CRECIMIENTO DEL CIBERFRAUDE EN COLOMBIA DURANTE LA PANDEMIA POR COVID-19

INCREASE OF CYBERFRAUD IN COLOMBIA DURING COVID-19 PANDEMIC

Ensayo presentado por:

ANA MARIA CADENA ALVARADO[1]

https://orcid.org/0000-0002-0155-4350

Tutor:

Cr. JAIRO ANDRÉS CÁCERES GARCÍA

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ESPECIALIZACION EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTA D.C.

2021

[1] Profesional bilingüe en el campo de la Criminalística, Investigación y Ciencias Forenses con experiencia en el área de la Investigación Judicial, Investigación de Fraudes, Seguridad Privada y Atención a Clientes. Universidad Militar Nueva Granada. Colombia.

Resumen

El siguiente ensayo se realizó con el fin de mostrar el aumento que han tenido los delitos informáticos en Colombia con ocasión de la pandemia por COVID-19, debido a la digitalización y virtualidad necesarios con el fin de evitar altas tasas de contagio en las distintas actividades de trabajo y estudio, al igual que tramites bancarios, médicos, comercio en general, entre otros.

La estadística e información recopilada y posteriormente analizada, asociada a la cantidad de denuncias registradas en la Fiscalía General de la Nación y el Centro Cibernético Policial durante el 2019, 2020 y el primer trimestre del 2021, permitió identificar que el uso necesario de los medios web para el desarrollo de las actividades cotidianas generó un impacto en el aumento de ciberdelitos, al ser un canal más expuesto y utilizado por la ciudadanía.

Se llegó a la conclusión, que entre 2019 y 2020 los delitos informáticos en Colombia aumentaron entre un 48% a 360%, y que el número de casos registrados para el primer trimestre del 2021, para los cinco delitos analizados, ya superó a los registrados durante el mismo espacio de tiempo para el 2019 y 2020.

Palabras Clave: Delito Informático, Colombia, COVID-19, Virtual, Teletrabajo.

Abstract

The following essay was written in order to show the increase in computer crimes in Colombia due to the COVID-19 pandemic, related to the necessary digitization and virtuality in order to avoid high rates of contagion in different activities like work and study, as well as banking, medical, general business procedures, among others.

The statistics and information collected and subsequently analyzed, associated with the number of reports registered in the Fiscalia General de la Nacion and the Centro Cibernetico Policial during 2019, 2020 and the first quarter of 2021, allowed to identify that the necessary use of web media for the development of daily activities, itself generated an impact on the increase in cybercrimes, because the web is more exposed and used by citizens.

It was concluded that between 2019 and 2020 computer crimes in Colombia increased between 48% to 360%, and that the number of cases registered for the first quarter of 2021, for the five crimes analyzed, already exceeded those registered during the same time frame for 2019 and 2020.

Key Words: Cibercrime, Colombia, COVID-19, Virtual, Home Office.

Introducción

El ensayo escrito a continuación pretende analizar las cifras y tipos de delitos informáticos ocurridos durante la pandemia por COVID-19 en Colombia, realizando un comparativo del año 2019 frente al año 2020, en el cual el 22 de marzo se decretaron las medidas de aislamiento y cuarentena por parte del Presidente de la República por medio del Decreto 457 de 2020.

Con base en lo anterior, se realizará inicialmente un abordamiento de la normatividad colombiana de cara a los delitos informáticos, así como las instituciones que defienden, controlan, analizan y monitorean las actividades asociadas a estos ilícitos con el fin de proteger al Estado, a las instituciones y ciudadanía. Posteriormente, se relacionará información asociada a el cambio de la presencialidad a la virtualidad, explorando algunas vulnerabilidades en seguridad de la información. Así mismo, se analizan las estadísticas de ciberdelitos, efectuando un comparativo de los números registrados entre 2019 y 2020, y el primer trimestre de 2021, reportados por la Fiscalía General de la Nación y el Centro Cibernético Policial.

Finalmente, y con base a los hallazgos, se brindarán recomendaciones con el fin de que lo evidenciado y presentado durante 2020 y 2021, conlleve a tomar medidas reales en busca de la disminución en la materialización de ciberdelitos.

Desarrollo

Definiciones

COVID-19: es la enfermedad causada por el nuevo coronavirus conocido como SARS-CoV-2 (Organización Mundial de la Salud, 2020).

Dato Personal: es toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos. (Superintendencia de Industria y Comercio, s.f.)

Delito Informático: son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc. (Policía Nacional de Colombia, 2021).

Sistema Informático: más conocido en el ámbito de la tecnología por sus siglas “SI” es una técnica que permite el almacenamiento y el proceso de información, para lo cual se vale de un grupo de elementos que se relacionan entre sí.

Estos elementos no son otros que el hardware, el software y finalmente el usuario, quien es el que requiere de la información procesada, y quien es también el que en definitiva tiene el control total de lo que sucede en el sistema. (Marker, s.f.)

Software Malicioso: también conocido como programa malicioso o *malware*, contiene virus, *spyware* y otros programas indeseados que se instalan en una computadora, teléfono o aparato móvil sin consentimiento. Estos programas pueden colapsar el funcionamiento de un aparato y se pueden utilizar para monitorear y controlar la actividad en internet. Además, con estos programas una computadora puede quedar expuesta al ataque de virus y enviar anuncios indeseados o inapropiados. Los delincuentes usan programas maliciosos para robar información personal, enviar spam y cometer fraude. (Comisión Federal del Comercio, 2015)

Teletrabajo: De acuerdo con el Artículo 2 de la Ley 1221 de 2008 “es 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 específico de trabajo". (Congreso de la República, 2021)

Marco Legal

En Colombia, se encuentran distintas normativas y lineamientos asociados a los ciberdelitos, como los siguientes:

- **Ley 1273 de 2009**

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Congreso de la República, 2021)

Tabla N° 1. Ley 1273 de 2009 – Delitos Informáticos.

Capitulo I: De los atentados contra la confidencialidad, la integridad y la	
Artículo 269A: Acceso abusivo a un sistema informático.	Acceder sin autorización a un sistema informático, que se encuentre o no protegido.
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.	Impedir u obstaculizar, sin ninguna facultad, el acceso o funcionamiento de un sistema informático o sus datos, o una red de telecomunicaciones.
Artículo 269C: Interceptación de datos informáticos.	Interceptar datos informáticos en su origen, destino o al interior de un sistema informáticos, sin orden judicial previa.
Artículo 269D: Daño Informático.	Destruir, dañar, borrar, deteriorar, alterar o suprimir, sin encontrarse facultado, datos informáticos, o un sistema de tratamiento de información.
Artículo 269E: Uso de software malicioso	Producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer del territorio nacional, sin tener ninguna facultad, un software malicioso u otros programas de computación de efectos dañinos.
Artículo 269F: Violación de datos personales.	Obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, sin tener ninguna facultad y en beneficio propio de un tercero.

Artículo 269G: Suplantación de sitios web para capturar datos personales.	Diseñar, desarrollar, traficar, vender, ejecutar, programar o enviar páginas electrónicas, enlaces o ventanas emergentes, sin facultad alguna y con fines ilícitos.
Artículo 269H: Circunstancias de agravación punitiva:	Se relacionan ocho (8) tipo de situaciones en las que las penas descritas para cada artículo aumentarán de la mitad a las tres cuartas partes, como son: afectar sistemas o datos informáticos de entes estatales u oficiales, del sector financiero, conducta ejecutada por un servidor publico al ejercer sus funciones, aprovechando confianza brindada, con provecho para él mismo o un tercero, con fines terroristas, utilizar como medio a un tercero de buena fe y/o ser responsable de la administración de la información.
Capítulo II: De los atentados informáticos y otras infracciones	
Artículo 269I: Hurto por medios informáticos y semejantes.	Apoderarse de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, por un medio informático.
Artículo 269J: Transferencia no consentida de activos.	Transferencia no consentida de cualquier activo en perjuicio de un tercero, con ánimo de lucro y valiéndose de alguna manipulación informático o de una estafa. La sanción puede aumentar en la mitad si la cuantía de la transferencia es superior a 200 SMLM (Salario Mínimo Legal Vigente).

Fuente: Elaboración del autor basada en la Ley 1273 de 2.009.

- **CONPES 3701 de 2011 - Lineamientos de Política para Ciberseguridad y Ciberdefensa**

El documento CONPES 3701 tiene como objetivo principal el fortalecimiento de la capacidad del estado para enfrentar las amenazas que atentan contra su seguridad y defensa. Por lo cual, con el fin dar cumplimiento a dicho objetivo, se determinaron unos lineamientos como (Departamento Nacional de Planeación, 2011):

- Implementación de instancias apropiadas con el fin de atender lo pertinente a amenazas y riesgos cibernéticos, las cuales se muestran en la siguiente gráfica:

Gráfica N° 1. Modelo de Coordinación – CONPES 3701

Fuente: Documento CONPES 3701 de 2011.

- Realizar capacitaciones especializadas al personal en temas de seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad, con el fin de fortalecer las capacidades y así poder dar atención a las amenazas.
- Fortalecimiento de la legislación en materia de ciberseguridad y ciberdefensa, con el fin de contar con herramientas jurídicas que permitan realizar la prevención, investigación y judicialización de los delitos cibernéticos.

ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia

El colCERT tiene como responsabilidad principal la coordinación de la Ciberseguridad y Ciberdefensa Nacional. A partir de esto su propósito principal será la coordinación de las acciones necesarias encaminadas a proteger la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. (colCERT, 2017)

Comando Conjunto Cibernético (CCOC)

Las Fuerzas Militares de Colombia trabajan las 24 horas del día y los 7 días de la semana luchando en contra ataques cibernéticos y desinformación, las cuales tienen como fin desacreditar y desvirtuar el trabajo de las instituciones.

El Comando Conjunto Cibernético (CCOC) cuenta con software de análisis y procesamiento de datos, con capacidad de investigación, contención y defensa virtual, al igual que con monitoreo de información publicada en redes sociales, con el fin de evitar la publicación de información falsa o alterada que busca desprestigiar instituciones, robar información, influir en toma de decisiones, entre otros. (Pelcastre, 2019)

Centro Cibernético Policial

El Centro Cibernético Policial es un servicio que ha dispuesto la Policía Nacional para atender los delitos informáticos o incidentes cibernéticos que afectan a la ciudadanía. Por medio del “CAI VIRTUAL”, los ciudadanos que son víctimas de este tipo de delitos o que

requieran alguna orientación, pueden informar a las autoridades de manera gratuita y durante las 24 horas del día, donde les indicarán las medidas a tomar. (Barreto, 2020)

- **Circular Externa 052 de 2007 – Superintendencia Financiera de Colombia**

La circular de la Superintendencia Financiera de Colombia contempla los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios. Para esto contempla unos criterios para la seguridad de la información, que son los siguientes (Superintendencia Financiera Colombia, 2007):

a) Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

b) Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

c) Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Ciber Gaula - Unidad Especializada de la Dirección Antisecuestro y Antiextorsión de la Policía Nacional de Colombia

En cuanto a instituciones también se encuentra el Ciber Gaula, el cual comenzó a operar en abril de 2016 para atender casos asociados a secuestro y extorsión en medios digitales, como por ejemplo el *ransomware* y ciberchantaje sexual. El Ciber Gaula cuenta con personal conformado por investigadores y peritos en Informática Forense, quienes por medio de distintos software y hardware de informática forense pueden realizar análisis y recuperación de información, que permite identificar patrones y victimarios. (Perez & Millan, 2018)

De presencial a virtual

El 06 de marzo de 2020 el Ministerio de Salud y Protección Social confirmó el primer caso de COVID-19 en Colombia (Ministerio de Salud y Protección Social, 2020) y el 22 de marzo de 2020 se impartió el Decreto 457 de 2020 por medio del cual el Presidente de la República impartió instrucciones y ordenó el Aislamiento Preventivo Obligatorio o cuarentena de todos los habitantes del país por el COVID-19 (Presidencia de la Republica, 2020), el cual se postergó debido al incremento de casos por ciudad y a nivel nacional.

Por lo anterior y con el fin de continuar, poder seguir una "cotidianidad" y con la necesidad de retomar actividades como médicas, bancarias, comerciales, laborales, culturales, entre otras, cada empresa, institución o individuo se vio obligado a repensar en como establecer la continuidad de su negocio, y vio en el internet la opción de poder continuar o fortalecer por este medio sus actividades y/o ofertando sus servicios por medio de redes sociales, páginas web, aplicaciones móviles, sin embargo sin evaluar en muchos casos los riesgos que estos podían traer y elevando así el riesgo de fraude.

De acuerdo con el artículo "El impacto de la pandemia en el uso de las aplicaciones móviles" una de las consecuencias del COVID-19 es el aumento en las descargas y tiempo dedicado a las aplicaciones móviles asociadas a educación y productividad, al igual que la descarga de juegos para pasar el tiempo de cuarentena (Slotnisky, 2020).

Y es que el COVID-19 no solo ha generado una emergencia a nivel médico y sanitario, sino también a nivel de ciberseguridad con el aumento de la utilización del medio virtual y

digital para la ejecución de la mayoría de actividades, debido a que algunas personas prefieren permanecer en casa por miedo al contagio, lo que han aprovechado los ciberdelincuentes para obtener información por medio ingeniería social, envío de correos electrónicos maliciosos con el fin de hurtar o secuestrar la información personal de la personas, desarrollo de aplicaciones malignas, aprovechar las vulnerabilidades del teletrabajo, entre otros. Por eso es muy importante que las compañías efectúen campañas de concientización sus clientes, usuarios y empleados frente a la importancia de la seguridad en todos los procesos, fortalecer los canales de comunicación y, trabajar de manera proactiva y preventiva, y no reactiva (Portafolio, 2020).

Ataques Cibernéticos ante la oficina remota – Deloitte

La firma Deloitte como proveedor en servicios de riesgo empresarial entre ellos la gestión de seguridad de la información y la privacidad, ha desarrollado distintos artículos y presentaciones asociadas a las condiciones generales de ciberseguridad en tiempos de pandemia por Covid-19, donde en uno de sus análisis de nombre *COVID-19 Ataques cibernéticos ante la oficina remota ¿Cuál será el futuro del trabajo después de esta pandemia?* presenta ejemplos de relajación de controles de ciberseguridad de frente al trabajo en casa, ocasionados por las medidas para evitar el contagio y propagación del Covid-19 en la comunidad, como se relacionan a continuación (Deloitte, 2020):

Gráfica N° 2. Ejemplos observados de relajación de controles de ciberseguridad - Deloitte

Fuente: COVID-19 Ataques cibernéticos ante la oficina remota ¿Cuál será el futuro del trabajo después de esta pandemia? – Deloitte

La anterior grafica demuestra los errores en los controles por parte de las organizaciones al momento de la generación del teletrabajo, lo que la lleva a tener un gran número de vulnerabilidades y estar expuesta a las amenazas de ataques cibernéticos o el acceso a información confidencial por parte de los ciberdelincuentes, por medio de la computadora de uno de sus empleados que no tenga medidas de seguridad adecuadas o que al tratarse de una computadora personal acceda a páginas de internet no seguras.

Lecciones en materia de seguridad a causa COVID-19

La página web *We Live Security* relaciona el artículo “8 lecciones en materia de seguridad que el COVID-19 dejó a las organizaciones”, escrito por Miguel Ángel Mendoza, donde interesantemente aborda entre algunos los siguientes puntos:

- **Agilidad en transformación digital:** En este punto el autor indica que a pesar de que el proceso de transformación digital comenzó ya hace algunos años, algunas organizaciones lo postergaron, por lo que al llegar la pandemia se vieron afectadas por falta de disponibilidad.

- **Seguridad sin límites:** El autor indica que a pesar de que las organizaciones han invertido recursos en seguridad de la información, en ocasiones estas solo piensan en espacios físicos. Sin embargo, con la llegada de la pandemia y las nuevas condiciones de trabajo muestran la necesidad de tener mecanismos de protección en los puntos donde se procesen datos, más aún cuando los riesgos aumentan por el uso de equipos y redes no corporativos, que no cuentan con los debidos controles de seguridad.

- **Ciberfraude no tiene cuarentena:** El autor precisa que, con el avance de la pandemia y la declaración de cuarentenas, las herramientas de videollamadas tuvieron un auge, las cuales los ciberdelincuentes no desaprovecharon en encontrar sus vulnerabilidades para propagar archivos maliciosos.

- **Tener en cuenta todos los escenarios:** El autor se pregunta si dentro de las organizaciones se consideró una pandemia como escenario realista dentro de la evaluación de riesgos, e indica que a pesar de ser un evento de baja probabilidad de ocurrencia tiene un impacto elevado.

- **Segura continuidad del negocio:** El autor precisa que con lo rápido que algunas organizaciones tomaron medidas para proveer conectividad, acceso y operación para sus colaboradores, se obviaron medidas de seguridad. Por lo anterior, indica la necesidad de contar con condiciones de seguridad para trabajar desde cualquier punto y concientizar a los colaboradores de proteger los datos sensibles, tanto corporativos como personales. (Mendoza, 2020)

Los cinco puntos que se consideran con mayor relevancia en el artículo demuestran que las organizaciones no contaban con una preparación real de cara a enfrentar una pandemia y tener la respuesta a la misma, por lo que quedaron vulnerables en la seguridad de su información al tener que ceder la transmisión de datos por redes pertenecientes a la organización y así poder dar continuidad al negocio.

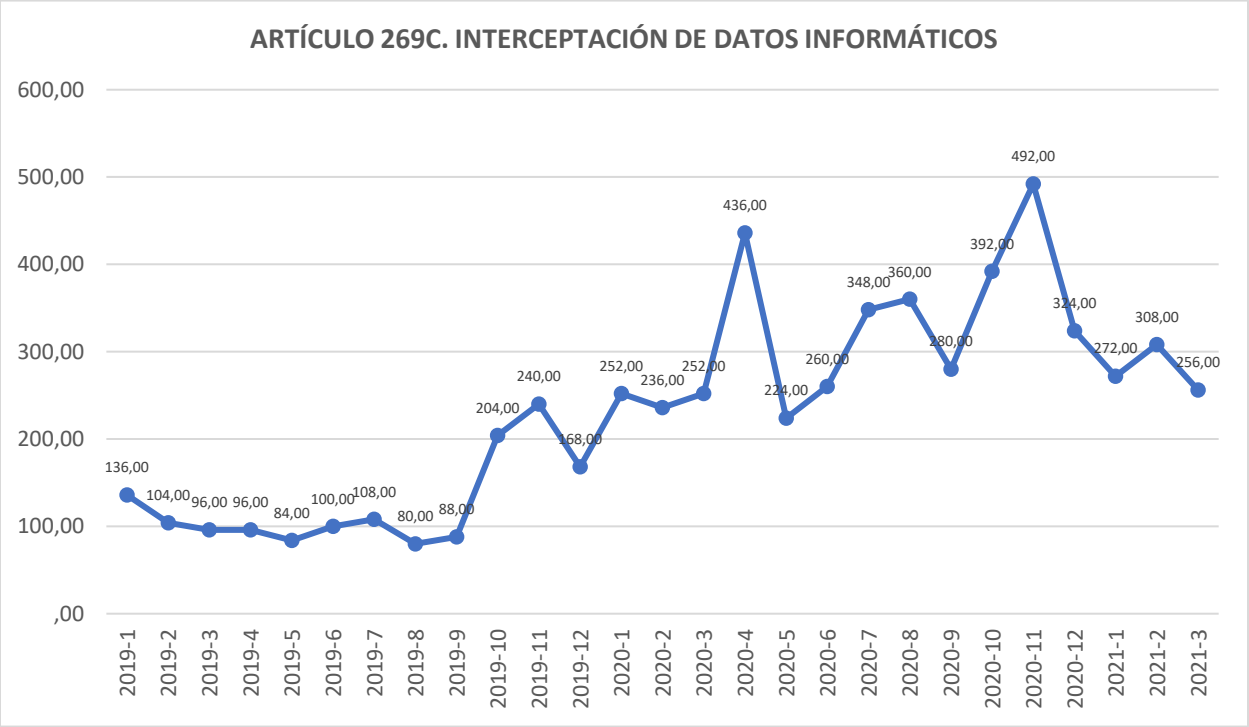
Estadísticas

Fiscalía General de la Nación

De acuerdo con las cifras registradas en la Fiscalía General de la Nación, se reporta que con respecto al delito ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS de la Ley 1273 de 2009, en el año 2019 se presentaron un total de 1.504 noticias criminales y

para el año 2020 un total de 3.856, reflejando para este un aumento del 156%. En cuanto al primer trimestre del 2021, se registran un total de 836 noticias criminales, frente 336 del 2019 y 740 del 2020.

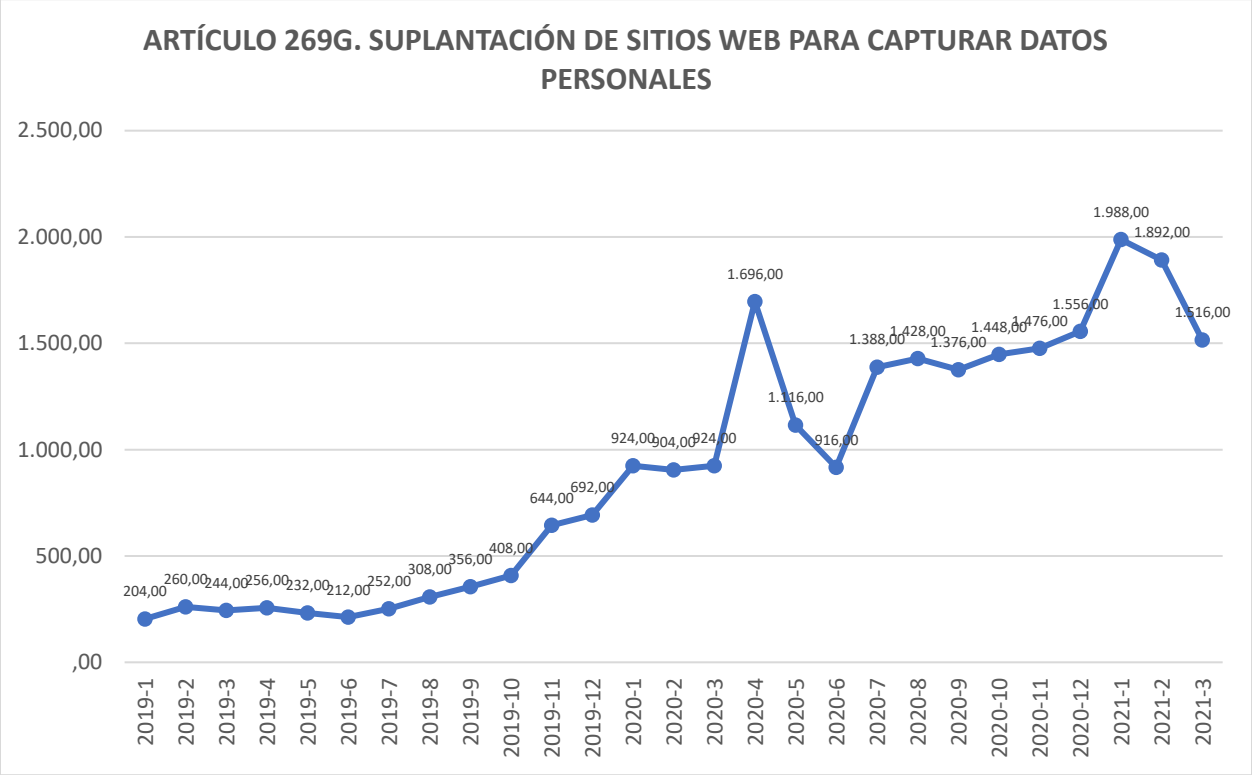
Gráfica N° 3. Cantidad de Noticias Criminales asociadas al delito de Interceptación de Datos Informáticos entre 2019 a 2021.



Fuente: Modificado por el autor de estadísticas de Fiscalía General de la Nación

Por otra parte, el delito tipificado en el ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES de la Ley 1273 de 2009, en el año 2019 se registró un total de 4.068 noticias criminales y para el año 2020 un total de 15.112, reflejando para este un aumento del 271%. En cuanto al primer trimestre del 2021, se registran un total de 5.396 noticias criminales, frente 708 del 2019 y 2.752 del 2020.

Gráfica N° 4. Cantidad de Noticias Criminales asociadas al delito de Suplantación de Sitios Web para Capturar Datos Personales entre 2019 a 2021.



Fuente: Modificado por el autor de estadísticas de Fiscalía General de la Nación

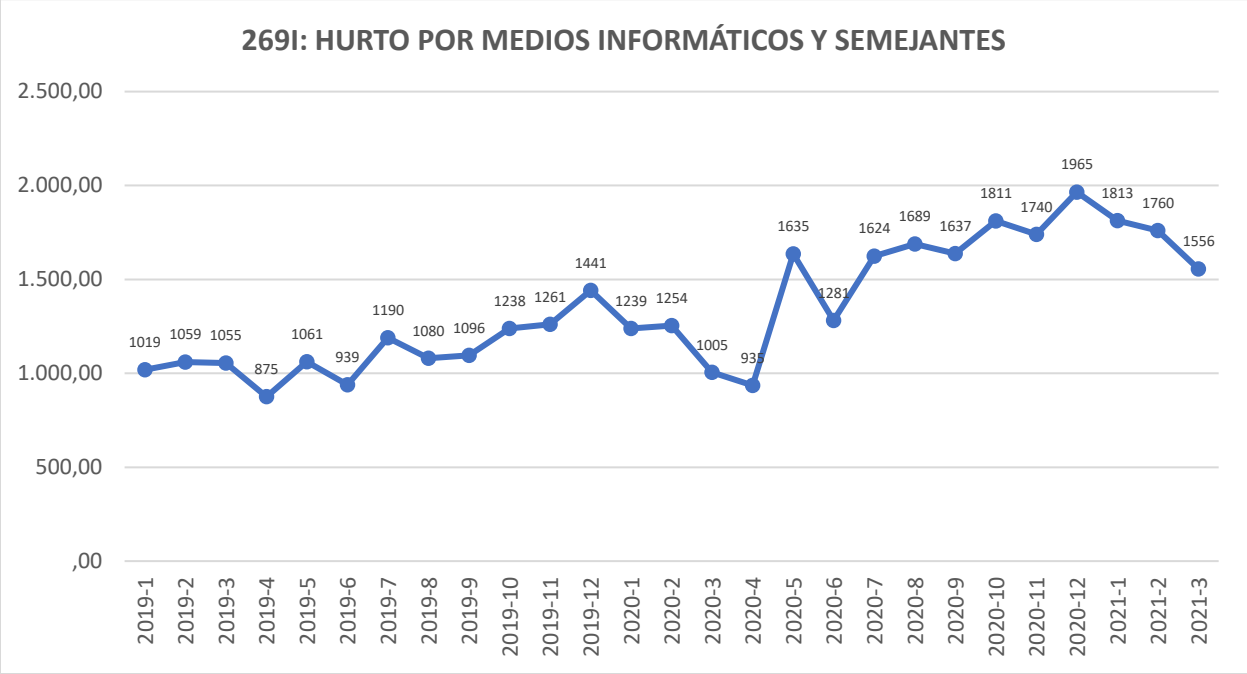
El delito ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES de la Ley 1273 de 2009, reporta en el año 2019 se presentaron un total de 12.772 noticias criminales y para el año 2020 un total de 29.756, reflejando para este un aumento del 133%. En cuanto al primer trimestre del 2021, se registran un total de 11.588 noticias criminales, frente 3.096 del 2019 y 4.536 del 2020.

Gráfica N° 5. Cantidad de Noticias Criminales asociadas al delito Violación de Datos Personales entre 2019 a 2021.

Fuente: Modificado por el autor de estadísticas de Fiscalía General de la Nación

Para el delito HURTO POR MEDIOS INFORMATICOS – ART269I de la Ley 1273 de 2009, se reporta en el año 2019 se presentaron un total de 13.314 noticias criminales y para el año 2020 un total de 17.815, reflejando para este un aumento del 34%. En cuanto al primer trimestre del 2021, se registran un total de 5.129 noticias criminales, frente 3.133 del 2019 y 3.498 del 2020.

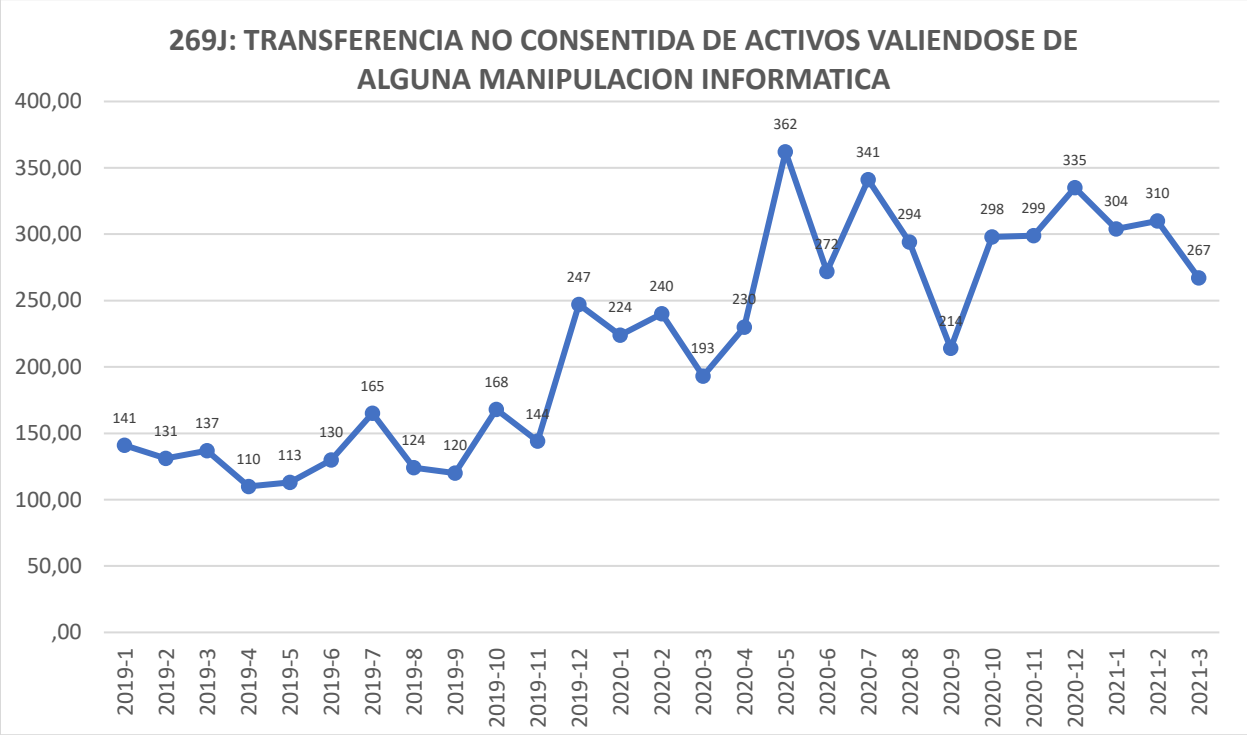
Gráfica N° 6. Cantidad de Noticias Criminales asociadas al delito de Hurto por Medios Informáticos y Semejantes entre 2019 a 2021.



Fuente: Modificado por el autor de estadísticas de Fiscalía General de la Nación

En cuanto al delito de TRANSFERENCIA NO CONSENTIDA DE ACTIVOS VALIENDOSE DE ALGUNA MANIPULACION INFORMATICA – ART269J de la Ley 1273 de 2009, en el año 2019 se presentaron un total de 1.730 noticias criminales y para el año 2020 un total de 3.302, reflejando para este un aumento del 91%. En cuanto al primer trimestre del 2021, se registran un total de 881 noticias criminales, frente 409 del 2019 y 657 del 2020 (Fiscalia General de la Nacion, 2021).

Gráfica N° 7. Cantidad de Noticias Criminales asociadas al delito de Transferencia No Consentida de Activos entre 2019 a 2021.



Fuente: Modificado por el autor de estadísticas de Fiscalía General de la Nación.

Centro Cibernético de la Policía Nacional de Colombia

El Centro Cibernético Policial cuenta con el reporte de los incidentes informáticos que son reportados por los ciudadanos por medio del CAI Virtual, los cuales para 2019, 2020 y el primer trimestre de 2021 registran los siguientes datos (Centro Cibernético Policial, 2021):

Tabla N° 2. Números de denuncias de delitos informáticos de 2019, 2020 y 2021 (Enero a Marzo) – Centro Cibernético Policial.

Delito	2019	2020	2021 (Ene-Mar)
Artículo 269I. Hurto por medios informáticos y semejantes	11.050	17.374	4.732
Artículo 269F. Violación de datos personales	3.444	9.851	3.830
Artículo 269A. Acceso abusivo a un sistema informático	3.118	7.208	2.197
Artículo 269G. Suplantación de sitios web para capturar datos personales	1.202	5.531	1.795
Artículo 269J. Transferencia no consentida de activos	1.648	3.491	972
Artículo 269C. Interceptación de datos informáticos	478	1.630	431
Artículo 269E. Uso de software malicioso	452	669	110
Artículo 269D. Daño informático	282	639	136
Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación	126	277	72

Fuente: Modificado por el autor estadísticas aplicativo SIEDCO PLUS –Policía Nacional.

De acuerdo con la tabla anterior, los delitos con mayor crecimiento de acuerdo con las estadísticas de la Centro Cibernético de la Policía Nacional en comparación con las cifras del año 2019 y 2020, son: Suplantación de Sitios Web para Capturar Datos Personales, Interceptación de Datos Informáticos y Violación de Datos Personales, como se detalla a continuación.

Tabla N° 3. Porcentaje de Aumento de Casos 2019Vs2020.

DELITO	% de Crecimiento 2019 Vs 2020
Artículo 269I. Hurto por medios informáticos y semejantes	57%
Artículo 269F. Violación de datos personales	186%
Artículo 269A. Acceso abusivo a un sistema informático	131%

Artículo 269G. Suplantación de sitios web para capturar datos personales	360%
Artículo 269J. Transferencia no consentida de activos	112%
Artículo 269C. Interceptación de datos informáticos	241%
Artículo 269E. Uso de software malicioso	48%
Artículo 269D. Daño informático	127%
Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación	120%

Fuente: Modificado por el autor estadísticas aplicativo SIEDCO PLUS –Policía Nacional.

Como se observa en la relación de gráficas y tablas de los datos presentados por la Fiscalía General de la Nación y el Centro Cibernético Policial, los delitos cibernéticos aumentaron significativamente entre el 2019 y 2020.

Conclusiones

Dentro del análisis del documento, se pudo establecer que en Colombia se registró un aumento de los delitos informáticos de 2019 al 2020 de un **114%**, de acuerdo con las cifras registradas por el Centro Cibernético Policial, el cual por medio del CAI VIRTUAL recolecta la información reportada por los ciudadanos y organizaciones, que registren afectaciones por cualquiera de los delitos tipificados en la Ley 1273 de 2009. El aumento se registró principalmente en tres delitos Suplantación de Sitios Web para Capturar Datos Personales, Interceptación de Datos Informáticos y Violación de Datos Personales, asociados al robo de información sensible de los ciudadanos.

Así mismo en cuanto a las cifras del primer trimestre del 2021, se observa un aumento del **41%** frente al mismo periodo del 2020, lo cual genera una alta probabilidad que el 2021 continúe y finalice con número de casos superiores a los del 2020.

Por otra parte, se evidencia que Colombia cuenta con amplias dependencias en las Fuerzas Militares y Policía Nacional que tienen, de acuerdo con su descripción, personal capacitado para atender las necesidades de ciberseguridad del Estado y la ciudadanía, sin embargo, de acuerdo con las cifras y lo expuesto en distintos artículos analíticos, existe una falta de respuesta y preparación de las organizaciones para la continuidad de negocio bajo medidas tolerables de seguridad de la información.

El teletrabajo y las actividades de la cotidianidad que se volvieron virtuales, como medida para la continuidad de las organizaciones y del diario vivir, es una de las más grandes brechas, debido a que, al habilitarlo de manera rápida o en una creación apresurada, no se tuvo en cuenta las respectivas medidas de seguridad de la información, lo que dejo espacio a los ciberdelincuentes para efectuar nuevos tipos de ataques más complejos.

Es importante contemplar la nueva realidad global ocasionada por la pandemia, donde los ciberataques son más comunes día a día, por lo que se realza la insuficiente cultura cibernética y la poca inversión en temas de ciberseguridad, donde la web cada vez más es un ámbito de conflicto y donde la información se convierte cada vez en el poder y tesoro más preciado de todas las organizaciones, sin importar que tan grandes sean las mismas.

Recomendaciones

De acuerdo con los hallazgos durante la elaboración del ensayo, se considera pertinente brindar las siguientes recomendaciones:

- Establecer una ciber estrategia a nivel país donde se encuentren asociados el colCERT, el Comando Conjunto Cibernético, el Centro Cibernético Policial y el Ciber Gaula en conjunto con el MinTic - Ministerio de Tecnologías de la Información y las Comunicaciones, encaminada a la búsqueda de formar y ampliar los accesos seguros a la web para la ciudadanía, a partir de la identificación de los riesgos y modalidades en cada momento, lo que lleve a poder de manera conjunta, adaptar las respectivas gestiones por medio de recursos técnicos y humanos, que se encuentren en la capacidad de mantener un ambiente informático seguro.

- Generar una mayor sinergia entre las instituciones públicas y privadas en pro de hacer frente al aumento de los delitos informáticos, apoyando así a las organizaciones quienes no tienen unos protocolos de seguridad definidos y teniendo mayor cercanía a la ciudadanía, por medio de capacitaciones o mensajes de canales diferentes a la web (radio, televisión, etc.), y así crear una cultura de ciberseguridad en el país.

- Fortalecimiento de las medidas y campañas de seguridad en el teletrabajo, por medio de capacitaciones, reemplazando soluciones tecnológicas ineficientes, acceso seguro a la red (VPN).

- Replanteo de los planes de continuidad de negocio de las organizaciones, teniendo en cuenta la situación de la pandemia y otros riesgos que a pesar de su baja probabilidad de ocurrencia puedan generar un gran impacto.

Referencias

Barreto, L. (19 de Octubre de 2020). *Bogotá*. Obtenido de Bogotá: https://bogota.gov.co/mi-ciudad/seguridad/conoce-como-funciona-el-cai-virtual-de-la-policia

Centro Cibernético Policial. (03 de Junio de 2021). *Centro Cibernético Policial*. Obtenido de Centro Cibernético Policial: https://caivirtual.policia.gov.co/

colCERT. (12 de Julio de 2017). *colCERT*. Obtenido de colCERT: http://www.colcert.gov.co/

Comisión Federal del Comercio. (Noviembre de 2015). *Comisión Federal del Comercio*. Obtenido de Comisión Federal del Comercio: https://www.consumidor.ftc.gov/articulos/s0011-software-malicioso

Congreso de la República. (04 de Mayo de 2021). *Congreso de la República*. Obtenido de Congreso de la República: http://www.secretariasenado.gov.co/senado/basedoc/ley_1221_2008.html

Congreso de la República. (20 de Abril de 2021). *Secretaria Senado*. Obtenido de Secretaria Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Deloitte. (Abril de 2020). *Deloitte.* Obtenido de Deloitte: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cambiando%20la%20forma%20de%20trabajo%20y%20la%20ciberdefensa.pdf

Departamento Nacional de Planeación. (14 de Julio de 2011). *ALTA CONSEJERIA DISTRITAL TIC.* Obtenido de ALTA CONSEJERIA DISTRITAL TIC: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

Fiscalia General de la Nacion. (30 de Abril de 2021). *Fiscalia General de la Nacion*. Obtenido de Fiscalia General de la Nacion: https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

Marker, G. (s.f.). *tecnología+informatíca*. Obtenido de tecnología+informatíca: https://www.tecnologia-informatica.com/que-es-sistema-informatico/

Mendoza, M. Á. (5 de Mayo de 2020). *WeLiveSecurity*. Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2020/05/05/lecciones-seguridad-informatica-covid-19-dejo-organizaciones/

Ministerio de Salud y Protección Social. (06 de Marzo de 2020). *Ministerio de Salud y Protección Social*. Obtenido de Ministerio de Salud y Protección Social: https://www.minsalud.gov.co/Paginas/Colombia-confirma-su-primer-caso-de-COVID-19.aspx#:~:text=%E2%80%8B%2DLa%20paciente%20acudi%C3%B3%20a,6%20de%20marzo%20de%202020.

Organización Mundial de la Salud. (10 de Noviembre de 2020). *Organización Mundial de la Salud*. Obtenido de Organización Mundial de la Salud: https://www.who.int/es/news-room/q-a-detail/coronavirus-disease-covid-19

Pelcastre, J. (13 de Diciembre de 2019). *Diálogo*. Obtenido de Diálogo: https://dialogo-americas.com/es/articles/militares-colombianos-en-guerra-contra-cibercriminales/

Perez, F., & Millan, L. (25 de Octubre de 2018). *SeguriLatam*. Obtenido de SeguriLatam: https://www.segurilatam.com/entrevistas/el-exito-del-ciber-gaula-se-fundamenta-en-la-formacion-en-inteligencia-e-investigacion-criminal_20181025.html

Policía Nacional de Colombia. (05 de Junio de 2021). *Policía Nacional de Colombia*. Obtenido de Policía Nacional de Colombia: https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Portafolio. (15 de Septiembre de 2020). *Portafolio*. Obtenido de Portafolio: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

Presidencia de la Republica. (22 de Marzo de 2020). *Coronavirus Colombia.* Obtenido de Coronavirus Colombia: https://coronaviruscolombia.gov.co/Covid19/decretos.html

Slotnisky, D. (20 de Abril de 2020). *Digital House*. Obtenido de Digital House: https://www.digitalhouse.com/ar/blog/el-impacto-de-la-pandemia-en-el-uso-de-las-aplicaciones-moviles

Superintendencia de Industria y Comercio. (s.f.). *Superintendencia de Industria y Comercio*. Obtenido de Superintendencia de Industria y Comercio: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia Financiera Colombia. (25 de Octubre de 2007). *Superintendencia Financiera Colombia.* Obtenido de Superintendencia Financiera Colombia: https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/-20145