CAMPAÑA

"Desenmascara el delito informático, no al fraude en las redes sociales"

Primer informe de avance del proyecto[1]:

ANÁLISIS SITUACIONAL

7 noviembre de 2019

Sandra Benitez, Beatriz Sandia y Edmundo Vitale

[1] Proyecto aprobado por el Comité de Selección del Fondo de Respuesta Rápida (FRR) de Derechos Digitales en el mes de septiembre de 2019.

CONTENIDO

Contenido

INTRODUCCIÓN

Este documento tiene como finalidad presentar el primer informe de avance del proyecto denominado: "Desenmascara el delito informático, no al fraude en las redes sociales", el cual es una campaña para orientar a los ciudadanos venezolanos sobre los riesgos que corren al realizar prácticas inadecuadas en las redes sociales, que los exponen al fraude y a la violación de su seguridad digital.

El informe comprende el análisis situacional del contexto en el que los ciudadanos se exponen al delito informático, específicamente en las redes sociales. Este informe está estructurado de la siguiente manera: a) disposiciones generales, b) recolección de la información, c) análisis de las Fortalezas, Oportunidades, Debilidades y Amenazas (FODA), d) análisis del árbol del problema, y e) análisis del árbol de objetivos.

1.- DISPOSICIONES GENERALES

La campaña "Desenmascara el delito informático, no al fraude en las redes sociales" está orientada a los ciudadanos venezolanos que son víctimas de delitos informáticos en las redes sociales. Para realizar el análisis situacional de la campaña, en el presente informe, se evalúa la realidad venezolana y se determina la problemática y las potenciales áreas que pueden ser atendidas en la misma.

Actualmente la crisis económica, política y social que se vive en Venezuela ha traído como consecuencia un empobrecimiento acelerado de la población, producto de la escasez de bienes y servicios, así como de la paralización del aparato productivo del país; lo cual ha llevado a los ciudadanos a buscar medios alternativos para solventar las necesidades básicas en lo que respecta a alimentación y medicamentos. Igualmente la dificultad para adquirir divisas, gestionar documentos oficiales (pasaportes, partidas de nacimiento, etc.) y realizar remesas ha encaminado a los ciudadanos a buscar gestores en medios digitales para facilitar estos tipos de trámites. Entre los medios alternativos empleados se encuentran el uso de las redes sociales para realizar gestiones oficiales y transacciones económicas sin una regulación y control por parte del Estado, lo cual expone a los ciudadanos a ser víctimas de delitos informáticos.

En este contexto el Estado de Derecho de los ciudadanos es vulnerable y su seguridad digital se encuentra en riesgo, lo cual afecta los Derechos de Internet (DI) y Derechos Económicos, Sociales y Culturales (DESC) de los mismos. Particularmente, la situación de fraude en las redes sociales pareciera prolongarse en el tiempo, de no existir mecanismos efectivos para orientar a los ciudadanos sobre el uso adecuado de los medios y los servicios digitales.

En este sentido, se realizó una investigación documental del marco legal venezolano relacionado con el delito informático, así como también se determinaron algunos aspectos vinculados con el uso y manejo de las redes sociales por parte de los ciudadanos, prácticas de ingeniería social que promueven ataques cibernéticos, y el manejo de estadísticas sobre casos de delitos informáticos, población afectada, entre otros. De esta manera, se comprende la problemática y se determina la situación actual que promueve el delito informático en las redes sociales. Adicionalmente se categorizaron los delitos informáticos y se determinaron casos de ciudadanos afectados, con el interés de evaluar tendencias.

Por otra parte, se realizó un análisis de las potenciales causas y consecuencias que originan una serie de problemas críticos, que promueven significativamente el delito informático. Igualmente se presenta, en una segunda parte, el análisis de objetivos y las soluciones posibles a ésta problemática, que servirán de insumo para el diseño de la campaña de orientación y sensibilización sobre el delito informático en las redes sociales. Por otra parte, se sistematizó en una matriz FODA la situación del entorno interno y externo del contexto al que se exponen los ciudadanos cuando se enfrentan a los delitos informáticos, lo cual permitió determinar una visión más amplia sobre las soluciones que podría promover la campaña, compromiso final del presente proyecto.

2.- REVISIÓN DOCUMENTAL

2.1.- MARCO LEGAL

Durante los últimos 20 años, en Venezuela se han desarrollado un conjunto de regulaciones jurídicas y políticas públicas dirigidas a incorporar y proteger de manera integral los sistemas que utilicen las Tecnologías de Información y Comunicación (TIC), así como también se han incorporado normativas para la prevención y sanción de los delitos cometidos mediante el uso de las TIC. De igual forma las políticas públicas diseñadas por el ejecutivo nacional dan muestra de ello a través de los planes de la nación establecidos por el Gobierno actual.

2.1.1.- Leyes

La última reforma de la carta magna, sienta las bases para comenzar a partir del año 1999, el desarrollo de políticas públicas dirigidas a garantizar el acceso universal a las tecnologías y a los servicios informativos de interés público, como se refleja en el artículo 110 de la Constitución de la República Bolivariana de Venezuela[2] (CRBV) el cual señala:

"El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía".

Es por ello que a partir del 2000, Venezuela desarrolla un amplio cuerpo normativo donde la prioridad fundamental es el desarrollo de tecnologías, el acceso universal y la incorporación de las mismas en el sistema educativo, según lo prevé el artículo 108 de la CRBV, donde, el Estado asume la responsabilidad de garantizar servicios públicos de radio, televisión, redes de bibliotecas y de informática, a fin de permitir el acceso universal a la información. Para cumplir estos mandatos el Gobierno establece que los centros educativos deben incorporar el conocimiento y la aplicación de las nuevas tecnologías e innovaciones, dando inicio a una nueva cultura educativa donde el uso de las tecnologías marca el hilo conductor del proceso de aprendizaje. A continuación se presenta un resumen sucinto de leyes y decretos establecidos en el marco normativo Venezolano:

[2] http://www.conatel.gob.ve/constitucion-de-la-republica-bolivariana-de-venezuela-2/

- **Decreto presidencial 825[3]:** Con base al principio constitucional previsto el artículo 110 de la CRBV, el 10 de mayo del 2000, se promulgo el decreto Presidencial 825, el cual reconoce de interés público la ciencia, la tecnología, el conocimiento y los servicios de tecnologías de la información, imponiendo a los órganos de la Administración Pública, la obligación de incluir, en el desarrollo de sus actividades, metas relacionadas con el uso de internet, a objeto de facilitar el intercambio de información. El decreto declara el acceso y uso de internet, como política prioritaria para el desarrollo cultural, económico, social y político de la Nación; así como también establece como objetivo el de insertar a los ciudadanos en una sociedad del conocimiento permitiendo la capacitación a través de internet.

- **Ley Orgánica de Telecomunicaciones[4]:** El 12 de junio del 2000, se dictó la Ley Orgánica de Telecomunicaciones, publicada en Gaceta Oficial número 36.970, con la finalidad de generar un marco adecuado para la modernización y apertura de las telecomunicaciones en el país, la cual introduce un cambio paradigmático en la función del estado cambiando la noción general de servicio público por la de actividad de interés general, correspondiéndole a los particulares, prestar el servicio en régimen de libre competencia. Su objetivo principal es la promoción de la investigación, el desarrollo y la transferencia tecnológica en materia de telecomunicaciones, la utilización de nuevos servicios, redes y tecnología con el propósito de asegurar el acceso a estos en igualdad a todos los ciudadanos.

- **La Ley de Mensajes de Datos y Firmas Electrónicas[5]:** El 10 de febrero del 2001, se dictó la Ley de Mensajes de Datos y Firmas Electrónicas, la cual reconoce jurídicamente el valor y eficacia jurídica de los documentos electrónicos, equiparándolos a los documentos tradicionales. Esta Ley constituye el punto de partida para la tramitación de los procedimientos electrónicos en el campo de la administración pública y la administración de justicia, se comienza a construir las bases de la Seguridad Digital en el país. A partir de esta Ley, los cuerpos legislativos posteriores a ella, comienzan a introducir la posibilidad de realizar procedimientos tradicionales a través de la vía electrónica, con pleno valor probatorio y jurídico, tal es el caso de la reforma del Código Orgánico Tributario en el 2001, el cual permite la notificación electrónica y la posibilidad de realizar declaraciones electrónicas, sustituyendo el procedimiento tradicional por medios completamente digitalizados.

- **Ley Especial contra los Delitos Informáticos[6] (LEDI):** Con el fin de comenzar a regular y sancionar el uso indebido de las tecnologías, efectuado a través de conductas que vulneran los bienes jurídicos, y que hasta el 2001, no se encontraban regulados en el código penal vigente, se publica en Gaceta Oficial número 37.313, de fecha 30 de octubre del 2001, la LEDI, con la intención de proteger la privacidad de las comunicaciones y de la información contenida en medios digitales. La característica principal de la LEDI, es que trata de ir más allá de la tipificación de los delitos y de atender de manera integral los aspectos y necesidades de las personas afectadas, tal como lo señala el artículo 1 de la citada Ley:
  "La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el

[3] http://www.conatel.gob.ve/wp-content/uploads/2017/01/sobre-internet.pdf
[4] http://www.conatel.gob.ve/ley-organica-de-telecomunicaciones-2/
[5] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Mensajes-de-Datos-y-Firmas-Electr%C3%B3nicas.pdf
[6] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf

uso de dichas tecnologías, en los términos previstos en esta Ley".

La LEDI, cobra hoy en día gran importancia, debido al crecimiento de operaciones electrónicas que se realizan; ya que la misma es de utilidad para los ciudadanos al momento de reportar y tipificar fraudes cometidos y afectaciones al patrimonio personal. Igualmente la LEDI es aplicable en el uso y manejo de redes sociales, ya que las mismas son usadas para realizar distintos tipos de operaciones en línea, lo cual expone a un segmento de ciudadanos vulnerables a ser víctimas de delitos informáticos.

- **Ley de Tecnología de Información[7]:** En el mismo orden de ideas el Estado, a fin de permitir el acceso universal a la información, como política pública, en el 2005, crea la Ley de Tecnología de Información, con el propósito de impulsar la extensión, desarrollo promoción y masificación, de las tecnologías de información en el país, conformando las bases del gobierno electrónico.

- Posteriormente la **Ley de Infogobierno[8]** en 2013, junto con la Ley de Tecnología de Información, desarrollan y complementan los cimientos para promover el gobierno electrónico, la extensión, el desarrollo, promoción y masificación, de las tecnologías de información en el país.

- Por otra parte, el Estado con el interés de analizar el comportamiento de las redes sociales crea en el 2014, una instancia como la **Dirección de estudios tecnológicos y de información[9]**, para procesar y analizar la información proveniente de la web y así determinar el comportamiento de las redes sociales, con el fin de identificar fortalezas o amenazas para el desarrollo y estabilidad política del país.

- **Ley contra el odio (2017):** En el 2017 se establece la Ley contra el odio, la cual prevé penas de prisión, hasta por veinte años a quienes, a través del uso de servicios de radio y televisión y uso de plataformas de redes sociales, cometan acciones que sean calificadas como incitación al odio.

A continuación se presenta un resumen de las leyes e instancia que regulan el uso de las TIC y las redes sociales:

ORDENAMIENTO JURÍDICO	PRINCIPIO TUTELADO
Constitución Nacional de la República Bolivariana de Venezuela (1999)	El Estado asume la responsabilidad de garantizará servicios públicos de radio, televisión, redes de bibliotecas y de informática, a fin de permitir el acceso universal a la información
Decreto 825 (2000)	Insertar a los ciudadanos en una sociedad del conocimiento permitiendo la capacidad de capacitación a través de internet.
Ley de Telecomunicaciones (2000)	Se reconoce a la tecnología el carácter de interés general.
Ley de Mensaje de Datos y Firmas Electrónicas (2001)	Esta Ley constituye el punto de partida para la tramitación de los procedimientos electrónicos en el campo de la Administración Pública y la administración de justicia, sienta las bases de la Seguridad Digital en el país
Ley Especial contra los Delitos	Proteger la privacidad de las comunicaciones y de la información

[7] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Org%C3%A1nica-de-Ciencia-Tecnolog%C3%ADa-e-Innovacion.pdf
[8] http://www.conatel.gob.ve/ley-de-infogobierno/
[9] https://www.ipys.org.ve/2014/02/25/reglamento-del-cesppa-contiene-disposiciones-contrarias-a-la-libertad-de-expresion/

Informáticos (2001)	contenida en medios digitales. Regular y sancionar el uso indebido de las tecnologías
Ley de Tecnología de Información (2005)	Pretende la extensión, desarrollo promoción y masificación, de las tecnologías de información en el país, sienta las bases del gobierno electrónico.
La Dirección de estudios tecnológicos y de información (2014)	Se crea la dirección de estudios tecnológicos y de información, entre cuyas funciones se encuentra procesar analizar la información proveniente de la web y analizar el comportamiento de las redes sociales.
Ley contra el Odio (2017)	Esta Ley prevé penas de prisión, hasta por veinte años a quienes, a través del uso de servicios de radio y televisión y uso de plataformas de redes sociales, cometan acciones que sean calificadas como incitación al odio.

2.1.2.- Políticas públicas y planes de la nación

Durante los últimos 20 años, se han desarrollado en Venezuela cuatro planes de la Nación, centrados en el desarrollo de políticas dirigidas al fortalecimiento de la economía, la paz y el desarrollo social: 1) Plan Simón Bolívar 2001-2007[10]; 2) Primer Plan de Desarrollo Económico y Social de la Nación 2007-2013[11]; 3) Segundo Plan de Desarrollo Económico y Social de la Nación 2013-2019[12];4) Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2019-2025[13].

El objeto del último Plan recientemente aprobado, es cambiar la sociedad, generar un nuevo asiento, para dar el salto cualitativo y consolidar el socialismo, sobre la base de las condiciones creadas en los últimos 18 años de ejercicio del gobierno actual.

En el Plan 2019-2025 la problemática central a asumir, resolver y desarrollar, es la económica, para ello, el Plan presenta en su estructura objetivos históricos, nacionales, y estratégicos, con indicadores y políticas que van en concordancia con los Objetivos de Desarrollo Sostenible[14] de la Agenda 2030 (ODS 2030) de la Organización de Naciones Unidas. Entre los objetivos relacionados con el uso de las tecnologías para el impulso económico y prevención de delitos informáticos, se plantea diseñar procesos informáticos estandarizados, transparentes y auditables, con la incorporación de legislación referente a gobierno electrónico y demás componentes asociados a las tecnologías libres de información, además de promover e incentivar el uso de las tecnologías y el comercio electrónico seguro en el intercambio de servicios, materias primas, bienes semielaborados y productos finales, a fin de reducir los eslabones de las cadenas de comercialización de bienes y servicios básicos para la población.

Entre los objetivos más resaltantes planteados en el Plan 2019-2025, relacionados con el uso de nuevas tecnologías e incorporación de normas que regulen el uso de las tecnologías abiertas, y la aplicación del comercio electrónico de una manera segura para el intercambio de bienes y servicios de la población, se pueden citar:

- Generar un amplio y paradigmático proceso de modernización socialista del Estado, a efectos de unificar la gestión de la administración pública nacional mediante procesos

[10] http://www.mppp.gob.ve/wp-content/uploads/2013/09/Plan-de-la-Naci%C3%B3n-2001-2007.pdf
[11] http://www.mppp.gob.ve/wp-content/uploads/2013/09/Plan-de-la-Naci%C3%B3n-2007-2013.pdf
[12] http://www.mppp.gob.ve/wp-content/uploads/2013/09/Programa-Patria-2013-2019.pdf
[13] http://www.mppp.gob.ve/wp-content/uploads/2019/04/Plan-Patria-2019-2025.pdf
[14] https://www.ve.undp.org/content/venezuela/es/home/sustainable-development-goals.html

informáticos estandarizados, óptimos, transparentes, auditables e interoperables, Plan de la Patria 2025 orientados a derechos y servicios. Este objetivo considera los siguientes aspectos:

- Desarrollar la normativa legal del gobierno electrónico y demás componentes asociados a las tecnologías libres e información, a efectos de impulsar la participación ciudadana y la gestión pública eficiente y transparente.
- Desarrollar las bases legales y normativas para la democratización de la información, simplificación de trámites, así como el proceso de modernización del Estado y desarrollo del gobierno electrónico como sistema para facilitar la participación ciudadana y la gestión pública eficiente y transparente.
- Fortalecer el marco legal de la firma electrónica, su desarrollo y soporte técnico, la expansión de su uso, así como de la información digital.
- Desarrollar los mecanismos y nodos de acceso al gobierno electrónico, mecanismos de pagos de servicios, cédula y pasaporte electrónico, Carnet de la Patria, a efectos de ampliar la capacidad de acción directa del Estado, su máxima eficiencia y beneficio del pueblo.
- Crear, integrar, desarrollar, fortalecer y mantener una plataforma tecnológica y de sistemas de información automatizados, que incorporen las tecnologías libres, que sean integradas e interoperables, con documentación digital de calidad, que pueda ser accesible, a fin de evitar orfandad en el mantenimiento y escalabilidad de los mismos, sujetos a la mejora continua y completamente auditable, con el fin de labrar el camino de la modernización de la gestión pública.
- Generar un plan nacional de modernización tecnológica del Estado, con economía de escala, matriz energética y tecnológica, a efectos de actualizar la infraestructura y tecnologías libres en correlación con el apalancamiento industrial propio, transferencia tecnológica y sustitución de importaciones.
- Generar una plataforma de Estado para el desarrollo de tecnologías libres, formación, protección y desarrollo de los equipos humanos de informática, así como correlación con las unidades productivas del Estado, a efectos de impulsar y garantizar el soporte de la política de modernización tecnológica del Estado, integrando los distintos componentes existentes en los entes sobre esta materia.
- Fortalecer y expandir la política y programa Papel Cero, como optimización de trámites digitales de plena validez legal.
- Generar un marco de compatibilidad y diseño integral de los sistemas de registro e información de las políticas públicas, su seguimiento, en un desarrollo de un sistema automatizado y estandarizado, su interacción con otros sistemas de la administración pública, con el fin de optimizar las políticas públicas y evaluar la eficiencia de las mismas.
- Generar una plataforma y sistema integrado de información, simplificación de trámites, denuncia, con visión integral, del Estado venezolano.

- Fomentar el uso de la tecnología y el comercio electrónico seguro en el intercambio de servicios, materias primas, bienes semielaborados y productos finales, como aporte a la reducción de los eslabones de las cadenas de comercialización de bienes y servicios básicos para la población, contribuyendo al acercamiento entre productores y compradores, así como a nuevas formas organizativas que enfrenten el mercado especulativo.

Con lo anterior, se observa la existencia de un amplio cuerpo normativo y políticas públicas que promueven la incorporación de tecnologías para la concreción de actos administrativos, como

son los pagos de servicios, cédula de identidiad y pasaporte electrónico, lo que conlleva a la modernización tecnológica del Estado. Igualmente se incorpora, en el Plan Socialista 2019-2025, la firme intención de promover la comercialización de bienes y servicios básicos para la población, a través del uso del comercio electrónico y mecanismos de pagos de servicios en línea para así evitar el mercado especulativo actual.

2.2. DELITOS INFORMÁTICOS

En la actualidad la informatización y su desarrollo acelerado en medios digitales, permean las actividades diarias realizadas por las organizaciones del sector público y privado, así como también se encuentra presente en la investigación científica, en la producción industrial, en el sistema educativo, y en el ocio; es por ello que el uso de la informática se ha vuelto absolutamente necesario y muy conveniente desde el punto de vista económico. No obstante junto a sus grandes ventajas, comienzan a surgir aspectos negativos como los delitos informáticos y la transgresión de la norma jurídica, como consecuencia de interpretaciones inadecuadas o por la presencia acelerada de delincuentes informáticos que aplican estrategias novedosas para violar la seguridad digital de los ciudadanos.

Las TIC han creado nuevas posibilidades de delincuencia impensables, con consecuencias graves para el patrimonio de los ciudadanos. El fraude desde los computadores y redes sociales con ánimo de lucro, la violación de la privacidad, las ofertas engañosas, entre otros, son algunos de los procedimientos mediante los cuales es posible obtener grandes beneficios o causar importantes daños materiales a los ciudadanos.

Es por ello que abordar el delito informático requiere enfrentarlo con una visión amplia, ya que el mismo transciende ámbitos locales y las transgresiones pueden ser gestionadas desde cualquier parte del mundo. Es tal sentido es necesario visualizar el delito informático bajo distintos enfoques y entender las visiones de organismos como la Organización de Naciones Unidas e instancias nacionales como la Asamblea Nacional de Venezuela.

2.2.1. El delito informático en el ámbito internacional

La globalización y el uso de internet han marcado la evolución de los delitos tradicionales en el mundo, otorgándole características particulares, provenientes del uso de nuevas tecnologías, configurando nuevas tipologías delitos como la ciberdelincuencia, considerada hoy en día un problema universal. Desde la década de 1960 muchos países han reconocido como delitos ciertos actos relacionados con la informática, como el uso no autorizado de sistemas informáticos y la manipulación de datos electrónicos. Pero ha sido con la llegada de internet que las tecnologías globalizadas de la información y las comunicaciones han empezado a usarse para cometer delitos a escala internacional, en la forma de ciberdelincuencia que conocemos actualmente.[15]

La Organización para la Cooperación Económica (OCDE) reunida en París en 1983, definió al delito informático como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos[16] .

[15] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal
[16] https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

Las Naciones Unidas convienen en denominar este tipo de delito como ***Ciberdelincuencia,*** y reconoce que la ciberdelincuencia no es necesariamente un término jurídico técnico, sino más bien un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. Otros enfoques se centran en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos.

Las Naciones Unidas, consideran como supuestos de hecho para materializar delitos informáticos, "ciberdelincuencia" aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito. Algunos ejemplos de los primeros son los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos, como el acceso ilegal a datos o sistemas informáticos. Algunos ejemplos de los segundos son el uso de datos o sistemas informáticos para estafar, robar o causar daño a otras personas, así como los delitos relacionados con contenidos informáticos o de Internet, como los discursos de incitación al odio, la pornografía infantil, los delitos relacionados con la identidad y la venta por internet de mercancías ilícitas[17].

En abril del año 2017, se reunió en Viena, un grupo de expertos de las Naciones Unidas, encargado de realizar un estudio exhaustivo sobre el Delito Cibernético, se discutió ampliamente sobre la necesidad de establecer una normativa jurídica de carácter internacional, a continuación, se presenta el resumen de las deliberaciones del grupo de expertos[18]:

- La prevalencia y el papel que desempeñaban las tecnologías de la información y las comunicaciones en sus países y cómo esos factores están vinculados con la ciberdelincuencia. La mayoría de los expertos señalaron que el delito cibernético iba en aumento. También señalaron que existían vínculos concretos y complejos entre a) la prevalencia y el uso de las tecnologías, tanto en los Estados Miembros como a nivel regional y b) la evolución de la ciberdelincuencia. Se señaló que la difusión de las tecnologías y el problema conexo de la ciberdelincuencia también planteaban cuestiones relacionadas con la soberanía nacional, la independencia, la gobernanza, los derechos humanos y la cultura. Varios expertos mencionaron la necesidad de respetar la independencia soberana y la diversidad cultural, tanto al elaborar las definiciones de ciberdelincuencia como al estudiar las respuestas nacionales, transnacionales y mundiales ante ella.
- La necesidad de disponer de datos mundiales fiables y exhaustivos sobre la naturaleza y la extensión del problema. Entre las dificultades más importantes a ese respecto figuraban el muy amplio alcance del problema, la gama de fuentes de información que debían tenerse en cuenta y la necesidad de actualizar constantemente los datos y los análisis para reflejar su evolución dinámica. De acuerdo al UpTime Institute[19], para el año 2021 la mitad de todas las cargas de trabajo se ejecutarán fuera del centro de datos empresarial, ya sea en infraestructuras de centros de datos, en la nube, en multinubes o en el borde de la red. En consecuencia las amenazas a la ciberseguridad serán cada vez más sofisticadas y peligrosas en toda una superficie de ataque más amplia que ya no está contenida dentro de perímetros bien definidos y defendidos. En particular, a medida que las cargas de trabajo salen de las

[17] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Doha, 12 a 19 de abril de 2015
[18] rg/documents/organized-crime/cybercrime/Cybercrime-April-2017/UNODC-CCPCJ-EG-4-2017-2/V17 01129_S.pdf
[19] https://es.uptimeinstitute.com

instalaciones, existe el peligro de que la TI pierda visibilidad.

- La cuestión de los marcos jurídicos o de otro tipo para reglamentar y coordinar las respuestas internacionales al delito cibernético. Se expresaron opiniones divergentes. Algunos expertos sostuvieron que se necesitaba un nuevo instrumento jurídico internacional amplio y universal sobre el delito cibernético para establecer un consenso mundial sobre respuestas eficaces y proporcionar una base jurídica internacional clara para esas respuestas. Otros opinaron que sería más eficaz el uso de los regímenes jurídicos nacionales e internacionales existentes y enfoques más a medida para la cooperación caso por caso y la prestación de asistencia técnica.

- Varios expertos y representantes del sector privado destacaron la importancia de la prevención. Se mencionaron los medios técnicos, como el uso de aplicaciones de seguridad para proteger la integridad de los sistemas y los datos, y los medios sociales, como la educación de los usuarios de los sistemas y la inclusión de elementos relativos a la ciberdelincuencia en los programas escolares y universitarios pertinentes.
- Los expertos dijeron que era posible y deseable cooperar en un amplio conjunto de ámbitos específicos, como la prevención, la cooperación en las investigaciones, la reunión de información de carácter más general sobre la evolución de la delincuencia y sus tendencias y la formación de investigadores y expertos forenses en las nuevas tecnologías a medida que se creaban y comercializaban.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos[20]:

1. Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del

[20] https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas.

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados.

- **Sabotaje informático:** es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

  - Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
  - Gusanos: se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
  - Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su "detonación" puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

  - **Acceso no autorizado a servicios y sistemas informáticos**: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede

descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

- **Reproducción no autorizada de programas informáticos de protección legal**: ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Con lo anterior se observa que en el ámbito internacional existe un movimiento importante que busca identificar los riesgos de los delitos informáticos y diferenciar los distintos tipos de delitos, así como también crear conciencia sobre la necesidad de la prevención y educación de los ciudadanos como de los gobiernos.

2.2.2. El delito informático en Venezuela

En Venezuela la legislación que regula los delitos informáticos es de reciente data, fue publicada por la Asamblea Nacional el 30 de octubre de 2001, en Gaceta Oficial número 37.313, y denominada Ley Especial contra Delitos Informáticos[21] (LEDI). El Objeto de la Ley lo encontramos en su artículo 1:

"La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley".

La legislación especial relacionada con delitos informáticos surge, como consecuencia de regular conductas ilícitas nuevas, en la comisión de delitos ya previstos en el Código Penal, pero con la característica de un nuevo modus operandi, apoyado en el uso de tecnologías, convirtiéndolo en delitos emergentes, y dejando sin posibilidad de aplicación la regulación existente.

La LEDI, contempla en su articulado el principio de extraterritorialidad, relacionado a la sujeción de la jurisdicción nacional para quienes cometan los delitos tipificados en la norma, señala la LEDI, que cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros[22].

[21] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf
[22] Artículo 3 de la Ley Especial de Delitos Informáticos

2.2.2.1 Tipos de delitos informáticos

La LEDI, agrupa en cinco categorías los distintos tipos de delitos que en el área informática se pueden cometer:

1. Delitos Contra los Sistemas que Utilizan Tecnologías de Información.
2. Delitos Contra la Propiedad
3. Delitos Contra la Privacidad de las Personas y de las Comunicaciones
4. Delitos Contra Niños, Niñas o Adolescentes
5. Delitos Contra el Orden Económico

A continuación, se describen los distintos tipos de delitos informáticos previstos en la norma jurídica especial creada al efecto por la Asamblea Nacional de la República Bolivariana de Venezuela[23]:

TIPOS	CONCEPTUALIZACIÓN DEL DELITO	SANCIÓN
Delitos Contra los Sistemas que Utilizan Tecnologías de Información	**Acceso indebido**. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información.	Prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
	Sabotaje o daño a sistemas. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman.	Prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias
	Favorecimiento culposo del sabotaje o daño. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.	
	Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.	
	Posesión de equipos o prestación de servicios de sabotaje. Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
	Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de

[23] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf

		beneficio para sí o para otro.
	Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
Delitos Contra la Propiedad	**Hurto.** Quien, a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias
	Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno.	Prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.
	Obtención indebida de bienes o servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos,	Prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.
	Apropiación de tarjetas inteligentes o instrumentos análogos. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora,.	Prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias
	Posesión de equipo para falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias
Delitos Contra la Privacidad de las Personas y de las Comunicaciones	**Violación de la privacidad de la data o información de carácter personal**. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias

	Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
Delitos Contra Niños, Niñas o Adolescentes	**Difusión o exhibición de material pornográfico**. Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Exhibición pornográfica de niños o adolescentes. Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos.	Prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias
Delitos Contra el Orden Económico	**Apropiación de propiedad intelectual.** Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.	Prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.
	Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores.	Prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

2.2.2.2. Sanciones aplicables

Las sanciones por los delitos previstos en la LEDI, pueden ser principales y accesorias, y consisten en multas establecidas en unidades tributarias y/o penas privativas de libertad (prisión), las cuales oscilan desde 100 a 1000 unidades tributarias y prisión que va desde un (01) año a ocho (08) años de prisión, dicha sanción se encuentra prevista en la LEDI, en los artículos donde se tipifican los delitos.

2.2.2.3. Tendencias de los delitos informáticos en Venezuela

El presente apartado tiene como finalidad indagar sobre las tendencias y evolución de los delitos informáticos cometidos en Venezuela en el periodo 2002 al 2019, tomado como referencia lo establecido en La LEDI.

Año	Reporte de Caso	Fuente	Tipificación del Delito Informático
2002	El Paro Petrolero de 2002: Durante esa época, la situación política dio lugar a numerosas denuncias sobre ataques informáticos a PDVSA en donde se hablaba de robo de archivos electrónicos, información de cuentas en el exterior, entre otros. Fueron abiertos varios expedientes que muchos de ellos aún, siguen pendientes.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (bancario)

2005	En el año 2005 un SpyBanker capturo información de toda la banca venezolana, tomando fotografías de las pantallas de los empleados a medida que avanzaban en las acciones de tecleo, enviando los datos a destinos remotos. Las autoridades lograron detectar la computadora con la cual se cometió el delito, pero aún no hay capturas por este hecho.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (bancario)
2007	La División Contra Delitos Informáticos del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) develó que entre los primero seis delitos cometidos por medio de la tecnología se encontraba el "fraude electrónico" señalando un aumento considerable en el perfeccionamiento de los métodos y en el número de irregularidades cometidas. Esta instancia registró 170 denuncias de delitos informáticos durante el año.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (clonación de tarjetas de crédito y débito, obtención de información de cuentas bancarias)
	Delito de pornografía infantil en medios digitales.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Pornografía infantil
	Caso de un niño de tan solo 11 años de edad, residenciado en Barquisimeto, el cual logró estafar electrónicamente a un número no menor de 25 personas. Este pequeño trabajaba con la cuenta de su padre y cuando fue detenido señaló que hacía esto por simple diversión, dicha versión, aparentemente, fue creída por los cuerpos policiales ya que, al verificar la cuenta donde se depositaban los fondos se percataron de que el dinero estafado no había sido utilizado.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/ Nota: Según la División de Delitos informáticos para marzo del año 2007, se habían recibido 170 denuncias de delitos informáticos y el número actualizado no fue dado a conocer por falta de autorización del Ministerio del Interior y Justicia.	Fraude electrónico (este caso denota la vulnerabilidad de los sistemas de seguridad de las empresas financieras o bancos que operan en nuestro país)
2012	El CICPC capturó a varios empleados del Banco Bicentenario los cuales utilizaron información suministrada por clientes del banco para ingresar en sus cuentas de usuarios de CADIVI y apoderarse de un monto de 42 mil dólares.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude bancario
2017	La CICPC recibe a través de la división de delitos informáticos de 15 a 20 denuncias diarias relacionadas con estafas mediante ofertas engañosas publicadas en las redes sociales, en la mayoría de estos casos los compradores llegan a un acuerdo con el supuesto vendedor acordando fecha, hora y lugar para realizar la entrega, sin embargo este proceso no se concreta porque tan pronto, el estafador se percata que tiene el dinero, vía transferencia electrónica desparece o no contesta el teléfono.	http://www.correodelorinoco.gob.ve/cicpc-combate-proliferacion-delitos-redes-sociales/	Ofertas engañosas
	La segunda denuncia más frecuentes		Fraude

	que recibe la CICPC es la modalidad de fraude mediante el cambio o reemplazo de la tarjeta de débito o tarjeta de crédito por una falsa que no le pertenece a la víctima y que la realizan en cajeros automáticos o en los puntos de venta", informó la funcionaria del CICPC.		
2019	El inspector agregado del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), Alberto José Dugarte, reveló un incremento en los delitos informáticos en Venezuela, y resaltó que uno de los más frecuentes es el que se registra ante el acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos.	https://www.vtv.gob.ve/inspector-cicpc-acceso-indebido/	Ofertas engañosas
Septiembre 2019	Cicpc desmanteló dos laboratorios de pornografía en Caracas el director de la policía científica, C/G Douglas Rico, en compañía de funcionarios de la División Contra los Delitos Informáticos y División de Experticias Informáticas efectuaron un allanamiento en las instalaciones del edificio Ciencias Naturales ubicado en Caracas, donde operaba una red pornografía. Mediante labores de patrullaje informáticos, se determinó que estos operaban bajo un falso Call Center, donde al menos 70 personas, entre ellos 5 menores de edad, manejaban sitios web de pornografía, en el que ofrecían a diferentes costos dicho material, generando una de estas páginas en tan sólo un mes, 18 mil 500 dólares.	https://talcualdigital.com/index.php/2019/09/12/cicpc-desmantelo-dos-laboratorios-que-gestionaban-paginas-web-pornograficas-en-caracas/	Pornografía infantil
Agosto 2019	El inspector agregado del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), Alberto José Dugarte, reveló un incremento en los delitos informáticos en Venezuela, y resaltó que uno de los más frecuentes es el que se registra ante el acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos. https://vtv.gob.ve/wp-content/uploads/2019/07/CICPC.mp4 (Video)	http://www.ultimasnoticias.com.ve/noticias/sucesos/cicpc-combate-delitos-cometidos-en-redes/	Acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos.

Según se evidencia de los casos registrados o denuncias efectuadas ante la División de Delitos Informáticos del CICPC, el fraude y la oferta engañosa, incluidos dentro de los Delitos Contra la Propiedad y Delitos Contra el Orden Económico, son los que más se cometen en Venezuela, dada las condiciones políticas, económicas y sociales, muestran un crecimiento acelerado, igual importancia revisten los delitos contra los Niños, Niñas y Adolescentes, producto de la pornografía infantil. En este sentido en el 2017 la CICPC desarrolló campañas comunicacionales como la de "No te Enredes con las Redes", dirigida a más de mil doscientos alumnos pertenecientes a diez instituciones educativas de la Gran Caracas, con el objetivo de informar a

las niñas, niños y adolescentes en cuanto al uso adecuado, manejo y prevención de las diversas redes sociales.

2.2.2.4. Hechos delictivos en las redes sociales en Venezuela

Uno de los principales delitos informáticos que se cometen en Venezuela, a través de las redes sociales es el fraude, aunque el sabotaje y desmejoramiento de los servicios públicos también se presentan. Según CONATEL la delincuencia organizada de Venezuela encuentra en las redes sociales el lugar ideal para cometer delitos cibernéticos, el cual han venido aumentando desde el año 2012[24].

Los principales fraudes que se cometen a través de redes sociales en Venezuela son:

- **Transacciones comerciales** Es uno de los delitos virtuales más frecuentes en Venezuela. Los estafadores suelen ofrecer algún producto o servicio en un portal web o cuenta en redes sociales. El fraude ocurre, cuando el comprador, tras haber cancelado el importe del producto, nunca lo recibe. El principal fraude que se comete a través de las redes sociales deriva de las transacciones comerciales, y se materializa cuando el comprador, tras haber cancelado el importe del producto, nunca lo recibe.
- **El phishing** es un término informático que denota ingeniería social para adquirir información confidencial de forma fraudulenta. Por lo general el fraude es cometido con el envío de información engañosa, como el hacer creer que el usuario se ha ganado un premio y que para obtenerlo debe ingresar datos personales, como nombres y números de cuentas bancarias. El phishing también es reconocido como la suplantación de identidad en el medio fraudulento informático.
- **Catfish**, mejor conocido como identidad falsa. La implementación más común de este tipo de fraude es cuando las personas mienten sobre su identidad en la web con el fin de crear relaciones románticas y obtener beneficios económicos de esto. Las personas más vulnerables a este tipo de ataques cibernéticos son las niñas, niños y adolescentes, pues crean un vínculo con el estafador, quien, basándose en un sentimiento de amor, amistad o lástima, exige dinero a las víctimas.
- **Estafas por venta de divisas,** el delincuente usurpa la identidad de una persona en las redes sociales y oferta divisas, los estafados realizan la trasferencia del dinero y el delincuente desaparece. Posteriormente, los ciudadanos acuden al usurpado para exigir los montos equivalentes y el titular de la cuenta desconoce la operación[25].
- **Estafas por trámites para gestionar documentos oficiales,** los delincuentes ofrecen gestionar pasaportes y cédulas a través de las instituciones correspondientes, le exigen grandes cantidades de dinero a los ciudadanos para realizar el trámite, los ciudadanos transfieren los montos y después desaparecen los delincuentes[26].

También se pueden cometer a través de redes sociales delitos informáticos distintos al fraude enfocados en el sabotaje y desmejoramiento de los servicios públicos.

[24] http://www.conatel.gob.ve/el-fraude-y-las-redes-sociales-en-venezuela/
[25] https://twitter.com/leoperiodista/status/1186041936911781890?s=03
[26] https://twitter.com/noticias24/status/1190249675795968003

2.3.- ASPECTOS GENERALES DE LOS DELINCUENTES INFORMÁTICOS

2.3.1. Tipos de delincuentes informáticos

- **HACKER:**
  La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Los Hacker son capaces de crear sus propios softwares para entrar a los sistemas. Los Hacker son persona experta en materias informáticas, con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado "SHORT PANTS CRIMES", es decir, en pantalones cortos, su motivación no es la de causar daños sino burlar los sistemas de seguridad dispuestos.

- **CRACKER:**
  Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. Un Cracker siempre encuentran el modo de romper una protección debe conocer perfectamente las dos caras de la tecnología, aparte de programación y la parte física de la electrónica.

- **PHREAKER:**
  Es el especialista en telefonía (Cracker de teléfono). Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. Buscan burlar la protección de las redes públicas y corporativas de telefonía, con el fin de poner a prueba los conocimientos y habilidades, pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de "Hacking" a sus servidores.

- **LAMMERS:**
  Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

- **GURUS:**
  Son los maestros y enseñan a los futuros Hackers. Son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y se dedican a enseñar a o sacar de cualquier duda al joven iniciativo al tema. El guru no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimiento propio y solo enseña las técnicas más básicas.

- **BUCANEROS:**
  Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago, no existen en la Red, solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers. Son personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero sí de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial.

- **NEWBIE:**
  Son personas que empieza a partir de una WEB basada en Hacking. Inicialmente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a

veces fracasa en el intento.

- **TRASHING:**
  Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

2.3.2. Características de los delincuentes informáticos

Los delincuentes informáticos poseen características propias que los diferencian de los delincuentes comunes o de otra tipología de delitos. En la materialización del delito informático encontramos al Sujeto Activo, personas que cometen el delito informático y al Sujeto Pasivo, la víctima del delito, el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. En los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, entre otros, que usan sistemas automatizados de información, generalmente conectados a otros.

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Entre las principales características que presentan las personas que comenten delitos informáticos podemos señalar[27]:

- En general, son personas que no poseen antecedentes delictivos.
- La mayoría de sexo masculino.
- Actúan en forma individual.
- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación "hackers".
- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.
- En el caso de los "hackers", realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovechan la falta de rigor de las medidas de seguridad para obtener acceso o poder descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

[27] https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).
- Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia lo han catalogado como "delitos de cuello blanco", (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.)

2.3.2. Medidas de prevención y seguridad ante la delincuencia informática

Las estrategias de sensibilización orientadas a proteger a los consumidores contra el fraude en línea, por ejemplo, pueden requerir un enfoque distinto al de las estrategias de sensibilización en el ámbito de la protección de los niños en Internet. La información sobre las amenazas y las tendencias relacionadas con la ciberdelincuencia puede orientar también las respuestas en el ámbito de la investigación. La investigación de la venta de drogas ilícitas por internet, por ejemplo, requiere competencias y técnicas distintas de las que requiere el examen forense de dispositivos informáticos[28].

Entre las medidas de prevención, se encuentran unas prácticas que permiten mantener la seguridad de las cuentas de email:[29]

- Si te llegan mails de remitentes desconocidos con archivos adjuntos, no los abras.
- No hagas clic en los links que vienen en los correos de remitentes que no conoces
- No des información confidencial: Los bancos generalmente no piden a los clientes datos privados por email por lo que, si recibes uno que te solicita información confidencial, duda.
- Habilita el filtro anti-spam
- Créate diferentes cuentas de correo electrónico: De esta forma, en una de ellas podrás recibir promociones y otras informaciones de baja importancia y reservar otra para los mails más relevantes.
- Usa contraseñas seguras: Para garantizar la seguridad de la misma debes incluir mayúsculas, minúsculas, números y ser mayor a los diez caracteres.
- No accedas a tu cuenta desde equipos públicos
- Ten cuidado a la hora de usar redes públicas de Wi-Fi: Puede haber alguien que esté queriendo descifrar tu contraseña.
- Utiliza la opción de copia oculta: Será bueno que la uses cuando debas enviar un mismo material a varios destinatarios y para que no queden visibles las direcciones.
- Infórmate sobre seguridad informática

Existen otras medidas destinadas a prevenir los delitos informáticos, relacionada con la seguridad a implementar en el uso de equipos informáticos:[30]

Relacionados con su equipo informático:

- Actualice regularmente su sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web.

[28] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Doha, 12 a 19 de abril de 2015

[29] ¿De qué nos tenemos que cuidar?. Delito de espionaje informático, cómo se comete este delito informático. Disponible en: http://www.delitosinformaticos.com/10/2013/delitos/espionaje/delito-de-espionaje-informatico-como-se-comete-este-delito-informatico

[30] https://www.delitosinformaticos.info/consejos/sobre_seguridad_informatica.html

- Instale un Antivirus y actualícelo con frecuencia.
- Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
- Instale un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet.
- Es recomendable tener instalado en su equipo algún tipo de software anti-spyware, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.

Relacionados con la navegación en internet y la utilización del correo electrónico:

- Utilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente, además, que modifique sus contraseñas con frecuencia.
- Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad.
- Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos: deben empezar por https:// en lugar de http. En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.
- Sea cuidadoso al utilizar programas de acceso remoto. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.
- Ponga especial atención en el tratamiento de su correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:
- No abra mensajes de correo de remitentes desconocidos.
- Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
- No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos.
- Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

La Comisión Nacional de Telecomunicaciones de Venezuela (Conatel) ofrece anualmente charlas sobre los peligros y amenazas en Internet y las redes sociales, en donde recomiendan a las usuarias y usuarios medidas para evitar ser víctima del ciberfraude[31]:

- Cuida lo que publicas en Internet y en redes sociales.
- Todo lo que se hace en la red de redes deja rastros que pueden caer en manos de un ciberdelincuente.
- Nunca agregues contactos desconocidos.
- Evita ingresar correos electrónicos y números de teléfono al momento de crear o actualizar una red social.
- Configura el estado de seguridad de tus redes sociales.
- Utiliza contraseñas seguras, que contengan caracteres alfanuméricos, letras mayúsculas y minúsculas para mayor seguridad.
- Evita usar datos personales como nombres propios, de familiares o mascotas, apellidos,

[31] http://www.conatel.gob.ve/el-fraude-y-las-redes-sociales-en-venezuela/

fechas de nacimiento y nombres de usuarios en las contraseñas.
- Evita ingresar en enlaces sospechosos, puede ser un intento de fraude cibernético. Desconfía de promociones y concursos, sobre todo si son enviados por correo electrónico o aparecen en ventanas emergentes.
- Si vas a realizar compras en línea, hazlas en páginas con buena reputación y que sean reconocidas.

2.4.- ORGANISMOS PÚBLICOS PARA LA PREVENCIÓN Y CONTROL DE LOS DELITOS INFORMÁTICOS

El Estado venezolano, dispone de organismos para prevenir e investigar los crímenes informáticos y tecnológicos, los cuales analizan, preservan, presentan evidencias y apoyan las investigaciones judiciales, y prestan respaldo técnico al Ministerio Público y a otros organismos de seguridad.

- **División contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC):** el cual se encarga de la investigación y prevención de los delitos informáticos, al igual que el Ministerio Público. Las denuncias se pueden realizar a través del correo electrónico delitosinformaticos@cicpc.gob.ve, en Twitter @cicpcinformatco, en Instagram informaticoscicpc y a través del número telefónico 0212- 5640516, donde se dispone de personal capacitado para atender a los usuarios las 24 horas del día.

- **Superintendencia de Servicios de Certificación Electrónica** (SUSCERTE): es el organismo público del Estado venezolano responsable de gestionar, alertar y monitorear los incidentes informáticos, mediante el VenCERT y el CENIF, los cuales forman parte del Sistema Nacional de Seguridad Informática que establece la Ley de Infogobierno. La Ley de Mensaje de Datos y Firmas Electrónicas, promulgada en el año 2001, es otro aspecto nodal que el Gobierno Electrónico de Venezuela impulsa a través de SUSCERTE, organismo proveedor de la certificación de la firma electrónica y todo lo relacionado con este ámbito. Es el organismo encargado de coordinar e implementar el modelo jerárquico de la infraestructura Nacional de Certificación Electrónica. Acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC) y es el ente responsable de la gestión de la Autoridad de Certificación Raíz del Estado Venezolano. Así mismo, SUSCERTE es responsable del desarrollo, implementación, ejecución y seguimiento del Sistema Nacional de Seguridad Informática, a fin de crear las condiciones idóneas para el resguardo de la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos obtenidos y generados por el Poder Público.

- **Sistema Nacional de Gestión de Incidentes Telemático de la República Bolivariana de Venezuela**, cuyo objetivo es la prevención, detección y gestión de incidentes en los sistemas informáticos de la administración pública, así como asesorar a los responsables de las tecnologías de información y comunicación. Su creación responde a la necesidad estratégica de dotar al Estado de los mecanismos más adecuados para prevenir y actuar con efectividad ante los nuevos riesgos generados por el desarrollo de las nuevas tecnologías. De hecho, la seguridad de los sistemas y redes de información del sector público es un componente fundamental de la seguridad de un país.

- **Centro Nacional de Informática Forense.** El Centro Nacional de Informática Forense (CENIF), es un laboratorio de informática forense para la adquisición, análisis, preservación y presentación de las evidencias relacionadas a las tecnologías de información y

comunicación, con el objeto de prestar apoyo a los cuerpos de investigación judicial órganos y entres del Estado que así lo requieran.

3.- ANÁLISIS DE LA SITUACIÓN (FODA)

El análisis de la situación actual de los distintos tipos de delitos informáticos parte de la revisión del orden jurídico existente y la problemática que se ha venido suscitando como consecuencia de la evolución e incorporación en el quehacer diario del uso de nuevas tecnologías en la ejecución del comercio electrónico para el intercambio de servicios, materias primas, bienes semielaborados y productos finales. Esta nueva forma de comercializar por una parte reduce los eslabones de las cadenas de comercialización de bienes y servicios básicos para la población, pero también ha traído como consecuencia el acelerado incremento de delitos informáticos producto de conductas ilícitas nuevas, caracterizadas por modus operandi, apoyado en el uso de tecnologías, convirtiendo dichas conductas en delitos emergentes.

Se efectúo un análisis, e interpretación de los problemas o situaciones pertenecientes al entorno que rodea los delitos informáticos y los elementos intrínsecos que giran en torno a ellos, lo que permitió identificar las posibles estrategias para enfrentar la reciente aparición de conductas delictivas emergentes en la sociedad venezolana. Se identificaron fortalezas, oportunidades, debilidades y amenazas que rodean los delitos informáticos. Este análisis se realizó tanto en la fase de apreciación de la situación como en la de análisis y formulación de la estrategia con distintos grados de precisión.

A continuación se presenta el resultado de la construcción de la Matriz FODA.

MATRIZ FODA

FORTALEZAS

- Reciente publicación de Leyes, Decretos y Providencias que regulan los delitos informáticos.
- Incorporación en las políticas públicas del país (Plan de la Patria 2019-2025) de líneas de acción para fortalecer el comercio electrónico.y utilizar las TIC como un bien público.
- Diseño y creación de estructuras especializadas en la investigación de los delitos informáticos tales como la Superintendencia de Servicios de Certificación Electrónica (Suscerte), el Sistema Nacional de Gestión de Incidentes Temáticos (VenCert).
- Asistencia jurídica a las víctimas de delitos informáticos a través de la puesta en marcha de la División contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC)

OPORTUNIDADES

- Acuerdos por parte de organismos internacionales Policía Criminal (INTERPOL), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) para armonizar, y legislar mediante tratados internacionales los delitos informáticos y tratamiento de los delincuentes.
- Crecimiento acelerado del Comercio Electrónico a nivel nacional y mundial.
- Rápido crecimiento de Internet y de la tecnología informática para mayor acceso a servicios esenciales como gobernanza electrónica, y comercio electrónico.
- Alianzas para prevenir y combatir los delitos informáticos (ciberdelincuencia), a nivel nacional o multilateral.
- Inicio de alianzas para llegar a un consenso mundial sobre los datos que permita compartir y emplear la tecnología y la innovación para el bien común, lo que incluye la posible creación de una red mundial de innovación en materia de datos.
- Protocolos y herramientas para la prevención de los delitos informáticos y las buenas prácticas en los medios digitales.

DEBILIDADES

- Poca divulgación de las Leyes, Decretos y Políticas Públicas que regulan los delitos informáticos en Venezuela
- Poca publicidad de las leyes y decretos relacionados con Derechos de Internet establecidos por la Asamblea Nacional, Asamblea Nacional Constituyente y el Ejecutivos Nacional (órganos enfrentados)
- Ausencia de estrategias comunicacionales para alertar sobre los delitos informáticos
- Escasa divulgación de las distintas sanciones y responsabilidades que acarrean cometer delitos informáticos
- Poca información sobre medidas preventivas para evitar el fraude y promover buenas prácticas
- Poca confianza de los ciudadanos para realizar denuncias sobre delitos informáticos y desconocimiento de las sanciones y Derechos de internet
- Incremento de prácticas de ingeniería social que promueven ataques cibernéticos e ingeniería social
- Desconocimiento sobre el uso y manejo de las redes sociales y medios digitales
- Poca información sobre la población más vulnerable que es afectada por los delitos informáticos
- Poca información sobre la cantidad de delitos informáticos, discriminados por tipos de redes sociales (twitter, WhatsApp, etc.)
- Desconocimiento de estadísticas oportunas, fiables y accesibles que revelen datos relacionados con los fraudes cometidos en las redes sociales

AMENAZAS

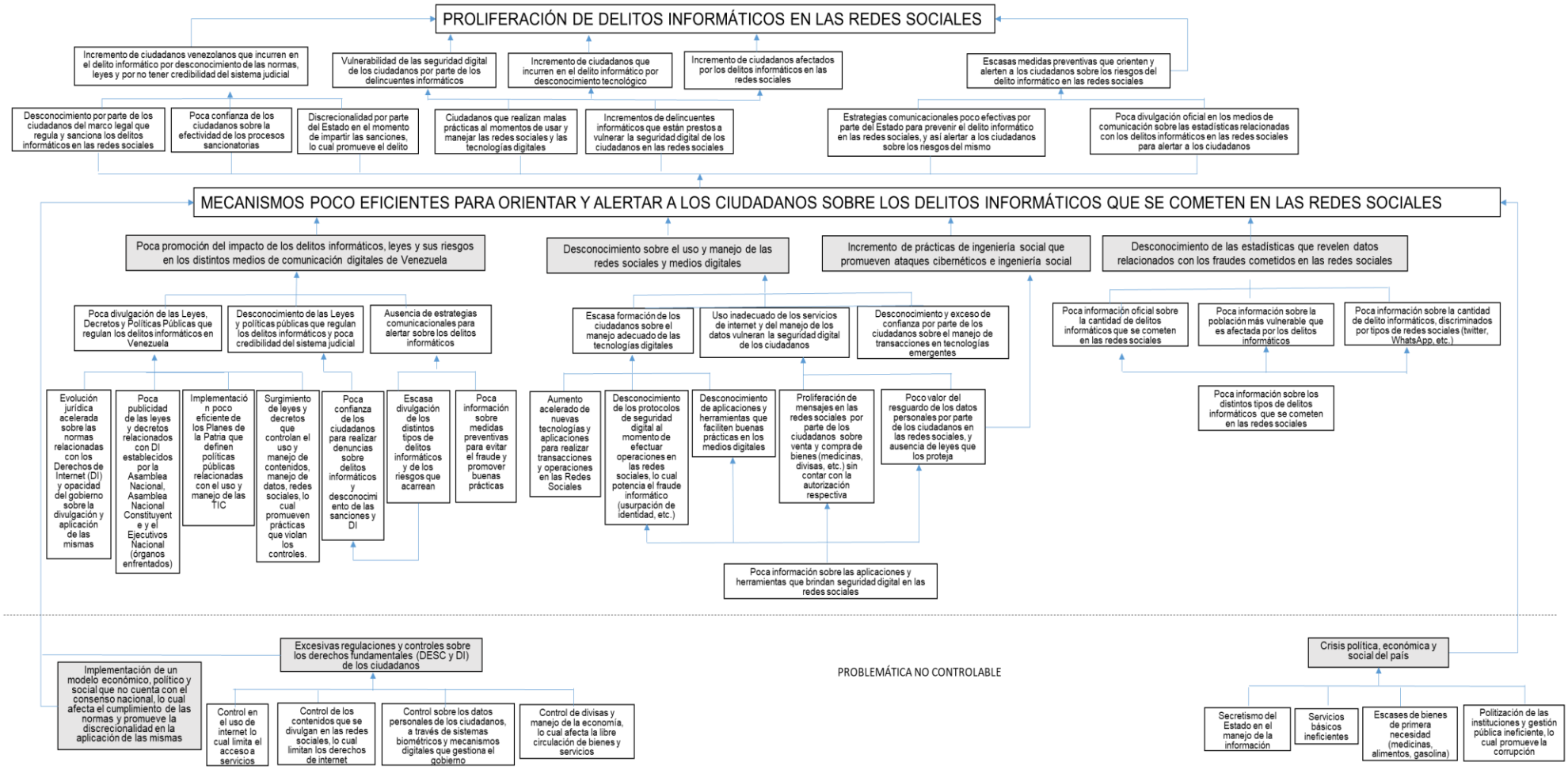
- Implementación de un modelo económico, político y social que no cuenta con el consenso nacional, lo cual afecta el cumplimiento de las normas y promueve la discrecionalidad en la aplicación de las mismas
- Surgimiento de leyes y decretos que controlan el uso y manejo de contenidos, manejo de datos, redes sociales, lo cual promueven prácticas que violan los controles.
- Altos niveles de impunidad por parte de los organismos encargados de sancionar los delitos informáticos.
- Excesivas regulaciones y controles sobre los derechos fundamentales (Derechos de acceso a la información) de los ciudadanos
- Control en el uso de internet lo cual limita el acceso a servicios
- Control sobre los datos personales de los ciudadanos, a través de sistemas biométricos y mecanismos digitales que gestiona el gobierno
- Control de los contenidos que se divulgan en las redes sociales, lo cual limitan los derechos de internet
- Fallas de los servicios públicos (electricidad, telecomunicaciones, etc.) necesarios para el uso adecuado de tecnologías de información

ANÁLISIS FODA	Fortalezas (F)	Debilidades (D)
	• Reciente publicación de Leyes, Decretos y Providencias que regulan los delitos informáticos. • Incorporación en las políticas públicas del país (Plan de la Patria 2019-2025) de líneas de acción para fortalecer el comercio electrónico. • Diseño y creación de estructuras especializadas en la investigación de los delitos informáticos tales como la Superintendencia de Servicios de Certificación Electrónica (Suscerte), el Sistema Nacional de Gestión de Incidentes Temáticos (VenCert). • Asistencia jurídica a las víctimas de delitos informáticos a través de la puesta en marcha de la División contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC)	• Poca divulgación de las Leyes, Decretos y Políticas Públicas que regulan los delitos informáticos en Venezuela • Poca publicidad de las leyes y decretos relacionados con Derechos de Internet establecidos por la Asamblea Nacional, Asamblea Nacional Constituyente y el Ejecutivos Nacional (órganos enfrentados) • Ausencia de estrategias comunicacionales para alertar sobre los delitos informáticos • Escasa divulgación de las distintas sanciones y responsabilidades que acarrean cometer delitos informáticos • Poca información sobre medidas preventivas para evitar el fraude y promover buenas prácticas • Poca confianza de los ciudadanos para realizar denuncias sobre delitos informáticos y desconocimiento de las sanciones y Derechos de internet • Incremento de prácticas de ingeniería social que promueven ataques cibernéticos e ingeniería social • Desconocimiento sobre el uso y manejo de las redes sociales y medios digitales • Poca información sobre la población más vulnerable que es afectada por los delitos informáticos • Poca información sobre la cantidad de delitos informáticos, discriminados por tipos de redes sociales (twitter, WhatsApp, etc.) • Desconocimiento de estadísticas oportunas, fiables y accesibles que revelen datos relacionados con los fraudes cometidos en las redes sociales
Oportunidades (O)	**Estrategia (FO)**	**Estrategia (DO)**
• Acuerdos por parte de organismos internacionales Policía Criminal (INTERPOL), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) para armonizar, y legislar mediante tratados internacionales los delitos informáticos y tratamiento de los delincuentes. • Crecimiento acelerado del Comercio Electrónico a nivel nacional y mundial. • Rápido crecimiento de Internet y de la tecnología informática para mayor acceso a servicios esenciales como gobernanza electrónica, y comercio	Promover alianzas internacionales en materia de regulación, control y prevención de delitos informáticos, aprovechando, por una parte, el rápido crecimiento de Internet y de la tecnología informática, la globalización en la realización de transacciones económicas, y el reconocimiento por parte del Gobierno Nacional, al incorporar como política pública en el plan de la patria 2019-2025, el fortalecimiento del comercio.	Impulsar estrategias comunicacionales para: alertar sobre los delitos informáticos, dar a conocer las leyes recientemente promulgadas por el País, educar sobre el uso y manejo de las redes sociales y medios digitales, medidas preventivas para evitar el fraude y promover buenas prácticas, apoyándose en las políticas internacionales que actualmente se desarrollan en materia de delitos informáticos o ciberdelitos.

electrónico. • Alianzas para prevenir y combatir los delitos informáticos (ciberdelincuencia), a nivel nacional o multilateral. • Inicio de alianzas para llegar a un consenso mundial sobre los datos que permita compartir y emplear la tecnología y la innovación para el bien común, lo que incluye la posible creación de una red mundial de innovación en materia de datos. • Protocolos y herramientas para la prevención de los delitos informáticos y las buenas prácticas en los medios digitales.		
Amenazas(A)	**Estrategias (FA)**	**Estrategias (DA)**
• Implementación de un modelo económico, político y social que no cuenta con el consenso nacional, lo cual afecta el cumplimiento de las normas y promueve la discrecionalidad en la aplicación de las mismas • Surgimiento de leyes y decretos que controlan el uso y manejo de contenidos, manejo de datos, redes sociales, lo cual promueven prácticas que violan los controles. • Altos niveles de impunidad por parte de los organismos encargados de sancionar los delitos informáticos. • Excesivas regulaciones y controles sobre los derechos fundamentales (Derechos de acceso a la información) de los ciudadanos • Control en el uso de internet lo cual limita el acceso a servicios • Control sobre los datos personales de los ciudadanos, a través de sistemas biométricos y mecanismos digitales que gestiona el gobierno • Control de los contenidos que se divulgan en las redes sociales, lo cual limitan los derechos de internet • Fallas de los servicios públicos (electricidad, telecomunicaciones, etc.) necesarios para el uso adecuado de tecnologías de información	Divulgar el marco jurídico existente para empoderar a los ciudadanos sobre los medios de defensa que posee al momento de ser víctima de un delito informático, así como también dar a conocer los distintos entes encargados de tramitar y sustanciar los hechos delictivos ante la División contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC).	Generar campañas de divulgación de las Leyes, Decretos y Políticas Públicas que regulan los delitos informáticos en Venezuela, a través de estrategias comunicacionales para alertar sobre los delitos informáticos, donde se indiquen las distintas sanciones y responsabilidades que acarrean cometer dichos delitos, divulgar medidas preventivas para evitar el fraude y promover buenas prácticas, y así generar confianza en los ciudadanos para que realicen denuncias al momento de ser víctimas de delitos informáticos.

4.- ANÁLISIS DEL PROBLEMA

4.1.- ESQUEMA GENERAL DEL ARBOL DEL PROBLEMA



4.2.- EXPLICACION DEL ARBOL DEL PROBLEMA

El árbol del problema considera los aspectos generales que inciden en la proliferación de los delitos informáticos en las redes sociales en Venezuela.

Es por ello que la sensibilización y orientación de los ciudadanos venezolanos sobre los riesgos que se corren al utilizar inadecuadamente las redes sociales, puede representar una vía para minimizar los delitos informáticos; particularmente aquellos relacionados con el fraude y las ofertas engañosas, los cuales en Venezuela tienen mayor auge, producto de la crisis económica, políticas y social.

Es importante resaltar que en el análisis del problema crítico, se hizo mayor énfasis en los aspectos relacionados con la promoción y divulgación del marco legal venezolano que considera el delito informático, con la formación de los ciudadanos sobre el uso y manejo de las redes sociales, la implementación de prácticas que prevengan los efectos de la ingeniería social y la difusión de estadísticas del delito informático en las redes sociales.

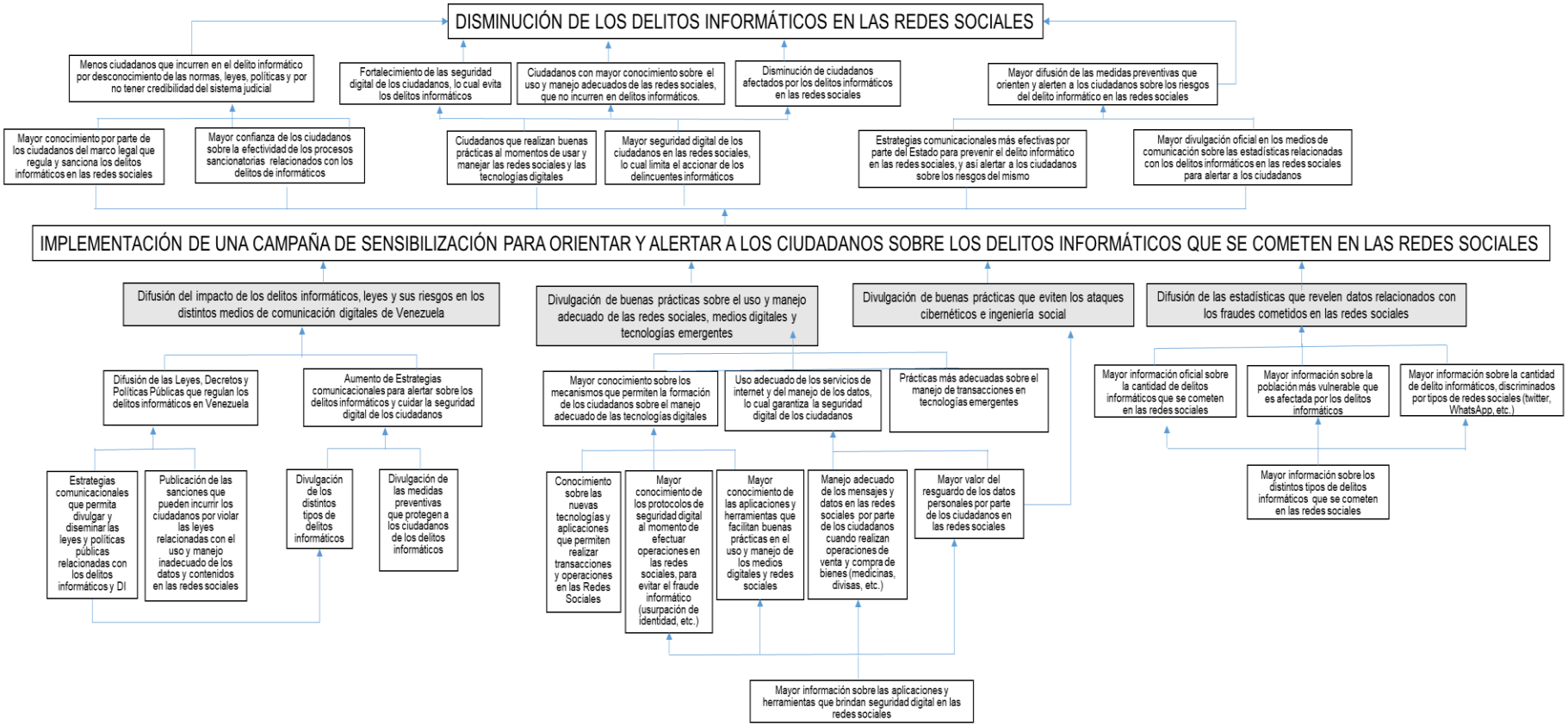
En tal sentido, se determinó que el problema crítico detectado es la presencia de "Mecanismos poco eficientes para orientar y alertar a los ciudadanos sobre los delitos informáticos que se comenten en las redes sociales, el cual es generado por las siguientes causas: a) poca divulgación de las leyes y sus riesgos en los distintos medios digitales de Venezuela, b) desconocimiento por parte de los ciudadanos sobre el uso y manejo de las redes sociales, c) incremento de prácticas de ingeniería social que promueven ataques cibernéticos, y d) desconocimiento de estadísticas relacionadas con los delitos informáticos en las redes sociales.

Estas causas traen como consecuencia el incremento de ciudadanos que incurren en los delitos informáticos, vulnerabilidad de la seguridad digital de los venezolanos por parte de los delincuentes informáticos, incremento de ciudadanos que comenten delitos informáticos por desconocimiento de las tecnologías, incremento afectados y ausencia de estadísticas que permitan aplicar medidas preventivas.

Con lo anterior se determina que al no implementar medidas preventivas y de sensibilización sobre la problemática, la proliferación de los delitos informáticos será mayor y en un mayor número de ciudadanos serán afectados.

5.- ANÁLISIS DEL OBJETIVO

5.1.- ESQUEMA GENERAL DEL ARBOL DEL OBJETIVO



5.2.- EXPLICACION DEL ARBOL DE OBJETIVOS - OPERATIVIDAD

Tomando como referencia las reflexiones realizadas en el árbol del problema surgen potenciales soluciones que permiten revertir las causas que generan el problema crítico, considerado en el estudio.

Estas soluciones se enfocan en buscar alternativas para implementar estrategias comunicacionales adecuadas que sensibilicen a los ciudadanos sobre los riesgos de utilizar inadecuadamente las redes sociales, así como también realizar buenas prácticas sobre el uso y manejo de las tecnologías. Adicionalmente se busca evaluar mecanismo para prevenir acciones que los delincuentes informáticos realizan y que afectan la seguridad digital de los ciudadanos.

Partiendo de lo expuesto anteriormente se determina que uno de los mecanismos adecuados para gestionar esta problemática es la implementación de una campaña de sensibilización para alertar a los ciudadanos sobre los riesgos de los delitos informáticos que pueden violar derechos fundamentales de los ciudadanos y afectar su patrimonio y accionar moral.

Segundo informe de avance del proyecto[32]:

ESTRATEGIA COMUNICACIONAL

7 diciembre de 2019

Proyecto aprobado por el Comité de Selección del Fondo de Respuesta Rápida (FRR) de Derechos Digitales en el mes de septiembre de 2019.

CONTENIDO

INTRODUCCIÓN

Este documento tiene como finalidad presentar el segundo informe de avance del proyecto denominado: "Desenmascara el delito informático, no al fraude en las redes sociales", que representa una campaña para orientar a los ciudadanos venezolanos sobre los riesgos que corren al realizar prácticas inadecuadas en las redes sociales, ya que los exponen al fraude y a la violación de su seguridad digital.

El informe comprende la estrategia y el plan de comunicación desglosado en la problemática, los objetivos de la campaña, la audiencia a quien va dirigida, la identidad de la campaña y el diseño del mensaje, las líneas de acción, el plan de contenidos y el plan de difusión, así como los indicadores para medir los resultados de la campaña.

1.- CONOCER LA PROBLEMÁTICA

Actualmente, la crisis económica, política y social que se vive en Venezuela ha traído como consecuencia un empobrecimiento acelerado de la población producto de la escasez de bienes y servicios, así como de la paralización del aparato productivo del país; lo cual ha llevado a los ciudadanos a buscar medios alternativos para solventar las necesidades básicas en lo que respecta a alimentación y medicamentos. Igualmente, la dificultad para adquirir divisas, gestionar documentos oficiales (pasaportes, partidas de nacimiento, otros) y realizar remesas ha encaminado a los ciudadanos a buscar gestores en medios digitales para facilitar estos tipos de trámites. Entre los medios alternativos empleados se encuentran el uso de las redes sociales para realizar gestiones oficiales y transacciones económicas sin una regulación y control por parte del Estado, lo cual expone a los ciudadanos a ser víctimas de delitos informáticos.

Para conocer y entender la problemática, se realizó una investigación documental del marco legal venezolano relacionado con el delito informático, así como también se determinaron algunos aspectos vinculados con el uso y manejo de las redes sociales por parte de los ciudadanos, prácticas de ingeniería social que promueven ataques cibernéticos, y el manejo de estadísticas sobre casos de delitos informáticos, población afectada, entre otros. De igual manera, se realizó un análisis de las potenciales causas y consecuencias que originan una serie problemas críticos, que promueven significativamente el delito informático. Este análisis permitió determinar los objetivos y las posibles soluciones a ésta problemática, insumo necesario para el diseño de la campaña de orientación y sensibilización sobre el delito informático en las redes sociales.

Del análisis situacional, primer informe de avance del proyecto entregado el 07/11/2019, se concluyó que el problema crítico detectado es la presencia de mecanismos poco eficientes para orientar y alertar a los ciudadanos sobre los delitos informáticos que se comenten en las redes sociales, el cual es generado por las siguientes causas: a) incremento de prácticas de ingeniería social que promueven ataques cibernéticos, b) desconocimiento por parte de los ciudadanos sobre el uso y manejo de las redes sociales, c) poca divulgación de las leyes y sus riesgos en los distintos medios digitales de Venezuela y d) desconocimiento de estadísticas relacionadas con los delitos informáticos en las redes sociales.

Estas causas traen como consecuencia el incremento de ciudadanos que incurren en los delitos informáticos, vulnerabilidad de la seguridad digital de los venezolanos por parte de los delincuentes informáticos, incremento de ciudadanos que comenten delitos informáticos por desconocimiento en el uso de las tecnologías de información, incremento de afectados y ausencia de estadísticas que permitan aplicar medidas preventivas. De lo anterior se puede inferir que al no implementarse medidas preventivas y de sensibilización sobre la problemática, la proliferación de los delitos informáticos será mayor y crecerá proporcionalmente el número de ciudadanos afectados.

Partiendo de lo expuesto anteriormente se determinó que uno de los mecanismos adecuados para gestionar la problemática, es la implementación de una campaña de sensibilización para alertar y orientar a los ciudadanos sobre los riesgos de los delitos informáticos que pueden violar los derechos fundamentales de los ciudadanos y afectar su patrimonio y accionar moral. De igual manera, las soluciones se enfocan en buscar alternativas para implementar estrategias comunicacionales adecuadas que sensibilicen a los ciudadanos sobre los riesgos de utilizar inadecuadamente las redes sociales, así como también realizar buenas prácticas sobre el uso y manejo de las tecnologías de información. La campaña "Desenmascara el delito informático, no al fraude en las redes sociales" pretende dar respuesta a la problemática.

2.- TÍTULO

Campaña comunicacional: "Desenmascara el delito informático, no al fraude en las redes sociales".

3.- OBJETIVOS DE LA ESTRATEGIA COMUNICACIONAL

3.1.- OBJETIVO GENERAL

El objetivo general de esta campaña comunicacional, es crear conciencia en los ciudadanos sobre los delitos informáticos que violan sus derechos fundamentales y afectan su patrimonio y accionar moral.

3.2.- OBJETIVOS ESPECÍFICOS

a. Alertar a los ciudadanos sobre los delitos informáticos que se cometen en las redes sociales para evitar que sean víctimas.
b. Orientar sobre el uso y manejo adecuado de las redes sociales, medios digitales y tecnologías de información emergentes.
c. Orientar sobre medidas preventivas para evitar el fraude y promover buenas prácticas.
d. Divulgar el marco jurídico (leyes, decretos y políticas públicas) que regulan los delitos informáticos en Venezuela para empoderar a los ciudadanos sobre los medios de defensa que posee al momento de ser víctima de un delito informático.
e. Informar sobre los distintos entes encargados de tramitar y sustanciar los hechos delictivos para generar confianza, y que los ciudadanos puedan

denunciar al momento de ser víctimas de delitos informáticos.

Observamos que la estrategia comunicacional tiene cuatro finalidades para enfrentar la problemática, en función del público a quien va dirigida para: alertar, luego orientar, concientizar e informar, lo cual se verá con mayor detalle en la descripción del mensaje.

4.- PÚBLICO RECEPTOR

El grupo de enfoque central para el mensaje de la campaña "Desenmascara el delito informático, no al fraude en las redes sociales", serán los adultos mayores y los adolescentes esencialmente, conscientes de que la campaña no hace distinción en la canalización del mensaje por sectores de edad, es decir, el alcance de la campaña será la **ciudadanía en general**, solo que los elementos semióticos principales están enfocados en captar la audiencia con mayor riesgo de exposición al delito informático, tales como adolescentes y jóvenes (entre 12 a 25 años) y adultos (50 a 70 años).

5.- MENSAJE

El análisis situacional, los objetivos de la campaña y el público receptor, permiten centrar el foco en el ámbito propiamente dicho de la estrategia comunicacional que es el mensaje.

La estrategia que se implementará está orientada a la concientización y la información. Por lo tanto, el mensaje debe alcanzar la exactitud de su concreción en función de su finalidad, con respecto al público a quien va dirigido, y conseguir su máxima credibilidad.

El tono del mensaje de la campaña será de **Alerta/Advertencia** Se buscará comunicar acciones que prevengan situaciones posibles de delitos informáticos enfocadas en el público audiencia. Este **Alerta** se expresará en toda la campaña *a dos tiempos*: primero en la señalización e identificación de la amenaza (el delincuente o el delito digital), y segundo en la advertencia sobre la acción – orientación - que se ofrecerá a la audiencia para evitar ser víctima del delito.

Es importante señalar que se evitará usar un tono Infantil/Gracioso/Relajado ni tampoco Informativo/Serio/Sin Emociones en la aplicación del concepto a las piezas comunicacionales centrales. Sin embargo, en algunos casos se tendrán piezas más informativas y explicativas, que permitan apoyar el mensaje inicial de **Alerta**.

5.1.- TEMATICA – DISEÑO DEL MENSAJE

Tal y como se observó en el análisis situacional, la temática de los delitos informáticos es muy amplia, toca distintas aristas y genera una variedad de tipos de delitos, que a su vez, dependen de las características regionales y circunstanciales de cada grupo o población.

Venezuela, en la actualidad, presenta una realidad de emergencia que llega incluso a poner en riesgo los Derechos Humanos Fundamentales, un fenómeno social que pone en situación extrema a la mayoría de la población con respecto al acceso a

bienes y servicios. El venezolano se ve en la necesidad de adquirir y vender divisas internacionales para poder estabilizar el proceso de intercambio comercial, y de comprar bienes de primera necesidad a través de las redes sociales. Es entonces cuando ***el delincuente digital actúa cometiendo fraude y otros actos diversos para lograr engañar a las víctimas en una transacción comercial***. Éste tipo de sucesos ocurre con una frecuencia tal que ha llegado a un punto de emergencia.

El proyecto pretende proponer soluciones a través de una campaña de concientización, que debe delimitar ciertos aspectos fundamentales de especificidad de la audiencia a quien va dirigida, para aumentar las probabilidades de afectar efectivamente a la población con la temática de delitos informáticos.

La campaña estará enfocada en Venezuela, país con características socio-económicas, políticas, legislativas, tecnológicas y culturales muy particulares, podría decirse que únicas, en el mundo actual y que remiten a ese *estado de emergencia,* ya señalado, en el tema de los delitos digitales. Del análisis situacional y otras investigaciones documentales, se pueden determinar los actos delictivos digitales que cubrirá la campaña, relacionados con las características demográficas propias de los venezolanos, como:

- **Fraude** y falsificación informática
- Acceso ilegal a un sistema informático
- Acceso ilegal, intercepción o adquisición de datos informáticos
- Interferencia ilegal de datos o sistemas
- Delitos informáticos, relacionados con la identidad

Si bien existen otros delitos digitales importantes, éstos no quedan dentro de la situación de emergencia que da origen a la campaña. Además, en otro sentido, una campaña debe delimitarse lo más posible hacia el conjunto de problemas interconectados a los que puede llegar un proceso de comunicación, sobre todo los de concientización.

Las piezas esenciales de descripción del Tema/Mensaje que comunicará en la campaña serán las siguientes:

- Tema/Situación General = Delitos Digitales en Venezuela
- Tema/Situación Específica = ***En Venezuela se cometen muchos Fraudes, delitos de identidad y acceso a datos privados durante el proceso de intercambio de divisas y compra de bienes de primera necesidad, de difícil acceso***.

5.2 – IDENTIDAD DE LA CAMPAÑA

a) Título: Los Descarados

b) Líneas fundacionales de la campaña.

En un mundo sin ley, donde el dinero y artículos de primera necesidad, como alimentos y medicinas, se han vuelto difíciles de conseguir, y la desolación ha alcanzado el corazón de muchos, un grupo de maleantes digitales ha aprovechado estas circunstancias para desatar una ola de delitos sobre los usuarios de la Internet

en Venezuela. Debemos estar atentos y evitar ser víctima de los Descarados.

Estas son las líneas fundacionales de la campaña. Contiene las palabras clave para los intereses descritos previamente y ofrece el rasgo de identidad referido al "ámbito" sobre el cual se ejecutarán los símbolos y subsecuentes contenidos. Advierte también la línea estética gráfica que seguirá el diseño de los símbolos visuales: ***Se Busca-Estafador-Digital.*** Esta frase se usa como descripción básica y pública, para los contactos y alianzas necesarias en la aplicación de la estrategia y de ella se derivan otros contenidos claves en las estructuras de redes (*taglines, hasthags, links*, etc.).

c) Descripción Base – Argumentación.

Los Descarados será una campaña de **Alerta - Advertencia**, fundamentada en el estado de emergencia de la sociedad venezolana, con respecto al alto índice de delitos digitales cometidos en torno al fraude y ofertas engañosas.

La idea está basada en ambientar una mezcla estética del símbolo colectivo donde ***"Se Buscan"*** forajidos y delincuentes que roban el dinero en un pueblo *sin ley*, donde las autoridades pueden ayudarte, pero también pueden estar corruptas por lo que tienes que saber EVITAR -antes que nada- que el delito se cometa contra "*ti mismo, como individuo*".

Se puede apreciar la traza de esta estética en el imaginario colectivo desde las películas del *viejo oeste*, pasando por los *gánsteres*, los retratos hablados y más recientemente los espías y *hackers*. La identidad tendrá los rasgos venezolanos de reconocimiento en la propiedad de los símbolos. *Los Descarados* busca los rasgos del estafador latino, el embaucador, el tracalero, el delincuente o maleante actual, para anclar ambas estéticas en una y obtener una identidad propia. Sin embargo, podría lograrse que esta identidad permita que la campaña se replique en otros países latinoamericanos.

d) Estética Base: Se Busca-Estafador-Digital

Aquí es importante recordar el *Tono*, que será de Alerta y en un marco editorial de Emergencia, es decir, se evitará caer en rasgos estéticos que remitan a lo Infantil-Gracioso- Relajado, que es uno de los aspectos más resaltantes en otras campañas (por lo cual perderíamos identidad y coherencia) así como también se evitarán rasgos Informativos –Serios – Descriptivos, ya que para establecer el estado de emergencia y decisión autónoma posterior, es necesario trabajar las emociones en las personas que reciben el mensaje.

Los símbolos están enfocados en el **Alerta**, en el estado de tensión inicial que advierta de manera emocional e individual, sobre la responsabilidad que se tiene al evitar ser víctima de un crimen. Es por ello que la estética *"Estafador Buscado"* vuelve a tener sentido y el usuario debe ver el cartel de "SE BUSCA", reconocer al delincuente/delito y un posible curso de acciones (buenas prácticas) que puede ejecutar, como "gente normal", para no caer víctima del fraude, robo de datos, robo de identidad, acceso a cuentas privadas, etc.

Como consecuencia, "*Los Descarados"* se muestra ante el público como tres delincuentes, tracaleros y estafadores que acechan a un pueblo imaginario llamado *Internetzuela,* o *Internet en Venezuela,* cada uno especializado y enfocado en

Advertir – Alertar sobre su existencia, el *historial de crímenes* que ha cometido y la forma en que se puede *evitar ser víctimas.* Se piensa, en principio, hacer similitudes visuales en las que estos criminales usen los teléfonos celulares y otros aparatos electrónicos como armas (revolver, dinamita, pólvora, bombas, virus, etc.).

La Banda de los Descarados estará formada por tres delincuentes:

- ***Arrobaldo:*** *experto en robo de identidad;*
- ***Zamureta:*** *delincuente reconocida por el robo de datos;*
- ***Wisin Wasap:*** *miente y engaña, construye trampas digitales;*

5.3.- LÍNEAS DE ACCIÓN DE LA CAMPAÑA

1) Imágenes para compartir por redes sociales.

Consiste en imágenes que contengan la identidad base de la campaña, que darán la información esencial respecto a las acciones que se pueden tomar para evitar los delitos digitales. Estas imágenes estarán adaptadas para funcionar en todos los entornos digitales y redes populares para facilitar su distribución masiva.

2) *Stickers*, Emoticones, *GIFs* para responder ante posibles delitos en redes.

Las redes de mensajería instantánea, principalmente *WhatsApp,* pareciera que son los ambientes con mayor riesgo de presentar/ocurrir intentos de fraude o robo. Razón por la que la campaña contemplará elementos comunes visuales que permitan responder, pedir aclaratoria, advertir de cualquier incomodidad respecto a una acción o conversación que pueda dejar vulnerable al usuario.

3) Videos Cortos, *GIFs* que permitan la descripción efectiva de la campaña.

Si bien las imágenes, posters digitales, Stickers y demás elementos son la vanguardia de la campaña, existirá una línea media de respaldo que permitirá la extensión del mensaje y su comprensión de una forma más detallada. Estos vídeos cortos pretenden dar descripciones visuales detalladas de las situaciones de delito y de sus posibles soluciones, además de contener el canal "auditivo" como respaldo del mensaje y refuerzo de la identidad de la campaña.

4) *Sitio Web* para información y contenido detallado.

Se considera necesario contar con la presencia de un espacio web (sitio web, blog, *wordpress*, etc.) que funja como **vitrina digital,** que permita congregar y ordenar todos los elementos informáticos de la campaña, así como poder detallarla a sus factores más especializados y posibilidad de extender la información. En este espacio se podrá presentar el marco legal y referencias a buenas prácticas en el uso de las tecnologías y redes digitales. Pudiera servir como receptor de experiencias y testimonios que permitan aumentar la eficiencia de los sistemas de alerta ante los delitos digitales.

Es importante señalar, con respecto al contenido de las piezas que estarán presentes en las diferentes líneas de acción, que no se pretende presentar el *marco legal* como solución de primera línea, que generalmente es *efectiva* ante los delitos digitales, ya que somos conscientes del desamparo que existe en todo marco legal en Venezuela.

Las piezas están enfocadas en poner a los usuarios de las redes y sistemas digitales, como responsables de su propia seguridad a través de herramientas que están a su alcance. Otra razón para no usar el marco legal, como tema principal del mensaje para la prevención de los delitos y crear conciencia con la campaña, es que esta estaría asociada a significados negativos y que, por lo general, este tipo de información no despierta interés en su lectura, y no ofrece una solución preventiva. La campaña intenta ofrecer diferentes posibilidades individuales de solución.

6.- ESTRATEGIA

6.1.- PLAN DE CONTENIDOS

En el plan de contenidos se plantea cómo captar la atención del público receptor, cómo despertar su interés con el mensaje, cómo generar confianza y credibilidad, para que despierte conciencia en la temática planteada. Para ello se requiere la producción (diseño y realización) de las piezas detalladas a continuación, definiendo su posición y utilidad en la campaña:

- 3 (tres) piezas graficas Artes Finales, de formato adecuado para impresos y digitales acordados, que contienen la *Imagen Base* de cada uno de los tres Descarados (Arrobaldo, Zamureta y Wisin Wasap).
- 1 (un) Titulo e Identidad Gráfica de la Campaña (*lettering*, papelería, imágenes).
- 6 (seis) *Stickers* para usar en redes sociales, especialmente en WhatsApp, tres para cada Descarado, en los cuales se les ve realizando una acción clave para responder o afrontar una posible situación de delito digital, pero a la vez para compartir y distribuir de manera *memética*.
- 3 (tres) *GIF* (*Graphic interlaced format*), referidos al formato que permite realizar animaciones de bajo peso digital –cuadro a cuadro- que suelen ser muy útiles en redes sociales y en captación de contenidos. Con estas piezas se pretende presentar a toda la Banda de los Descarados o a la Campaña en General y dar soporte al Sitio Web y demás contenidos y líneas de acción.
- 2 (dos) Videos de 1 minuto de duración cada uno, a través de técnicas de animación sencilla y efectiva que permitan generar contenidos más desarrollados respecto a la trama o historia de los Descarados, y producir respuestas afectivas de compromiso con la campaña a través de la captación de una narrativa menos inmediata, y más extendida. Sin embargo, éstas siguen siendo capsulas de narración a tomar en cuenta, considerando el alcance de la campaña y sus tiempos estipulados.
- 1 (un) espacio en la Web que contenga la Campaña los Descarados, que permita tener acceso a todo el contenido y además se pueda incluir información de largo tiempo de duración y atención como el marco legal, entre otros.

En la tabla siguiente se presenta todo el plan de contenidos para la Campaña.

- Tabla Plan de Contenidos Campaña "*Los Descarados*"

Pieza	***Objetivo***	***Cantidad***	***Formato***	***Plataforma***
Piezas Gráficas	• Arte final. Base de toda la campaña	3	Imágenes	Facebook Instagram Twitter Youtube Sitio Web
Sticker	• Alertar a los ciudadanos sobre los delitos informáticos. • Orientar sobre medidas preventivas para evitar el fraude.	6	Imágenes	WhatsApp Instagram Twitter
Gif	• Alertar a los ciudadanos sobre los delitos informáticos. • Orientar sobre medidas preventivas para evitar el fraude.	3	Animaciones	Facebook Instagram Twitter Youtube
Videos	• Alertar a los ciudadanos sobre los delitos informáticos. • Orientar sobre medidas preventivas para evitar el fraude.	2	Animaciones	Facebook Instagram Twitter Youtube
Espacio Web	• Divulgar (informar) el marco legal que regula los delitos informáticos en Venezuela. • Informar (divulgar) sobre los distintos entes encargados de tramitar y sustanciar los hechos delictivos. • Alertar a los ciudadanos sobre los delitos informáticos. • Orientar sobre medidas preventivas para evitar el fraude. • Orientar sobre el uso y manejo adecuado de las redes sociales, medios digitales y tecnologías emergentes.	1	Imágenes Hipertextos Animaciones	Sitio Web

6.2.- PLAN DE DIFUSIÓN

AL tener las piezas descritas ya desarrolladas, se procederá a activar los diferentes momentos de la campaña. Durante el *Inauguración/Estreno* se anuncian todas las piezas y sus interacciones con la audiencia, la página web, todos los videos y los *Stickers* en un acto de presentación a la comunidad. A partir de ese momento y durante aproximadamente **6 semanas** se activarán alianzas estratégicas con comunicadores, *influencers*, programas nacionales, radio, televisión y varios medios para iniciar la presencia mediática a mayor escala. El plan de difusión para la Campaña, estará diseñado de la siguiente manera:

El **día de Arranque/inicio** de la Campaña se hará un acto con los medios de prensa, local, donde se presentarán los objetivos de la campaña, los **3 Afiches base** y la proyección de los *Stickers*, *Gifs*, videos y finalmente se presenta el Espacio Web dando así inicio oficial a la campaña.

Durante la **Primera semana,** posterior al arranque, se realizara la difusión de las **3 imágenes base** de la campaña, representando a los descarados, con el objetivo de dar a conocer el estado de Alerta. Se activará, en paralelo la difusión de los **Videos**

y Página Web, a través de las redes sociales principales: **Instagram, Twitter, Facebook**.

En la **Segunda y Tercera Semana**, se harán anuncios especiales de refuerzo de la primera semana: nuevas imágenes derivadas de las tres iniciales, además se hará el estreno de los ***stickers*** y ***gifs*** para usar en los chats de las diferentes redes. En este momento se hará énfasis en Whatsapp y Telegram, y se señalará el **Sitio Web** como lugar donde se pueden descargar y usar los elementos de la comunicación para ayudar a prevenir los delitos digitales, así como acceder a información extra sobre el marco legal y buenas prácticas.

En la **Cuarta y Quinta Semana**, una vez estrenado todo el material con el contenido de la campaña, se inicia el Remate Final de asentamiento de la Campaña, que consiste en: 1) Charlas y foros en escuelas, colegios, casas de cuidado, bancos y sitios de congregación de los grupos vulnerables. 2) Difusión Radial Nacional, Difusión en Televisoras Nacionales (programas puntuales), alianzas con entes y servicios relacionados (personalidades nacionales, Grupos dedicados a la compra y venta de Divisas, actores especiales en el ámbito de las redes sociales, entre otros). La idea aquí es lograr alianzas en diferentes ciudades para poder difundir la campaña a través de organismos o grupos locales públicos o privados.

La **Sexta y Última** semana es de cierre y agradecimiento. Se mencionan los Agradecimientos a los diferentes entes de apoyo y difusión. Se puede volver a la radio y televisión nacional, se terminan las últimas charlas y exposiciones en vivo y se puede hacer un acto interno de cierre y análisis de resultados. Se deja el sitio web activo (por un determinado tiempo, a definir), para que la Campaña, como todo en el entorno de la Web, siga validándose según sus propios medios.
En este punto cabe destacar que, el plan de difusión específico, con los días y horas de publicación de cada pieza, se hará en el momento en que se tengan dichos recursos completamente definidos y desarrollados.

6.3.- INDICADORES PARA MEDIR RESULTADOS DE LA CAMPAÑA (KPI)

Para hacer el seguimiento a la campaña y conocer si se han logrado los objetivos planteados, se hará uso de algunos indicadores claves de desempeño (KPI – *Key Performance Indicators*) y métricas propias de las redes sociales.

Los KPI permiten dar seguimiento a los objetivos y las métricas son parámetros que brindan datos sobre la actividad en las redes sociales. Pueden medir alcance, compromiso, conversión o fidelización. Esto nos permitirá medir los resultados de la campaña. En nuestro caso haremos uso de indicadores que nos permitan medir principalmente el alcance de la campaña y el compromiso de la gente con el mensaje. Los indicadores a usar para las redes sociales Instagram, FaceBook, y Twitter, serán:

A) Visibilidad: Llegar a la mayor cantidad de personas.

1.- Alcance e impresiones: el KPI alcance indicará el número de personas que ha visto la publicación, mientras que el KPI de impresiones será el número de veces que las publicaciones han sido vistas. Para que los resultados tengan un valor positivo, se debe analizar la relación que existe entre el alcance/impresiones y el tipo de publicaciones y horario/tiempo de publicación. Solo teniendo en cuenta estos

parámetros, se podrá considerar el resultado como un indicador clave.

2.- Número de seguidores: el número de seguidores de la publicación en las Redes Sociales es un claro indicador del estado de la visibilidad que se está alcanzando con la estrategia.

B) Interacciones sociales: Relación de la gente con la publicación.

1.- Número de "Me Gusta" (o cualquier otro indicador de este tipo que use la red social en cuestión): a mayor número de "Me Gusta" en las publicaciones, significa que existe un nivel de compromiso bueno de parte del público. Cuando una persona coloca o selecciona "Me Gusta", es posible que sus amigos vean la publicación y en consecuencia la visibilidad aumenta.

2.- Shares o Compartidos: si una persona comparte el contenido de la publicación, está demostrando que le interesa y muestra mayor compromiso y fidelidad.

3.- Comentarios: si la audiencia comenta la publicación, esta consideración es muy positiva, ya que significa que está generando algún tipo de emoción.

Tercer informe de avance del proyecto1:

MUESTRARIO DE LOS RECURSOS MULTIMEDIA DE APOYO A LA CAMPAÑA

7 febrero de 2020

Proyecto aprobado por el Comité de Selección del Fondo de Respuesta Rápida (FRR) de Derechos Digitales en el mes de septiembre de 2019.

El informe presenta el muestrario de los recursos multimedia de apoyo a la campaña, que fueron desarrollados durante la fase tres del proyecto.

En la Estrategia Comunicacional para la Campaña Los Descarados, se definieron las piezas visuales que serían desarrolladas, las cuales están conformadas por:

- 3 (tres) piezas gráficas Artes Finales, de formato adecuado para impresos y digitales acordados, que contienen la Imagen Base de cada uno de los tres Descarados

(Arrobaldo, María Mirona y Wisin Wasap).

- 1 (un) Titulo e Identidad Gráfica de la Campaña (lettering, papelería, imágenes).

- 6 (seis) Stickers para usar en redes sociales, especialmente en WhatsApp, dos para cada Descarado, en los cuales se les ve realizando una acción clave para responder o afrontar una posible situación de delito digital, pero a la vez para compartir y distribuir de manera memética.

- 3 (tres) GIF (Graphic interlaced format), referido al formato que permite realizar animaciones de bajo peso –cuadro a cuadro- que suelen ser muy útiles en redes

sociales y en captación de contenidos. Con estas piezas se pretende presentar a toda la Banda de los Descarados o a la Campaña en General y dar soporte al Sitio Web y demás contenidos y líneas de acción.

- 2 (dos) Videos de 1 minuto de duración cada uno, a través de técnicas de animación sencilla y efectiva que permitan generar contenidos más desarrollados respecto a la trama o historia de los Descarados, y producir respuestas afectivas de compromiso con la campaña a través de la captación de una narrativa menos inmediata, más extendida. Sin embargo, siguen siendo capsulas de narración considerando el alcance de la campaña y sus tiempos estipulados.

- 1 (un) espacio en la Web que contenga la Campaña los Descarados, que permita tener acceso a todo el contenido y además se pueda incluir información de largo tiempo de duración y atención como el marco legal, entre otros.

En el sitio web http://dilomujer.org/losdescarados se puede acceder a toda la información relevante de la campaña, así como descargar todas las piezas visuales objeto de la misma.

Es decir, el sitio web de la campaña funge como repositorio del muestrario de los recursos multimedia de apoyo a la campaña.

Adicionalmente, los recursos multimedia (Vídeos, Gifs, y Stickers), así como un vídeo que muestra la apariencia y funcionamiento del sitio web, están disponibles en:

https://drive.google.com/drive/folders/1mmkdWY5p4oqueX4ZZ1AVFP5JV038zDeI?usp=sharing

Nota: La dirección del sitio web señalado es temporal. En el momento de inicio de la difusión de la campaña se tendrá la dirección de alojamiento definitiva.

Cuarto informe de avance del proyecto:

DESARROLLO DE LA CAMPAÑA

6 marzo de 2020

Este documento tiene como finalidad presentar el cuarto informe de avance del proyecto denominado: "Desenmascara el delito informático, no al fraude en las redes sociales", el cual es una campaña para orientar a los ciudadanos venezolanos sobre los riesgos que corren al realizar prácticas inadecuadas en las redes sociales, que los exponen al fraude y a la violación de su seguridad digital.

El informe presenta una breve reseña de cómo ha sido el desarrollo de la campaña de orientación sobre la temática de los delitos digitales.

En la Estrategia Comunicacional, presentada en el mes de diciembre próximo pasado, se esbozó un plan de contenidos para la Campaña "Los Descarados", la cual contemplaba el tipo de piezas visuales, el objetivo para el que fueron creadas y la plataforma o red social en las que serían publicadas.

De esta manera, para el desarrollo de la Campaña, luego de haber producido todas las piezas visuales, se procedió a la apertura de los distintos enlaces y cuentas desde los cuales se puede tener acceso a las mismas.

1) Sitio Web:

http://losdescarados.eslared.net

Procedimos a crear un sitio web bajo el dominio EsLaRed que se encuentra hospedado en la organización Colnodo de Colombia, miembro de APC, para tener un mejor acceso desde internet y con cobertura global. Es un elemento esencial comunicacional en donde está contenida toda la información de la Campaña Los Descarados. Desde aquí se puede tener acceso a todas las piezas visuales de la campaña, descargarse para usarse en cualquiera de las otras redes o plataformas, y al contenido completo. Este espacio en la web permitirá incluir información de largo tiempo de duración y atención como el marco legal, las medidas preventivas y de seguridad, entre otras. Por ésta razón, el sitio web permitirá entre otros objetivos informar sobre los distintos entes encargados de tramitar y sustanciar los hechos delictivos, así como divulgar el marco legal que regula los delitos informáticos en Venezuela; pero más importante, además de alertar sobre los delitos informáticos, permitirá orientar sobre el uso y manejo adecuado de las redes sociales, medios digitales y tecnologías emergentes.

2) Fan Page:

https://www.facebook.com/Descarados-Delitos-101866178089577/?modal=admin_todo_tour

Esta fanpage de Facebook nos permite tener un canal de comunicación con fans dentro de FaceBook, que estén interesados en la temática de los Delitos Digitales, sin la necesidad de la aprobación de su amistad, y donde podrán elegir seguir las actualizaciones de la página de Los Descarados. Esta fanpage nos permite hacer difusión de la campaña con un alcance muy amplio. Además es requerida para poder comprar publicidad en la red Instagram, con el fin de promover la campaña.

3) Instagram:

@Los_descaradosdelitos

Instagram es una red social que ha crecido de forma exponencial en los últimos años. La cuenta de Instagram se puede asociar con Facebook y con Twitter, compartiendo de manera automática el contenido subido en Instagram. Siendo que la temática de la campaña está referida a los delitos digitales, la difusión de las imágenes, Gifs y Stikers, a través de Instagram puede garantizar un amplio alcance e impacto en la población. Será la base central de la publicidad de la campaña. De esta manera, se puede hacer uso de esta red para alertar a los ciudadanos sobre los delitos informáticos, así como orientar sobre medidas preventivas para evitar el fraude.

4) Twitter:

@Los_descaradosdelitos

Twitter, como aplicación web de microblogging, nos permite compartir con el mundo mensajes cortos sobre la campaña, así como los Gifs y Stikers, que quizá para mucha gente sean interesantes, tantas veces como queramos. Para ésta red en particular, los influencers jugarán un papel importante en la difusión y promoción de la campaña. Al igual que Instagram, ésta red permitirá alertar a los ciudadanos sobre los delitos informáticos y orientar sobre medidas preventivas para evitar el fraude.

5) Youtube:

http://youtube.com/channel/UC9sOHdDaToovllNnlmw-bbw

El canal de Youtube permite compartir los videos desarrollados para la campaña. Se han subido dos vídeos que contienen la descripción de los delincuentes, denominados Los Descarados, así como los delitos que comenten, y algunas medidas de prevención y seguridad. El enlace al canal de youtube, y por ende el acceso a estos vídeos podrá compartirse desde cualquiera de las redes antes mencionadas.

6) WhatApp:

Esta red será la base fundamental para compartir los Stikers y Gifs, con los que de una forma muy breve y dinámica se ve a cada Descarado, lo que permite una acción clave para responder o afrontar una posible situación de delito digital, y a la vez para compartir y distribuir de manera memética. Por el WhatApp se pretende presentar a toda la Banda de los Descarados y a la Campaña en General para dar soporte al Sitio Web y demás contenidos y líneas de acción. Para la viralización de las piezas por ésta red social, es esencial el contacto con distintos grupos reconocidos e influencers.

Plan de difusión.

Según el plan definido, al tener las piezas desarrolladas y creadas las cuentas en las distintas redes sociales, se debe proceder a activar la campaña.

En este momento nos encontramos activando alianzas estratégicas con comunicadores, influencers, programas nacionales, radio, televisión y varios medios para iniciar la presencia mediática a mayor escala, y así proceder a la Inauguración/Estreno en la que se anunciarán todas las piezas y sus interacciones con la audiencia, la página web, los videos y los Stickers.

En paralelo, durante la Primera semana, se ha iniciado la difusión de las 3 imágenes base de la campaña, representando a los descarados, con el objetivo de dar a conocer el estado de Alerta. De igual manera se ha iniciado la promoción de los Videos y Página Web, a través de las redes sociales principales: Instagram, Twitter, WhatApp y Facebook.

En la Segunda y Tercera Semana, se harán anuncios especiales de refuerzo a lo expuesto en la primera semana: nuevas imágenes derivadas de las tres iniciales, además se hará el estreno de los stickers y gifs para usar en los chats de las diferentes redes. En este momento se hará énfasis en Whatsapp, y se señalará el Sitio Web como lugar donde se pueden descargar y usar los elementos de la comunicación para ayudar a prevenir los delitos digitales, así como acceder a información extra sobre el marco legal y buenas prácticas.

En la Cuarta y Quinta Semana, una vez estrenado todo el material con el contenido de la campaña, se inicia el Remate Final de asentamiento de la Campaña, que consiste en: 1) Charlas y foros en escuelas, colegios, casas de cuidado, bancos y sitios de congregación de los grupos vulnerables. 2) Difusión Radial Nacional (parcial), Difusión en Televisoras Nacionales (programas puntuales), alianzas con entes y servicios relacionados (personalidades nacionales, Grupos dedicados a la compra y venta de Divisas, actores especiales en el ámbito de las redes sociales, entre otros). La idea aquí es lograr alianzas en diferentes ciudades para poder difundir la campaña a través de organismos o grupos locales públicos o privados.

La Sexta y Última semana es de cierre y agradecimiento. Se mencionan los Agradecimientos a los diferentes entes de apoyo y difusión. Se puede volver a la radio y televisión nacional, se terminan las últimas charlas y exposiciones en vivo y se puede hacer un acto interno de cierre y análisis de resultados. Se deja el sitio web activo (por un determinado tiempo, a definir), para que la Campaña, como todo en el entorno de la Web, siga validándose según sus propios medios.

Nota: Cabe destacar que para el desarrollo de la Campaña nos hemos encontrado con problemas severos relacionados con cortes de electricidad por períodos muy largos (de hasta 12 horas continuas) y de conexión a internet, que nos han

retrasado en la puesta en marcha de la misma en la redes. Sin embargo, todas las cuentas han sido creadas y se ha iniciado la publicidad y promoción de las distintas piezas visuales. Adicionalmente a esta acción se decidió hospedar el sitio web fuera de Venezuela con el fin de tener en todo momento la posibilidad de accederlo desde nuestro país y desde el exterior.

Quinto informe de avance del proyecto[33]:

ACCESO A LA CAMPAÑA "LOS DESCARADOS" EN MEDIOS DIGITALES RESULTADOS DE LA CAMPAÑA

7 de abril 2020

Este documento tiene como finalidad presentar el quinto informe de avance del proyecto denominado: "Desenmascara el delito informático, no al fraude en las redes sociales", en el cual se desarrolló la **Campaña Los Descarados** con la finalidad de orientar a los ciudadanos venezolanos sobre los riesgos que corren al realizar prácticas inadecuadas en las redes sociales, que los exponen al fraude y a la violación de su seguridad digital.

El informe presenta una reseña sobre la implementación de la campaña **Los Descarados** en las redes sociales y los resultados e impacto que ella produjo en la población en general.

La campaña consistió en activar, inicialmente, alianzas estratégicas con comunicadores, *influencers*, programas nacionales, radio, televisión y varios medios para iniciar la presencia mediática a mayor escala, y así proceder a la Inauguración/Estreno de la campaña en la que se anunciaron todas las piezas y sus interacciones con la audiencia, la página web, los videos y los *Stickers*.

En paralelo, durante la primera semana del 22 al 29 de febrero de 2020**,** se inició la difusión de las 3 imágenes base de la campaña, representando a los descarados, con el objetivo de dar a conocer el estado de Alerta. De igual manera se inició la promoción de los Videos y Página Web, a través de las redes sociales principales: Instagram, Twitter, WhatApp y Facebook (Ver informe 4 sobre el desarrollo de la campaña).

En la segunda y tercera semana, del 01 al 15 de marzo de 2020, se procedió a hacer anuncios especiales de refuerzo de las piezas de la primera semana

[33] Proyecto aprobado por el Comité de Selección del Fondo de Respuesta Rápida (FRR) de Derechos Digitales en el mes de septiembre de 2019.

incorporando los *stickers* y *gifs* usados en los chats de las diferentes redes. En este momento se hizo énfasis en Whatsapp, y se hacía referencia al Sitio Web desde el cual se pueden descargar y usar los elementos de la comunicación para ayudar a prevenir los delitos digitales, así como acceder a información extra sobre el marco legal y buenas prácticas.

En la cuarta y quinta semana (16 al 31 de marzo de 2020) debíamos realizar la fase final de asentamiento de la campaña a través de charlas y foros en escuelas, colegios, universidades, bancos y sitios de congregación de los grupos vulnerables; así como la difusión radial Nacional, Difusión en Televisoras Nacionales (programas puntuales), para lograr alianzas en diferentes ciudades que permitieran difundir la campaña a través de organismos o grupos locales públicos o privados. Es importante señalar, que debido a la problemática generada por la pandemia del Covid-19, esta fase no se pudo ejecutar por encontrarnos en cuarentena. Sin embargo, si se pudo continuar con la publicidad y promoción de las piezas visuales de la campaña a través de las cuentas en las redes sociales creadas para tal fin.

Nota: *Cabe destacar que para la implementación de la Campaña nos ENCONTRAMOS con problemas severos relacionados con cortes de electricidad por períodos muy largos (de hasta 12 horas continuas) y de conexión a internet, que retrasaron la puesta en marcha de la misma en la redes. Sin embargo, la publicidad y promoción de las distintas piezas visuales en las cuentas creadas se mantuvo durante el período definido para tal fin. Por otro lado, toda la situación de la pandemia del COVID 19 ha alterado el interés de las personas en este tipo de información, así como ha hecho difícil el establecimiento de alianzas con comunicadores sociales y/o influencers*.

INDICADORES CONSIDERADOS PARA MEDIR RESULTADOS DE LA CAMPAÑA (KPI)

Para hacer el seguimiento a la campaña y conocer si se lograron los objetivos planteados, se hizo uso de algunos indicadores claves de desempeño (KPI – *Key Performance Indicators*) y métricas propias de las redes sociales.

Estos indicadores brindan datos sobre la actividad en las redes sociales, y nos permitieron dar seguimiento a los objetivos y las métricas. El principal objetivo era medir principalmente el alcance de la campaña y el compromiso de la gente con el mensaje. Los indicadores usados para las redes sociales Instagram, FaceBook, y Twitter, fueron:

A) Visibilidad: Llegar a la mayor cantidad de personas.

Alcance e impresiones: el KPI alcance indica el número de personas que ha visto la publicación, mientras que el KPI de impresiones es el número de veces que las publicaciones han sido vistas.

B) Interacciones sociales: Relación de la gente con la publicación.

Número de "Me Gusta": a mayor número de "Me Gusta" en las publicaciones, significa que hay un nivel de compromiso bueno del público. Cuando una persona poner "Me Gusta", es posible que sus amigos vean la publicación y la visibilidad aumenta.

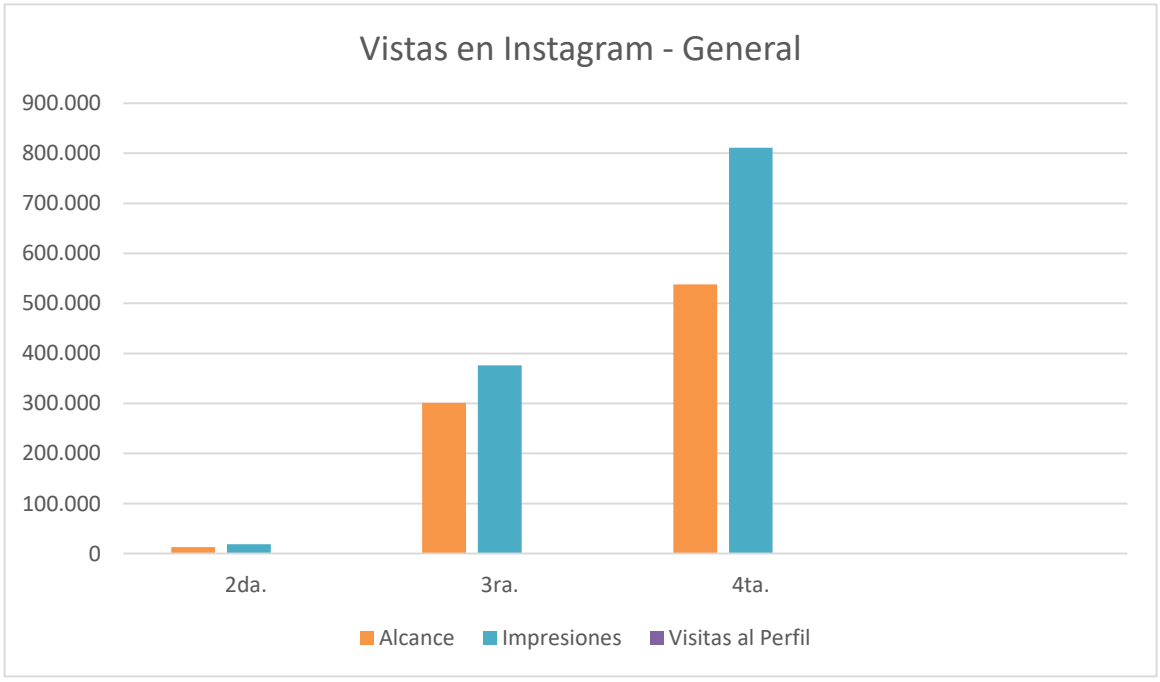
A continuación se presentan los resultados obtenidos en las diferentes redes sociales. Los cuadros que se presentan están referidos a la publicidad que fue contratada en las distintas redes.

RESULTADOS PUBLICACIONES EN LAS REDES SOCIALES

1. INSTAGRAM

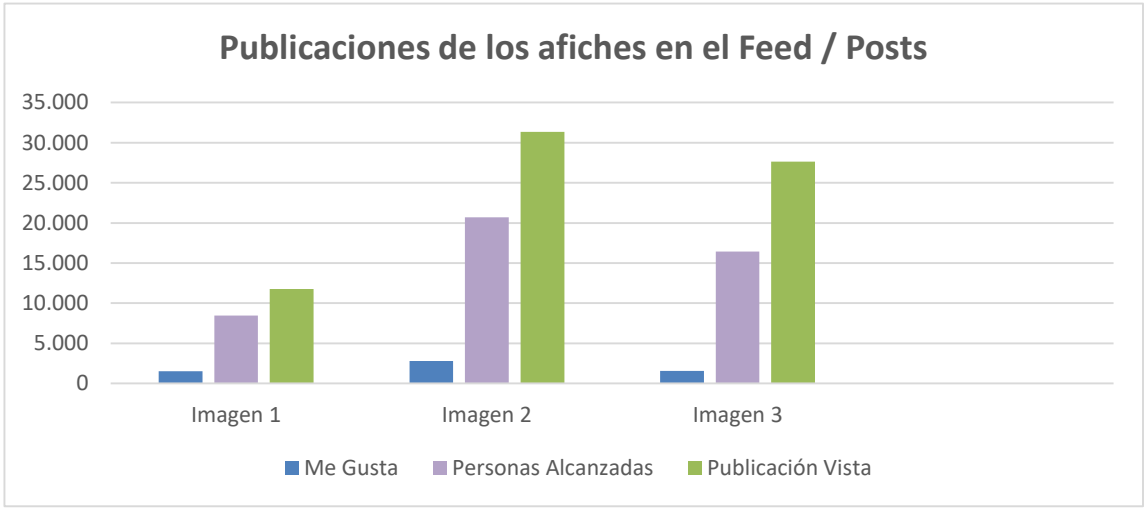
1.1.- Actividad en general.

Semana	Alcance	Impresiones	Visitas al Perfil
2da. (12 al 18 Marzo)	12.559	18.395	43
3ra. (19 al 25 Marzo)	301.075	376.026	212
4ta. (26 al 31 Marzo)	538.025	811.030	461



1.2.- Publicaciones de los afiches en el Feed / Posts.

				Interacciones		Descubrimiento		Audiencia		
Imagen	**Tiempo (días)**	**Me gusta**	**Clicks en Promoción**	**Visita página web**	**Visita al Perfil**	**Número de Personas alcanzadas**	**Número de veces publicación vista**	**Género**	**Ubicación (Top Location)**	**Edad**
1 María Mirona. JPG	26	1.510	22	24	23	8.457	11.760	51% Hombres 49% Mujeres	12% DC 11% Zulia 10% Táchira	25% 13-17 21% 18-24 16% 25-34 13% 35-44 12% 45-54 8% 55-64 4% 65+
2 Wissin Wassap JPG	26	2.791	45	55	60	20.700	31.355	67% Hombres 33% Mujeres	13% DC 10% Zulia 9% Táchira	26% 13-17 25% 18-24 20% 25-34 13% 35-44 8% 45-54 5% 55-64 3% 65+
3 Arrobaldo .JPG	26	1.556	31	49	52	16.432	27.645	62% Hombres 38% Mujeres	13% DC 10% Zulia 9% Táchira 9% Aragua	21% 13-17 25% 18-24 16% 25-34 15% 35-44 10% 45-54 8% 55-64 4% 65+


Publicaciones de los afiches en el Feed / Posts
35.000
30.000
25.000
20.000
15.000
10.000
5.000
0
Imagen 1
Imagen 2
Imagen 3
Me Gusta
Personas Alcanzadas
Publicación Vista

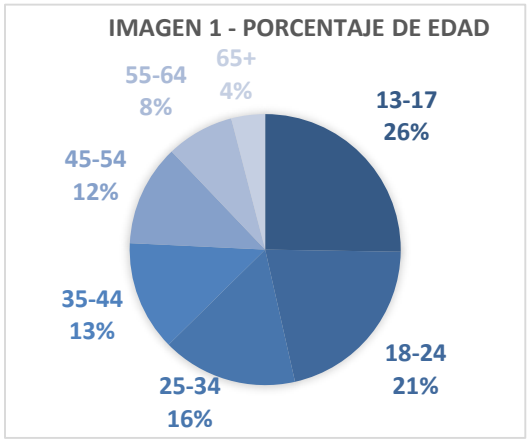


IMAGEN 1 - PORCENTAJE DE EDAD
13-17 26%
18-24 21%
25-34 16%
35-44 13%
45-54 12%
55-64 8%
65+ 4%

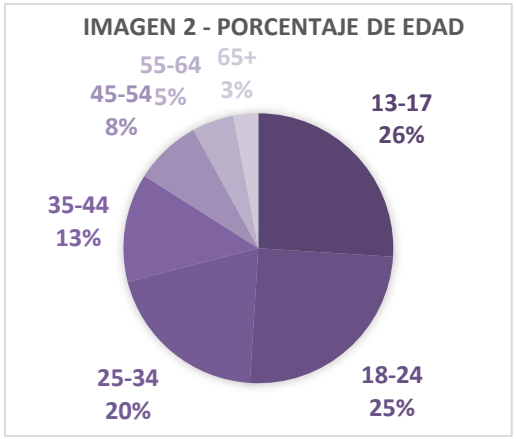


IMAGEN 2 - PORCENTAJE DE EDAD
13-17 26%
18-24 25%
25-34 20%
35-44 13%
45-54 8%
55-64 5%
65+ 3%

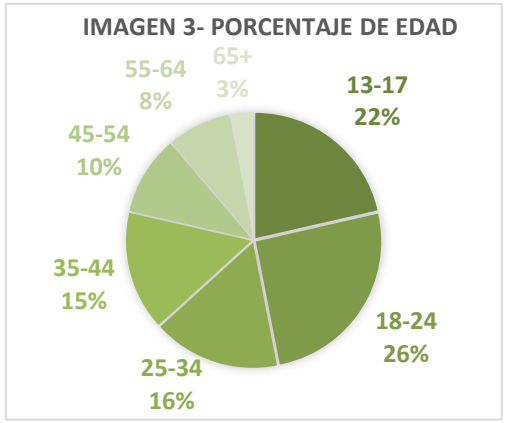
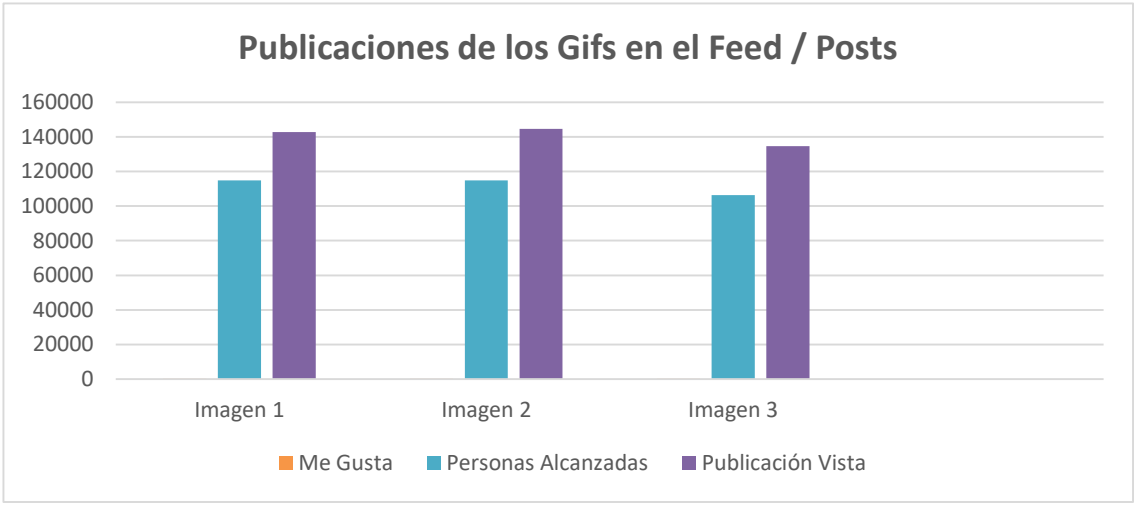


IMAGEN 3- PORCENTAJE DE EDAD
13-17 22%
18-24 26%
25-34 16%
35-44 15%
45-54 10%
55-64 8%
65+ 3%

1.3.- Publicaciones de los Gifs en el Feed / Posts.

				Interacciones		Descubrimiento		Audiencia		
Imagen	**Tiempo (días)**	**Me gusta**	**Veces Vista**	**Visita página web**	**Visita al Perfil**	**Número de Personas alcanzadas**	**Número de veces publicación vista**	**Género**	**Ubicación (Top Location)**	**Edad**
1 María Mirona. Gif	7	159	42.268	422	105	114.849	142.827	35% Hombres 65% Mujeres	13% DC 10% Zulia 9% Táchira 9% Aragua	4% 13-17 4% 18-24 12% 25-34 24% 35-44 25% 45-54 21% 55-64 10% 65+
2 Wissin Wassap. GIf	7	114	40.001	421	86	114.746	144.516	33% Hombres 67% Mujeres	13% DC 10% Zulia 9% Táchira 9% Aragua	2% 13-17 4% 18-24 13% 25-34 23% 35-44 25% 45-54 21% 55-64 11% 65+
3 Arrobaldo .Gif	7	158	38.271	451	108	106.337	134.591	28% Hombres 72% Mujeres	14% DC 11% Zulia 9% Táchira 9% Aragua	2% 13-17 5% 18-24 13% 25-34 24% 35-44 25% 45-54 21% 55-64 10% 65+


Publicaciones de los Gifs en el Feed / Posts
160000
140000
120000
100000
80000
60000
40000
20000
0
Imagen 1
Imagen 2
Imagen 3
Me Gusta
Personas Alcanzadas
Publicación Vista

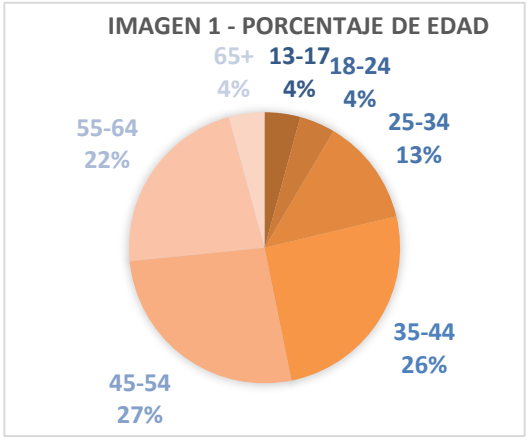


IMAGEN 1 - PORCENTAJE DE EDAD
65+ 4%
13-17 4%
18-24 4%
25-34 13%
35-44 26%
45-54 27%
55-64 22%

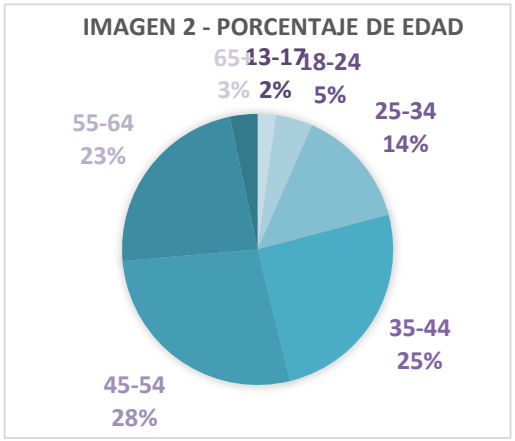


IMAGEN 2 - PORCENTAJE DE EDAD
65+ 3%
13-17 2%
18-24 5%
25-34 14%
35-44 25%
45-54 28%
55-64 23%

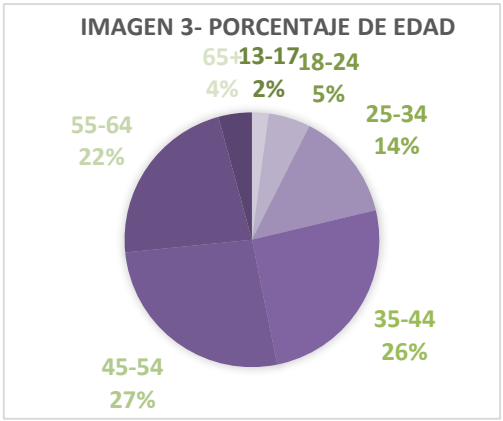
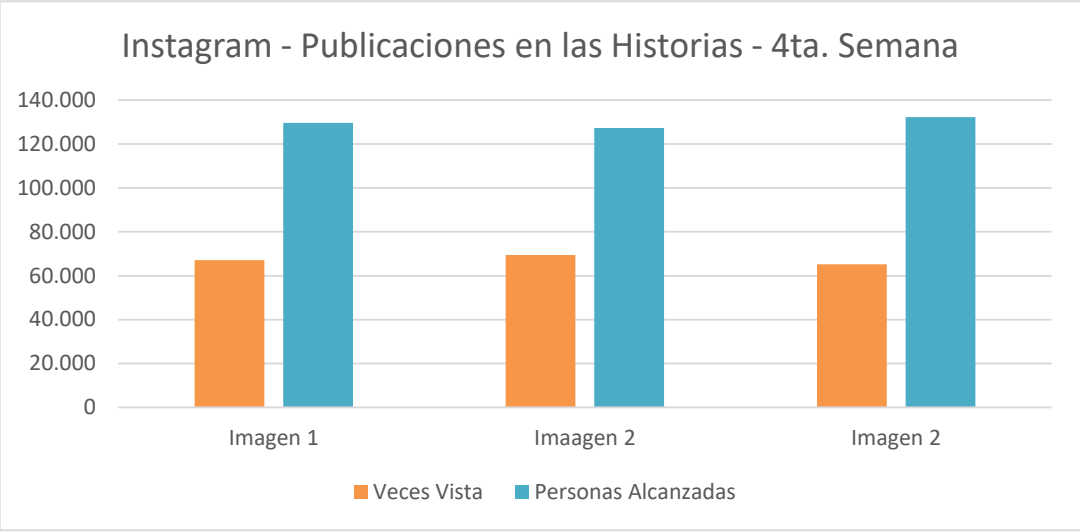


IMAGEN 3- PORCENTAJE DE EDAD
65+ 4%
13-17 2%
18-24 5%
25-34 14%
35-44 26%
45-54 27%
55-64 22%

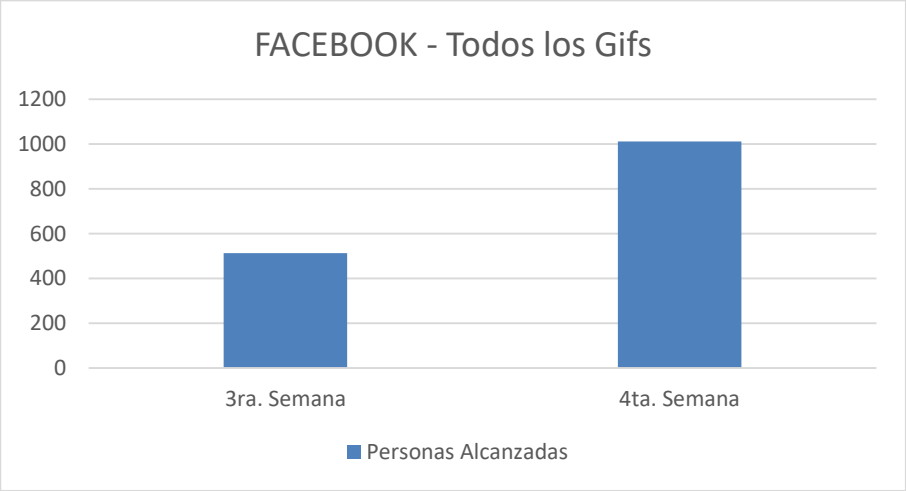
1.4. Publicaciones en las Historias

Imagen	Tiempo (días)	Veces Vista	Número de Personas alcanzadas	Visitas al Perfil	Género	Ubicación (Top Location)	Edad (Top three)
1 Arrobaldo . Gif	7	67.093	129.698	32	37% Hombres 63% Mujeres	15% DC 13% Zulia 10% Táchira	36% 25-34 32% 18-24 10% 35-44
2 María Mirona . Gif	7	69.364	127.322	43	42% Hombres 58% Mujeres	13% DC 12% Zulia 10% Táchira	32% 25-34 29% 18-24 12% 35-44
3 Wissin Wassap .Gif	7	65.228	132.231	42	35% Hombres 64% Mujeres	13% DC 13% Zulia 10% Táchira	30% 25-34 29% 18-24 13% 35-44



2. FACEBOOK

Imagen	Semana	Número de Personas Alcanzadas	Interacciones
Todos los .Gif	3ra. (19 al 25 de Marzo)	513	2
Todos los .Gif	4ta. (26 al 31 Marzo)	1.012	14



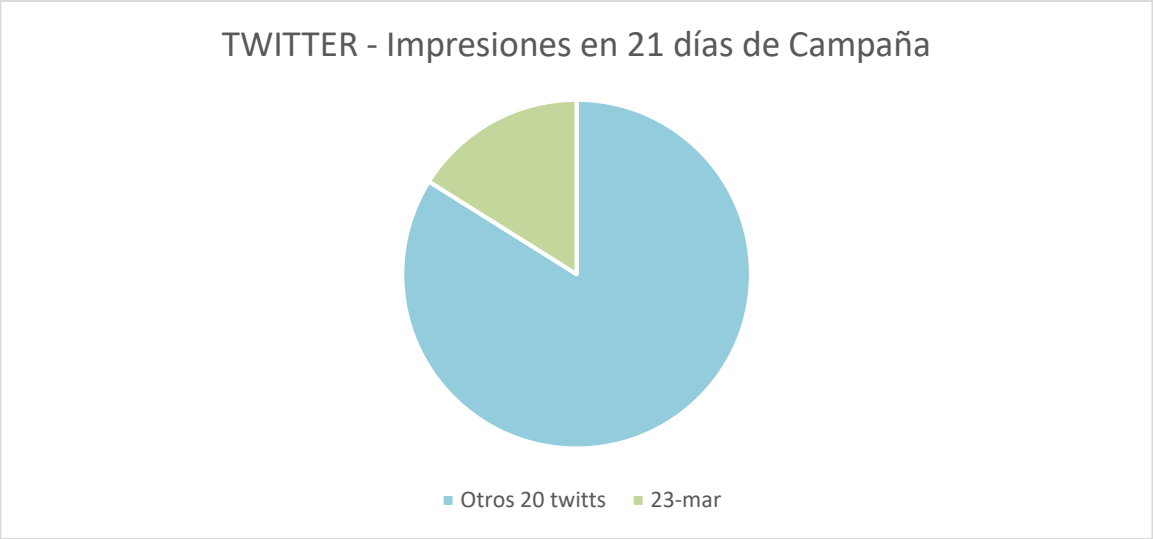
3. TWITTER

@LosDescaradosD1:

				Promedio de Interacciones			
Número de Tweets	**Fecha de Inicio**	**Fecha de Finalización**	**Promedio de Tweets Diario**	**Impresiones**	**Likes**	**Retweet**	**Comentario**
21	08/03	29/03	1	91	4	1	1
Total de impresiones				**1728**			

TWITT DESTACADO

Contenido	Fecha de Publicación	Impresiones	Likes	Retweet	Comentario
¡Debemos estar atentos y evitar ser víctimas de los DESCARADOS! Wissin Wassap . Gif	23de Marzo	**278**	1	1	0



CONCLUSIONES Y RECOMENDACIONES

Es importante resaltar que el período de exposición de la campaña Los Descarados, durante estas 4 semanas, en las redes sociales, lo hemos considerado como la fase de dar a conocer el mensaje, de generar conciencia, para lo cual se monitorearon las publicaciones en las distintas redes sociales y observar que tan lejos se llegó, cuál fue el alcance, y cuántas personas fueron alcanzadas. De esta manera se puede definir el crecimiento de la población alcanzada a medida que avanza el tiempo de exposición de la campaña.

Se observa a través de la actividad general en Instagram, que a medida que la campaña avanzaba en el tiempo, el alcance iba siendo mayor, pasando de 12.559 personas alcanzadas y 18.395 impresiones en la segunda semana, a tener más de 500.000 personas alcanzadas y 800.000 impresiones, para la cuarta semana. Se puede inducir que se fue creando una comunidad de interés en la temática durante el período de exposición de la campaña.

Con respecto a las publicaciones *feed/post* de Instagram de las imágenes en JPG y en GIFs, se observó que el 70% de las personas que tuvieron acceso a las 3 imágenes en JPG, correspondían a los grupos comprendidos entre los 13 hasta los 34 años de edad; esto contrasta con la edad de las personas que accedieron a las 3 imágenes en Gifs, donde aproximadamente el 85% estaban en los grupos entre los 35 y 65 o más años de edad. En relación al género, los datos arrojaron que aproximadamente el 65% de la población que tuvo acceso a las imágenes de la campaña correspondía al género femenino. De igual manera, se observó que la mayor cantidad de la población que tuvo acceso a la campaña se encontraba ubicado en la zona central (Estado Aragua, y Distrito Capital) y occidental (Estados Zulia y Táchira) del país.

En referencia a las publicaciones de las imágenes en Gifs en la historias de Instagram, las cuales se llevaron a cabo durante la última semana de la campaña, se observó que el alcance para las tres imágenes fue similar, llegando a un promedio de 130.000 personas alcanzadas.

En cuanto al alcance en FaceBook, se observó que el número de personas alcanzas en tan sólo dos semanas de Campaña se había duplicado, pasando de 513 a 1.012. En la red social Twitter se logró tener un total de 1.718 impresiones, para 1 twit diario durante 21 días.

Es importante señalar, que para mejorar la efectividad de la Campaña Los Descarados se podrían evaluar estos resultados, y analizar el perfil de los usuarios a los que se les ha llegado para redefinir la estrategia y generar una taza de crecimiento mayor de la población alcanzada, de ésta manera crear una comunidad de interés más amplia. Esto en caso de querer mantener la publicidad en las redes.

En general, podemos concluir que la Campaña Los Descarados, a pesar de la problemática generada por los cortes eléctricos, la falta de combustible y de conexión a Internet a la que estamos sometidos en Venezuela, y a la pandemia del Covid-19, logró tener en el período de duración de la misma, un alcance altamente satisfactorio, considerando el desinterés que pueden tener las personas, en estas circunstancias, por este tipo de información.

Es de hacer notar, que por las circunstancias suscitadas debido a la cuarentena a la que está obligada toda la población, se han incrementado los delitos digitales de fraude y estafa a través de las redes. Razón por la que consideramos, que aun cuando el proyecto con el Fondo de Respuesta Rápida haya concluido, la Campaña Los Descarados permanezca en las redes, siendo que el mensaje de la misma es atemporal y válido para cualquier otra región.

OBSERVACIONES FINALES Y REFLEXIONES DE LA CAMPAÑA

1. En los resultados obtenidos se debe aclarar que "la campaña no tenía un objetivo de comprobación sobre la validez mercadotécnica de ésta, se trató sólo de una campaña de emisión de mensaje para hacer observaciones singulares, no de análisis exhaustivo de resultados porque el presupuesto de ejecución era reducido, además no contábamos con una infraestructura sistémica, física, humana, de especialistas, para establecer este alcance, y por último, no teníamos tampoco tiempo suficiente para poderlo realizar de esa manera". La campaña, no tiene ese nivel de profundidad, y tampoco estuvo planteda originalmente de esa manera, de todos modos una respuesta adicional que abre espacio a la reflexión nos parece de interés porque en futuros trabajos similares podemos prever o plantear estudios con mayor alcance y efectividad desde el punto de vista de los resultados validables con identificación inclusive de fuente y receptor.
2. También nos parece de interés que en procesos como estos se pueda contar con nuevas mediciones para poder evaluar y comparar los resultados obtenidos con otros que provienen de dos o más escenarios diferentes y esta validación permitiría entender un poco más si se requiere cambiar alguna dinámica en estudios ulteriores.
3. Se pudieran establecer parámetros de base que permitan indicar

científicamente cuando la divulgación de la información, o la publicidad desarrollada resulte ser positiva, o exitosa. Se podría entender y definir un rango porcentual de respuestas o enlaces al sitio evidenciado o publicitado que permita asociar en un determinado estudio el éxito o fracaso de la publicidad o campaña (No era nuestro propósito). Pongámonos en un ejemplo: Si un "*influencer*" tiene 50.000 seguidores que comparten de manera general una determinada temática, cuando el aplica, pone en evidencia o publica una campaña, cual es el porcentaje esperado de respuestas sobre el total estimado con el que se cuenta, que permita asociar adicionalmente a otros elementos de medida el grado de validez del resultado de ese estudio?.

4. Los resultados de diversos estudios generales que guardan cierta relación con un determinado tema tratado pudieran servir de comparación, también a nivel geográfico, es decir, a nivel regional (interno), de país e internacionalmente, siempre que existan parámetros definidos y resultados confiables o que las instituciones que los realizan son confiables y de reconocido prestigio profesional.
5. La estadística que se basa en procesos aleatorios tiene bien definidos los parámetros y las suposiciones en cuanto a probabilidad asumida o considerada, resultados posibles o esperables, confiabilidad en valor %, el universo necesario de la muestra y otros elementos que se requieren para evidenciar que el estudio sea válido o creíble. Aunque este estudio no establece esta modalidad como metodología del proceso que determina los resultados y la confiabilidad de éstos, así como tampoco las especificaciones reales de ocurrencia del fenómeno, de todos modos nos permitimos adelantar y dar como sugerencia sobre este modelo de estudio para futuros experimentos. Se puede suponer que las estadísticas deben ir ligadas a variables y parámetros objetivos (o esperados) que se establecen al comienzo del estudio, y en función de éstos se organiza y realiza el trabajo.

Reporte narrativo de la CAMPAÑA

"Desenmascara el delito informático, no al fraude en las redes sociales"

Organización responsable: Fundación EsLaRed
En Mérida, Venezuela, el 15 de abril de 2020
Elaborado por: Beatriz Sandia, Sandra Benitez y Edmundo Vitale

1. Describa las actividades desarrolladas en el ámbito del proyecto apoyado por el FRR. Indique si hubo cambios en la propuesta original. (máx. 200 palabras)

En la Etapa 1, se identificaron la tipología, características y forma de ocurrencia de los delitos informáticos más difundidos en las redes sociales a las cuales se acceden en Venezuela. Se hizo un análisis situacional que incluyó el modelo FODA, la descripción del Problema y el esquema general del Árbol del Problema; con los cuales se pudo visualizar y enfocar definitivamente la orientación de la campaña.

La Etapa 2 se dedicó a definir, establecer y preparar la estrategia comunicacional de la campaña. Para ello se recurrió a identificar: el público receptor, el mensaje, la estrategia a seguir en el desarrollo de contenidos, el plan de difusión y los indicadores de resultados a emplear.

La Etapa 3 se dedicó a definir, diseñar y desarrollar los recursos multimedia de apoyo a la campaña y se logró tener disponible un MUESTRARIO DE LOS RECURSOS MULTIMEDIA a ser utilizados.

En la Etapa 4 se desarrolla la campaña de orientación y se crearon diferentes espacios en el entorno de Internet y las redes sociales, como los siguientes: **Sitio Web: http://losdescarados.eslared.net**; **Fan Page: https://www.facebook.com/Descarados-Delitos-101866178089577/?modal=admin_todo_tour ; Instagram: @Los_descaradosdelitos; Twitter: @Los_descaradosdelitos; Youtube: http://youtube.com/channel/UC9sOHdDaToovllNnlmw-bbw** y en **WhatApp:** como la red de base fundamental para compartir los Stikers, Gifs y otros componentes publicitarios o comunicacionales.

No hubo cambios con respecto a la segunda propuesta que se presentó, una vez que se redujo el presupuesto de USD 8,000 a 6.000

2. Describa cual es la situación actual de la emergencia que el proyecto buscó atender. (máx. 200 palabras)

Actualmente la crisis económica, política y social que se vive en Venezuela ha traído como consecuencia un empobrecimiento acelerado de la población, producto de la

escasez de bienes y servicios, así como de la paralización del aparato productivo del país; Igualmente la dificultad para adquirir divisas, gestionar documentos oficiales (pasaportes, partidas de nacimiento, cédula de identidad, otros.) y recibir remesas desde el exterior, ha encaminado a los ciudadanos a requerir de una permanencia mayor en los medios digitales, o a dejar en manos de terceros la solución de sus problemas, generando a su vez una mayor inseguridad en relación a los delitos informáticos que le puedan ocurrir.

En este contexto el Estado de Derecho de los ciudadanos venezolanos es vulnerable y su seguridad digital se encuentra en riesgo, afectando los Derechos de Internet (DI) y los Derechos Económicos, Sociales y Culturales (DESC) de ellos. Particularmente, la situación de fraude en las redes sociales pareciera prolongarse en el tiempo, de no existir mecanismos efectivos para orientar a los ciudadanos sobre el uso adecuado de los medios y los servicios digitales.

Esta campaña encendió estados de alerta y alarma para la protección y el cuidado que debe tener el ciudadano venezolano frente a la realidad antes descrita.

3. ¿Cuáles fueron los resultados alcanzados? ¿Considera que los objetivos del proyecto fueron cumplidos? Incluir indicadores si hay (ej. número de personas alcanzadas, cambios en términos de políticas públicas, etc.). (máx. 400 palabras)

A través de la actividad general en **Instagram,** se observó que a medida que la campaña avanzaba en el tiempo, el alcance se hacía mayor, **pasando de 12.559 personas alcanzadas y 18.395 impresiones en la segunda semana, a tener más de 500.000 personas alcanzadas y 800.000 impresiones, para la cuarta semana**.

Con respecto a las publicaciones *feed/post* de Instagram de las imágenes en JPG y en GIFs, se observó que el **70% de las personas que tuvieron acceso a las 3 imágenes en JPG, correspondían a los grupos comprendidos entre los 13 hasta los 34 años de edad**; esto contrastaba con la edad **de las personas que accedieron a las 3 imágenes en Gifs, donde aproximadamente el 85% se corresponden a los grupos de edad comprendida entre los 35 y 65 o más años de edad (interesante observación).** En relación al género, los datos arrojaron que aproximadamente e**l 65% de la población que tuvo acceso a las imágenes de la campaña correspondía al género femenino.** De igual manera, se observó que la mayor cantidad de la población que tuvo acceso a la campaña se encontraba ubicada en la **zona central (Estados Aragua, y Distrito Capital) y occidental (Estados Zulia y Táchira) del país**.

En referencia a las publicaciones de las imágenes en **Gifs** en la historias de **Instagram**, se observó que el alcance para las tres imágenes fue similar, llegando a un promedio de **130.000 personas alcanzadas.**

En cuanto al alcance logrado en **FaceBook**, se observó que el número de personas involucradas en tan sólo dos semanas de Campaña se había duplicado, **pasando de**

513 a 1.012. En la red social **Twitter** se logró tener un total de **1.718 impresiones, para 1 twit diario durante 21 días**.

En general, podemos concluir que la puesta en marcha de la Campaña "Los Descarados", a pesar de la problemática generada por la pandemia Covid-19, por los cortes eléctricos, la falta de combustible y la falla de los servicios de Internet a la que estamos sometidos en Venezuela, logró tener en el período de ejecución, un final altamente satisfactorio y los objetivos propuestos fueron alcanzados.

Finalmente, se debe mencionar que a la posibilidad de esperar cambios en términos de políticas públicas para favorecer este entorno de incertezas y desaciertos no se debe renunciar, sobre todo porque durante el último año transcurrido se han asomado posibles cambios de rumbo político en el país, como consecuencia de la presión e injerencia que ha tenido la política internacional sobre Venezuela.

4. **¿Cómo consideras que el proyecto ha contribuido para el avance de la protección a los derechos digitales en su país o región?** (máx. 150 palabras)

Si revisamos los resultados obtenidos en la campaña a través de las respuestas conseguidas durante el período de ejecución de ésta en las redes sociales en general, pareciera, y los indicadores mostrados en el 5to informe de la campaña así lo corroboran, que hemos de alguna manera hecho una contribución significativa con los ciudadanos venezolanos en este corto tiempo de desarrollo y aplicación de esta acción de alerta y protección contra el delito informático. Sin embargo, también nos parece justo indicar que en procesos como este es importante poder contar con ulteriores mediciones para poder evaluar y comparar los resultados obtenidos con los precedentes o para expandir el espacio de oferta de la campaña; e inclusive, si fuera posible, comparar resultados con otros que provienen de otros escenarios; en este caso una validación de mayor contingencia permitiría ir a una dinámica de trabajo con mejores expectativas de respuesta y seguimiento de parte de los ciudadanos o usuarios de las redes sociales. La nueva estrategia podría inclusive cambiar algunos parámetros de la oferta artística y publicitaria que envuelve de alguna manera la campaña.

5. **Considerando su experiencia ¿que sugerencias tendrías para futuras ediciones del FRR? (máx. 150 palabras)**

Quizás la principal sugerencia sería la de tomar en cuenta la posibilidad de continuar con el financiamiento de proyectos que ya han sido probados y acompañados a través del FRR, pero que tienen un potencial interesante que les permite trascender de la comunidad de origen o que requieren de nuevas etapas de desarrollo.

El tema de la replicación de experiencias logradas o alcanzadas con una estimación aceptable de éxito y que han sido financiadas por el FRR, deberían ser promovidas

para que puedan experimentar nuevos desempeños en otras comunidades de la región o subregión.

Aunque se trata de un fondo de respuesta rápida y obviamente se refiere al auxilio de propuestas o soluciones de muy corto plazo, el monto a ser dispuesto debería ser aumentado en función del alcance e interés que tiene el proyecto y de la garantía que ofrece la institución que se hace responsable de ejecutarlo.

Sería interesante que el FRR/DD, pueda recurrir a organizaciones de diferentes países de la región para plantearse la solución de problemas comunes en el ámbito de los Derechos Digitales.

Podría ser de interés, que el FRR/DD, queriendo ser el promotor de soluciones a problemas de Derechos Digitales en la región, proponga un temario de posibles ofertas de proyectos a ser realizables y financiables.