “Tenemos algunas limitaciones desde el punto de vista de que no se han autorizado todas las audiencias por parte del Consejo Superior de la

Judicatura en este tiempo. Y eso es uno de los temas que estamos trabajando", dijo el Fiscal General al señalar que esta semana espera que el tema quede superado "para avanzar en diferentes investigaciones que son prioritarias para la Fiscalía General". (El Tiempo, 2.020).

Así las cosas y con base en las respuestas anteriores, se confirma las limitaciones que producto del confinamiento tienen los investigadores y la extensa oportunidad que tienen los ciberdelincuentes para arreciar sus ataques a las diferentes personas que hagan uso de sus equipos o dispositivos, ya que allí los cibercriminales encuentran una ventana de oportunidades producto del desconocimiento para adoptar medidas de seguridad con los equipos o valerse estos delincuentes de la ingenuidad propia en temas de tecnología o seguridad de la información que tiene el común de los ciudadanos. Por fortuna se cuenta con talento humano especializado, capacitado y formado en la investigación de los delitos informáticos que con las capacidades que brindan las instituciones soportan el desarrollo de estas investigaciones que en tiempos de pandemia COVID-19, indiscutiblemente se han aumentado, así mismo la Fiscalía a robustecido su presupuesto a partir de los últimos 5 años. (La República, 2.015). Por solo simplificar el presupuesto comparado a los años 2.019 y 2.020 este paso en el sector defensa y policía de 33.522 a 35.797 billones con un crecimiento del 6,8%, mientras que la Fiscalía General de la Nación creció en presupuesto un 3% al pasar de 4 billones en el 2.019 a 4,12 billones en el 2.020. (Fiscalia.gov.co, 2.020).

Conclusiones

El Desarrollo tecnológico con que cuenta la ciudad de Bogotá se deriva de la madurez tecnológica que a través de los años ha crecido vertiginosamente, hoy existe una Comisión Intersectorial que bajo el ente coordinador (colCERT), el Comando Conjunto Cibernético (ciberdefensa) y el Centro Cibernético Policial (Seguridad Ciudadana en el Ciberespacio), fueron la punta de lanza para que en el año 2.016 se formalizara la Política Nacional de Seguridad Digital, hoy después de más 07 años de espera y adportas del 01 de Julio del año en curso iniciara el Convenio 24/7 Budapest C-4, que busca intercambiar información y evidencia en tiempo real entre sus países miembros, reduciendo con esto meses y años de trámites burocráticos para obtener una respuesta.

Institucionalmente, se destacan las capacidades humanas y tecnológicas desde el ámbito Investigativo en la Ciudad Capital, que cuenta con 35 Fiscales Especializados que lideran los Investigadores del CTI (70) y DIJIN (160) aproximadamente, además de 02 Laboratorios de Informática Forense, cada Institución cuenta con uno que contribuye de manera transversal en la Investigación Forense y además de tener las dos Instituciones su personal altamente capacitado y que es referente a nivel mundial, cada entidad creció en el presupuesto general asignado por la Nación, mientras el Sector Defensa y Policía creció un 6.8% , la Fiscalía creció 3,0% en el 2.020.

Los tiempos de Pandemia no solo han afectado a la ciudadanía en general producto del confinamiento o aislamiento obligatorio, estas medidas también han conllevado a que la sinergia institucional se vea limitada (audiencias que no se realizan producto de las medidas adoptadas por la judicatura, capturados a los que los jueces no legalizan su captura, pruebas que necesitan de la

legalización en menos de 36 horas que no se pueden llevar a cabo), también hay limitantes en oficios que en temas de Ciber, deben ser enviados a otras empresas, especialmente redes sociales.

Finalmente, al realizar el comparativo de los dos períodos tomados como muestra académica (12 de marzo al 12 de mayo de los años 2.019 y 2.020) se observa que los delitos informáticos aumentaron un **97%** y la dinámica reflejada en las diferentes modalidades de cibercrimen paso de 33 a 41 en el tiempo de Pandemia Covid-19 en la ciudad de Bogotá, con 991 denuncias de más reportadas en el Sistema Estadístico Delincuencial Contravencional y Operativo (SIEDCO) de la Policía Metropolitana de Bogotá, (ver Variables completas en los anexos A y B).

Todas las localidades de Bogotá registran aumentos desbordados en las denuncias empezando por un primer grupo que sobrepasa más del 100% de afectación e incremento estas Localidades en su orden de alza en denuncias son: Rafael Uribe +41 (178,26%), Ciudad Bolívar +42 (161,53%), Suba +203 (156,15%), Engativa +139 (143,29%), Usme +20 (133,33%), Usaquén +150 (130,43%) y Fontibón +59 (103,50%), se resalta la excepción de esta evaluación de localidades como La Candelaria (-33%) y Sumapaz .

En tiempos de Pandemia y durante el periodo señalado se registraron en promedio 33,6 denuncias diarias, del total de las 2.016 denuncias instauradas por delitos informáticos se pudo evidenciar que 1.900 se realizaron virtualmente (94,24%), por cruce de Fiscalía – SPOA- SIEDCO 70 denuncias (3,47%), por denuncia presencial 43 (2,13%), por información policiva 02 denuncias (0,09%) y 01 denuncia instaurada por Mindefensa (0,04%).

Recomendaciones

Sheila Berta, especialista en ciberseguridad y directora de investigación en Dreamlab Technologies, recomienda usar el sentido común, ante todo: no instalar cosas en la computadora o smartphone de las cuales el origen no es confiable. Controlar los permisos de las aplicaciones que se usan, no autorizar permiso de usar la cámara o el micrófono a una app que claramente no lo necesita. El hacer click en todo “si, si, ok, ok, acepto” sin mirar y entrar a cualquier link o descargar y ejecutar todo es el error de la mayoría de la gente. Usar el sentido común y tener una paranoia sana evita caer en todos los ataques masivos o más comunes.

Respecto de las VPN, la experta opina que es muy recomendable utilizarlas. Tener configurada una VPN de confianza en la computadora y el teléfono nos añade una capa más de protección a nuestras comunicaciones por internet. Es una medida muy recomendable de aplicar en todo momento, e indispensable si solemos conectarnos a wifi abiertas o desconocidas.¨

Martín Oettel, consultor en ciberseguridad y fundador de pasando data afirma ¨para evitar ser víctima debemos verificar que nuestras ¨comunicaciones estén encriptadas: usar siempre HTTPS al navegar por internet y en apps de comunicación, comprobar que la misma use cifrado punto a punto como WhatsApp/Signal o Cliente-Servidor como en el caso de Telegram. Hay que evitar usar medios de comunicación que no encripten como es SMS.

Margarita Abella Hernández, especialista en Educación a Usuarios en Seguridad Digital de Google opina ¨ Fomentamos entre los usuarios el uso de la autenticación de dos factores, un proceso de identificación que combina: algo que sabes (tu contraseña) y algo que tienes (clave o

código de seguridad)" Entonces, incluso si un hacker tiene tu contraseña, no podrá acceder a tu cuenta sin la clave de seguridad o el código y viceversa. Otra de las cosas importantes es denunciar los correos. Gmail identifica el correo sospechoso o que podría ser de suplantación de identidad y lo coloca en Spam o le muestra al usuario una advertencia. Si un correo no se ha marcado correctamente, es importante que los usuarios los denuncien por suplantación de identidad o los marquen como spam ya que con esta acción Google recibe una copia de este mail para analizarla y proteger a sus usuarios.

Andrea Fernández, gerente general para América del Sur de Kaspersky afirma que, para detectar cualquier actividad sospechosa, hay que contar con una solución de seguridad de calidad para monitorear archivos críticos del sistema en un nivel bajo para atrapar al malware que trate de modificar las estructuras del disco duro. Es posible encontrar nuevos rootkits, aún desconocidos, sólo comparando la actividad de la computadora como se ve al nivel del sistema operativo con resultados de monitoreo a niveles bajos, es crucial que la solución tenga una protección propia suficiente, para que el malware no pueda desactivarla.

Referencias

Avast. (19 de mayo de 2.020). Que es el Phishing? detecte y evite los correos electronicos. Recuperado de Avast: https://www.avast.com/es-es/c-phishing

Caivirtual.gov.co. (31 de Mayo de 2.020). Centro Cibernetico Policial. Recuperado de https://caivirtual.policia.gov.co/

Centro Cibernetico Policial. (Marzo de 2.017). Amenazas del Cibercrimen en Colombia 2.016 - 2.017. Recuperado de caivirtual.policia.gov.co: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017_1.pdf

Departamento Nacional de Planeacion. (14 de Julio de 2.011). Lineamientos de Politica para Ciberseguridad y Ciberdefensa. Recuperado de Documento CONPES 3701: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeacion. (11 de Abril de 2.016). Recuperado de CONPES 3854: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Desiree, J. (02 de Abril de 2.020). Zoom: alertan por graves fallas de seguridad en la popular aplicacion de videollamadas. Recuperado de infobae: https://www.infobae.com/america/tecno/2020/04/02/zoom-alertan-por-graves-fallas-de-seguridad-en-la-popular-aplicacion-de-videollamadas/

Directivos y Empresas. (28 de Abril de 2.020). Directivos y empresas. Recuperado de Ciberataques, Covid-19 y teletrabajo: https://www.directivosyempresas.com/internet/tecnologia/ciberseguridad-ciberataques-covid-19-y-teletrabajo/

Documento CONPES 3854. (11 de Abril de 2.016). Politica Nacional de Seguridad Digital en Colombia. Recuperado de colaboracion.dnp.gov.co: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

El Tiempo. (7 de Mayo de 2.020). Por pandemia, Fiscalía no ha podido acceder a información confidencial. Recuperado de https://www.eltiempo.com/justicia/delitos/por-coronavirus-fiscalia-no-ha-podido-acceder-a-informacion-confidencial-492842

El Heraldo. (15 de Marzo de 2.020). El teletrabajo, una alternativa laboral en medio del coronavirus. Recuperado de https://www.elheraldo.co/economia/el-teletrabajo-una-alternativa-laboral-en-medio-del-coronavirus-709135

El Tiempo. (17 de Mayo de 2.020). Riesgos del teletrabajo ¿No hay lugar como el hogar? Recuperado de https://www.eltiempo.com/colombia/medellin/riesgos-del-teletrabajo-no-hay-lugar-como-el-hogar-496406

Fiscalia.gov.co. (05 de Marzo de 2.018). ¿Qué se debe tener en cuenta para ser un buen usuario de internet y no ser víctima de los ciberdelincuentes? Recuperado de https://www.fiscalia.gov.co/colombia/noticias/que-se-debe-tener-en-cuenta-para-ser-un-buen-usuario-de-internet-y-no-ser-victima-de-los-ciberdelincuentes/

Fiscalia.gov.co. (8 de Junio de 2.020). Presupuesto general asigando. Recuperado de https://www.fiscalia.gov.co/colombia/la-entidad/presupuesto-general-asignado/

Incibe. (19 de septiembre de 2019). Ingenieria Social: tecnicas utilizadas por los ciberdelincuentes y como protegerse. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

Infobae. (04 de Abril de 2.020). Zoom: miles de videollamadas privadas quedaron expuestas en la web. Recuperado de Infobae: https://www.infobae.com/america/tecno/2020/04/06/zoom-miles-de-videollamadas-privadas-quedaron-expuestas-en-la-web/

Infolaft. (s.f.). Lo que debe saber sobre el cibercrimen en Colombia - Infolaft. Recuperado de https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

Instituto Nacional de CiberSeguridad. (14 de Noviembre de 2.019). E-skimming, qué es y cómo proteger tu tienda contra esta técnica maliciosa. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa.

Kaspersky. (2.020). ¿Qué es el ransomware? Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

La República. (13 de Abril de 2.015). Fiscalía, entidad que más aumento pide para el presupuesto del próximo año. Recuperado de https://www.larepublica.co/economia/fiscalia-entidad-que-mas-aumento-pide-para-el-presupuesto-del-proximo-ano-2242921

Mintic.gov.co. (16 de Julio de 2.008). Ley 1221 del 2.008 Min-TIC. Recuperado de https://www.mintic.gov.co/portal/604/articles-3703_documento.pdf

Mintic.gov.co. (13 de Noviembre de 2.019). CONPES-de-transformacion-digital-promovera-la-competitividad-del-pais-y-la-eficiencia-del-sector-publico. Recuperado de https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf

Ona Systems. (25 de marzo de 2020). *El teletrabajo puede abrir puertas a ciberataques - Ona Systems*. Recuperado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-teletrabajo-puede-abrir-puertas-a-ciberataques-477240: https://www.onasystems.net/el-teletrabajo-puede-abrir-puertas-a-ciberataques/

Reporte Digital. (19 de Julio de 2.019). Vishing: ¿Cómo reaccionar y cómo prevenirlo? Recuperado de https://reportedigital.com/seguridad/vishing/

Revista Semana. (31 de Mayo de 2.020). El otro virus: 5,4 millones de personas perdieron el empleo en abril. Recuperado de https://www.semana.com/nacion/articulo/coronavirus-en-colombia-54-millones-de-personas-perdieron-el-trabajo-en-abril/675140

Sebastian, P. (25 de junio de 2018). Se podría pagar cárcel por ocho años por delitos cibernéticos y cuantiosas multas. Recuperado de Asuntos legales: https://www.asuntoslegales.com.co/actualidad/carcel-por-ocho-anos-por-delitos-ciberneticos-2742015

Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. (30 de Marzo de 2020). Decreto 087 de 2020 Alcaldía Mayor de Bogotá, D.C. Recuperado de http://www.bogotaturismo.gov.co/sites/default/files/decreto_distrital_87_del_16_de_marzo_de_2020.pdf

Secretaria.gov.co. (01 de Mayo de 2.019). El Teletrabajo, una práctica Laboral que avanza en Bogotá. Recuperado de Alcaldia Mayor de Bogota: https://secretariageneral.gov.co/noticias/teletrabajo-practica-laboral-avanza-bogota

Secretariasenado. (31 de Diciembre de 2.019). Ley 1273 del 2.009. Recuperado de secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Telecomunicaciones, c. (29 de octubre de 2.019). informe tendencias cibercrimen. Recuperado de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Teletrabajo.gov.co. (2.015). Conoce los resultados del primer estudio sobre freelancers en Colombia. Recuperado de https://teletrabajo.gov.co/622/w3-article-13459.html

El Tiempo. (19 de abril de 2020). novedades tecnologia. Recuperado de ciberestafas en tiempos de coronavirus ¿como no caer en ellas?: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/estafas-en-internet-han-aumentado-durante-la-pandemia-del-coronavirus-486284

El Tiempo. (30 de marzo de 2020). Policia advierte sobre paginas web usadas para estafar por covid 19. Recuperado de https://www.eltiempo.com/justicia/delitos/coronavirus-modalidades-de-estafa-a-traves-de-paginas-web-aprovechando-la-pandemia-478642

Yeshica, O. (25 de Marzo de 2.020). El teletrabajo puede abrir puertas a ciberataques. Recuperado de El Tiempo: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-teletrabajo-puede-abrir-puertas-a-ciberataques-477240

Yubal, F. M. (4 de Noviembre de 2.019). ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etcétera? Recuperado de https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera

Anexos

ANEXOS A. Modalidades denunciadas periodo 2.019

MODALIDADES DE CIBERCRIMEN DENUNCIADAS PERIODO 2.019		
NUMERO	**MODALIDAD**	**DENUNCIAS 1203-120519**
1	INTERNET	155
2	PAGOS EN LINEA	145
3	ACCESO REMOTO NO AUTORIZADO	133
4	CAJEROS AUTOMATICOS	103
5	TRANSACCIONES ELECTRONICAS (compra venta de productos por Internet)	70
6	APROVECHAMIENTO DE MALAS POLITICAS EN SEGURIDAD DE LA INFORMACION	48
7	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	48
8	SUPLANTACION DE SITIOS WEB	43
9	BANCA MOVIL	36
10	SUPLANTACION DE DOMINIO o URL – BLOG	30
11	MANIPULACION DE CODIGO FUENTE	28
12	IMPLEMENTACION DE SOFWARE MALICIOSO (MALWARE)	24
13	EXTRACCION DE DATOS O REGISTROS PERSONALES	19
14	DATAFONO	18
15	INGENIERIA SOCIAL	12
16	SECUESTRO DE INFORMACION	12
17	SPAM CON CODIGO MALICIOSO	12
18	SUPLANTACION DE IDENTIDAD POR CORREOS AJENOS	12
19	MODIFICACION DE DATOS O REGISTROS PERSONALES	10
20	AUDIORESPUESTA	9
21	DESARROLLO O PRODUCCION DE SOFTWARE MALICIOSO	9
22	INGRESO CODIGO MALICIOSO AL SOFTWARE TENGA UNA CONDUCTA DELICTIVA	7
23	COMERCIALIZACION Y DISTRIBUCION DE SOFTWARE O PROGRAMA MALICIOSO (VIRUS, MALWARE, RASOMWARE. SPYWARE)	6
24	EXPLOTACION DE VULNERABILIDADES (PHARMING)	6
25	HARDWARE, SKIMMING, KEYLOGGER	3
26	PROPAGACION DE GUSANOS INFORMATICOS	3
27	SENSOR DE ACTIVIDADES TECLADO O PANTALLA (KEYLOGGER)	3
28	ALTERACION DE CODIGO FUENTE (ATAQUE CSRF)	2
29	DAÑO FISICO EQUIPO O MEDIO DE TRANSMISION	2
30	SUPLANTACION DE SITIOS WEB	2
31	BORRADO DELIBERADO DE INFORMACION	1
32	CAPTURA DE LAS TRAMAS DE UNA RED DE COMPUTADORAS (SNIFER)	1
33	INTRODUZCA O EXTRAIGA DEL TERRITORIO NACIONAL SOFTWARE MALICIOSO	1
34	NO REPORTADA	4
35	VACIA	8
	TOTAL, DENUNCIAS	1.025

ANEXOS B. Modalidades denunciadas periodo 2.020

MODALIDADES CIBERCRIMINALES PERIODO 2.020		
NUMERO	**MODALIDAD**	**DENUNCIAS 1203-120520**
1	INTERNET	272
2	SUPLANTACION SITIOS WEB	262
3	PAGOS EN LINEA	240
4	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	196
5	SUPLANTACION DE IDENTIDAD POR CORREOS AJENOS	126
6	IMPLEMENTACION DE SOFTWARE MAICIOSO (MALWARE)	122
7	APROVECHAMIENTO DE MALAS POLITICAS EN SEGURIDAD DE LA INFORMACION	96
8	EXTRACCION DE DATOS O REGISTROS PERSONALES	93
9	CAJEROS AUTOMATICOS	86
10	ACCESO REMOTO NO AUTORIZADO	76
11	INGENIERIA SOCIAL	51
12	BANCA MOVIL	48
13	SUPLANTACION DE DOMINIO o URL-BLOG	48
14	TRANSACCIONES ELECTRONICAS (compra venta de productos por internet)	47
15	MANIPULACION DE CODIGO FUENTE *	33
16	SIMULACION DE APLICACIÓN MOVIL FAKE APP	33
17	MODIFICACION DE DATOS O REGISTROS PERSONALES	31
18	SPAM CON CODIGO MALICIOSO	19
19	AUDIRESPUESTA	18
20	EXPLOTACION DE VULNERABILIDADES	15
21	INGRESO CODIGO MALICIOSO AL SOFTWARE TENGA UNA CONDUCTA DELICITIVA	11

22	SECUESTRO DE INFORMACION	11
23	DESARROLLO O PRODUCCION DE SOFTWARE MALICIOSO	10
24	PROPAGACION DE GUSANOS INFORMATICOS *	9
25	SENSOR DE ACTIVIDADES TECLADO O PANTALLA (KEYLOGGER)	9
26	CAPTURA DE LAS TRAMAS DE UNA RED DE COMPUTADORAS	5
27	DAÑO FISICO EQUIPO O MEDIO DE TRANSMISION	5
28	DATAFONO	5
29	COMERCIALIZACION Y DISTRIBUCION DE SOFTWARE O PROGRAMA MALICIOSO (VIRUS, MALWARE, RASOMWARE, SPYWARE)	4
30	CRIPTOMONEDAS *	4
31	ALTERACION DE CODIGO FUENTE (ATAQUE CSRF)	3
32	ATAQUE A DNS *	3
33	INTRODUZCA O EXTRAIGA DEL TERRITORIO NACIONAL SOFTWARE MALICIOSO	3
34	HARDWARE, SKIMMING, KEYLOGGER	2
35	SUPLANTACION BLOG *	2
36	ATACANTE INTERNO *	1
37	ATAQUE A DOS O DDOS *	1
38	BORRADO DELIBERADO DE INFORMACION	1
39	CORREO ELECTRONICO SPAM SCAM *	1
40	FACTOR DE OPORTUNIDAD *	1
41	SUPLANTACION DE SITIOS WEB	1
42	NO REPORTADA	8
43	VACIAS	4
	TOTAL	2.016