Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

CIBERSEGURIDAD: DELITOS Y PROTECCIÓN EN MEDIOS DIGITALES

Santiago, Villalba-Vera[1]
Universidad Autónoma de Encarnación - Paraguay

Recibido: 20/10/2022
Aprobado: 11/02/2025

RESUMEN

Este trabajo analiza los delitos más comunes surgidos en medios digitales, particularmente en Facebook y WhatsApp, debido a su amplio uso tanto personal como laboral. La investigación se justifica en la necesidad de comprender las amenazas presentes en estas plataformas, identificar bases de protección y examinar el marco legal aplicable a los delitos digitales. El objetivo principal es comprender la existencia y el funcionamiento de los ataques cibernéticos vinculados al uso constante de redes sociales, así como la importancia de aplicar de medidas de seguridad para garantizar los derechos de los usuarios y la aplicación de sanciones legales en casos de ilícitos virtuales. Para ello, se llevó a cabo una revisión sistemática de las disposiciones legales vigentes en materia de ciberseguridad, complementada con la lectura de investigaciones científicas sobre el tema. La metodología utilizada es la dogmática jurídica, lo que permite un análisis detallado de la normativa en ciberseguridad y su aplicación en el ámbito regional. Como resultado, se identifican los principales delitos informáticos en estas plataformas, las vulnerabilidades más frecuentes y las respuestas legales disponibles. Se concluye que, si bien existen marcos normativos que regulan estos delitos, es fundamental actualizar y fortalecer la legislación para abordar los riesgos emergentes, además de fomentar la educación digital como una herramienta clave para la prevención.

Palabras-clave: Data protection, Cybersecurity, Cybercrime, Digital media.

[1] Abogado. Especialista en Didáctica Universitaria. Universidad Autónoma de Encarnación. santiago.villalva35@unae.edu.py

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

ABSTRACT

This study analyzes the most common crimes that arise in digital environments, particularly on Facebook and WhatsApp, due to their widespread use for both personal and professional purposes. The research is justified by the need to understand the threats present on these platforms, identify protective measures, and examine the legal framework applicable to digital crimes. The main objective is to comprehend the existence and functioning of cyberattacks linked to the constant use of social networks, as well as the importance of implementing security measures to safeguard users' rights and enforce legal sanctions in cases of virtual offenses. To achieve this, a systematic review of current legal provisions on cybersecurity was conducted, complemented by the analysis of scientific research on the subject. The methodology used is legal dogmatics, which allows for a detailed analysis of cybersecurity regulations and their application at the regional level. As a result, the study identifies the main cybercrimes on these platforms, the most common vulnerabilities, and the available legal responses. It concludes that, although regulatory frameworks exist to address these crimes, it is essential to update and strengthen legislation to tackle emerging risks, as well as to promote digital education as a key tool for prevention.

Keywords: Cybersecurity, Cyberattack, digital media.

1. Introducción

La creciente expansión y dependencia de las tecnologías de la información y la comunicación (TIC) han transformado la forma en que interactuamos en la sociedad, tanto a nivel personal como profesional. En particular, plataformas digitales ampliamente utilizadas como Facebook y WhatsApp han creado nuevos espacios para la comunicación, pero también han puertas a una variedad de riesgos y delitos cibernéticos. Esta investigación tiene como objetivo explorar los delitos más comunes en estos medios digitales, identificar las amenazas que se presentan en ellos y analizar las medidas básicas de protección que los usuarios pueden adoptar para salvar su

información personal. Además, se examinan las implicancias jurídicas de los ciberdelitos en Paraguay, analizando la normativa vigente en materia de ciberseguridad y las opciones legales para que los usuarios puedan defender sus derechos frente a estos ataques. A través de una metodología dogmática jurídica, se pretende ofrecer un análisis detallado de la legislación paraguaya, identificar los desafíos que enfrenta el sistema legal y proponer estrategias de seguridad más efectivas para mitigar los riesgos asociados con los delitos informáticos en el ciberespacio (Cruz Pérez y otros, 2019).

2. Objetivos, metodología y límites de la investigación

Esta investigación tiene como objetivo identificar los delitos más comunes que ocurren en medios digitales, especialmente en Facebook y WhatsApp, plataformas ampliamente utilizadas tanto a nivel personal como profesional. Además, busca analizar las principales amenazas en estos espacios, identificar medidas básicas de protección para resguardar la información personal y comprender cómo funcionan los ciberataques, destacando la importancia de la seguridad digital para reducir riesgos. También se examina el marco legal vigente en materia de ciberseguridad y las opciones legales disponibles para que los usuarios puedan defender sus derechos en caso de sufrir un delito digital.

Para ello, se realizó una aproximación literaria de las normativas actuales y se analizaron estudios científicos sobre el tema, utilizando el método de dogmática jurídica, que permite un examen detallado de las leyes aplicables en el ámbito regional. Esta metodología facilita el análisis de la ciberseguridad desde una perspectiva legal, proporcionando conocimientos sobre sus implicaciones jurídicas y resaltando las ventajas que ofrecen los medios digitales en términos de acceso a la información, comunicación y desarrollo tecnológico.

En cuanto a los límites de la investigación, el estudio se enfoca en los delitos digitales dentro de Facebook y WhatsApp, abordando su regulación en el contexto regional sin profundizar en normativas internacionales. Asimismo, aunque se analizan las principales amenazas y estrategias de protección, no se desarrollan aspectos técnicos avanzados sobre ciberseguridad.

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

3. Resultados

3.1 Ciberseguridad

Existe una carencia de una definición propia para este término, tal es así que la comunidad internacional cuenta con una postura en referencia al significado de esta palabra, mientras que algunos Gobiernos o Estados mantienen diferencias con la comunidad cibernética. Así pues Carlini (2016), sostiene que la ciberseguridad es el conjunto de mecanismos informáticos cuya esencia es la prevención de las combates cibernéticos, donde la consecuencia directa es el perjuicio de datos personales, bienes y activos de organismos estatales, además de la exposición de informaciones con carácter de seguridad nacional etc.

El mismo autor abordar el contenido de ciberseguridad es una tarea difícil, pues es un tema de actualidad y de mucha amplitud, desde la aparición de la internet y por consiguiente los sistemas informáticos provocaron un cambio radical en la vida de cada persona en el mundo al igual a los gobiernos mundiales, donde cada accionar se evidencia en la red, esta red es un espacio virtual donde cada sujeto o individuo crea, construye y por supuesto evoluciona.

Debido a este nuevo espacio virtual o cibernético, se dejó en evidencia una nueva oportunidad, la oportunidad de los ciberterrorismos, los ciberdelitos, estos delitos informáticos aparecen de múltiples formas, desde pequeñas escalas a grandes escalas, su misión principal es la obtención de información confidencial (Carlini, 2016).

La ciberseguridad es un paradigma, pues desde la existencia y la introducción del espacio cibernético que sin dudad posee múltiples beneficios a la colectividad, contrae también un nuevo espacio, el espacio de la criminalidad virtual, es por ello por lo que se necesita la seguridad en ese espacio virtual. La presente investigación pretende demostrar las medidas de seguridad básicas que una persona debe realizar al momento de interactuar en este espacio cibernético, además de resaltar los hechos ciberdelitos más comunes en la sociedad paraguaya y por sobre todo identificar los tipos penales aplicables al caso (Carlini, 2016).

3.2 Ciberdelito o cibercriminalidad

Para Maroto (2016), el ciberdelito o la cibercriminalidad consiste en una serie de operaciones cibernéticas por la cuales se realizan ataques cibernéticos tendientes al robo

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

y la venta de datos, este sistema de ataques es efectuado a través de la distribución de mensajes no deseados (Spam), asimismo obtener direcciones IP, datos de carácter personal o simplemente información confidencial de organismos o entidades, en ese sentido la o las personas que intervienen en estas operaciones pueden robar y vender al mejor postor dichas informaciones.

En un mundo interconectado, donde una persona cuenta con información al instante y a la vez estar en comunicación directa con otras personas en cualquier parte del mundo, crea ese espacio cibernético en el cual la persona es blanco directo para los ciberdelincuentes que no conocen fronteras, pues los ataques son realizados a miles de quilómetros, de ahí se crea la interrogante ¿Qué ley es la aplicable?, una vez cometido el ciberataque es extremadamente difícil la identificación del autor material del hecho pues el rastro en la red es eliminado cada minuto (Maroto, 2016).

Según González y otros (2015), en la actualidad se pueden dar un sin números de ejemplos de ciberataques como ser: ataque del gusano, que básicamente consiste en causar daño a una unidad informática a través de códigos cibernéticos, esto puede efectuarse de forma directa o indirecta.

Otro caso resonante es el ataque del gusano Nimda, este ciberataque causo un gran daño a cientos de miles de usuarios del sistema operativo de Windows pues los ciberdelincuentes infectaron los servidores de esta compañía en varias partes del mundo, obteniendo de esta forma datos considerablemente confidenciales (Gualpa Cando & Rubio Rubio, 2011).

3.3 Ciberamenaza

Según Pierre (2017), amenaza es representación, una señal una disposición, o manifestación percibida como el anuncio de una situación no deseada o de riesgo para la existencia de quien la percibe, dicho esto la ciberamenaza es una acción desarrollada en el ciberespacio, como se ha mencionado anteriormente, en orden de ideas.

Tossi (2015) señala que la ciberamenza es el dominio interactivo que se compone por los medios digitales utilizados para modificar, almacenar y comunicar informaciones de sitios de internet, además de otros tipos de sistemas de datos utilizados por empresas, organizaciones, Estados etc.

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

Es sabido que desde la llegada de internet, millones de personas se encuentran conectadas a través de medios digitales, incluyendo empresas y naciones, ahora bien, la internet hace funcionar instalaciones, infraestructuras como telecomunicaciones, bancos, servicios de emergencias y fuerza pública, entre estos se destacan las Fuerzas Armadas y la Policía Nacional, además los servicios vitales de diversas características, en ese contexto la economía al igual que la seguridad de una nación dependen de la internet y de los medios digitales; por consiguiente son objeto de ciberataques.

3.4 Medios digitales

Los medios digitales abarcan cualquier tipo de contenido codificado en un formato que pueda ser procesado por dispositivos electrónicos. Esto permite su creación, visualización, distribución, modificación y almacenamiento a través de diversas herramientas tecnológicas. Entre los ejemplos más comunes de medios digitales se encuentran los programas informáticos y software, imágenes y vídeos en formato digital, videojuegos, páginas y sitios web, redes sociales, bases de datos, archivos de audio como MP3 y libros electrónicos (Grillo, 2019).

De lo expuesto anteriormente se puede entender que los medios digitales son todo aquel ciberespacio que utiliza internet destinado a la comunicación, en virtud del cual se produce el intercambio masivo de informaciones y contenidos de todo tipo, este ciberespacio puede ser utilizado para múltiples fines como ser noticias, difusión de bienes y servicios, bloggers entre otros, por otra parte los medios digitales más utilizadas en el mundo son sin dudas las redes sociales, ellas pueden ser: Facebook, Whatsapp, Snapchat, Twitter, Instagram, Messenger, Gmail, etc.

Los medios digitales citados precedentemente son las más utilizadas en el Paraguay, el uso continuo de estos medios digitales crea una oportunidad para el ciberdelincuente, así pues, surge la necesidad de conceptualizar los medios digitales más utilizados en Paraguay (Ministerio de Tecnologías de la Información y la Comunicación, 2022)

3.4 Facebook

Según Sans (2008), Facebook es una herramienta digital de uso social por medio del cual conecta a personas que se encuentran alrededor, se entiende que es una red social tendiente a la creación de una comunidad que interactúa entre sí, son variadas las

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

ventajas de esta red social por ejemplo poder incluir amigos, invitación a otros que no utilicen esta red social, solicitudes de amistad, apoyo de juegos, películas o libros favoritos, entre muchos otros, es decir, una vez creado el perfil, aparecen una gran cantidad de datos de carácter privado que se vuelven públicos.

Estos datos relevantes son el nombre, la edad, el domicilio, el grupo de amigos, los familiares, las cosas que pueden gustar al usuario; incluso un muro donde se comparte informaciones sobre eventos u actividades recientes, en fin, son tantos los datos de carácter personal que son expuestos al público abiertamente y es ahí que surgen los ciberataques (Sans, 2008).

Aquí el ciberdelincuente puede acceder, además de datos personales, a la imagen personal y de ello poder filtrarlo en portadas de páginas pornográficas, crear perfiles falsos usando la imagen personal de una persona y con ello hacer un sinfín de ilícitos, por ejemplo: extorciones, suplantaciones de identidad0, sextorción, pornografía infantil, etc.

3.5 WhatsApp Messenger

WhatsApp es una aplicación de carácter informático, destinada a la mensajería digital instantánea que opera en distintos software y sistemas operativos, como ser: Windows, Smartphone, Android, Apple entre otras más, la ventaja principal de este medio digital es la interacción constante entre las compañías citadas (Lozano y otros, 2019).

WhatsApp Messenger es sin lugar a dudas uno de los medios digitales más utilizados en el Paraguay, esto es debido a la versatilidad de esta aplicación que permite al usuario la interacción, compartiendo videos, audios, imágenes, notas de voz, archivos, documentos de todo tipo, además permite comunicación a través de la mensajería, actualización de estados de actividades recientes, cabe añadir la gran importancia de esta aplicación en el uso cotidiano de las empresas o simplemente como herramienta de trabajo, en este supuesto la aplicación puede conectarse a una computadora portátil por medio del Whatsapp Web, facilita la edición de trabajos, en fin, una infinidad de beneficios (Lozano y otros, 2019).

La facilidad de uso de esta aplicación, junto con la gran cantidad de datos e información que maneja, la convierte en un blanco atractivo para los ciberataques. En

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

este contexto, según el Ministerio Público, los delitos más frecuentes en Paraguay incluyen la usurpación de identidad, la extorsión, la sextorsión, la estafa y la difusión (Publico, 2020).

Como se ha mencionado precedentemente el uso cotidiano de esta red social es lo que la vuelve vulnerable, pues existen debilidades en el uso de la aplicación, y que, sin la debida precaución, el usuario puede ser usurpado de su identidad, a consecuencia del desconocimiento de las medidas básicas de seguridad en esta red, de aquí se genera uno de los problemas del uso de esta red social.

3.6 Tipificación de los ilícitos informáticos

Los medios se realizan en el ciberespacio y en este espacio se administran una innumerable cantidad de datos de carácter privado, por medio del cual funciona el sistema informático, por lo tanto, el bien jurídico a proteger es la información.

El código penal paraguayo sufrió modificaciones en el año 2012, por medio del cual se introdujo la Ley Nº 4339 donde se modifican varios artículos de la citada normativa, entre ellos:

Art. 140.- Pornografía relativa a niños y adolescentes.

La pornografía infantil y/o de adolescentes, queda netamente prohibida en el Paraguay, por ende, la producción y publicación de contenido sexual que involucre niños y adolescentes menores a 18 años o la simple exhibición de las partes genitales de los mismos es castigada según la citada normativa, ahora bien, el quid de la cuestión para la presente investigación se encuentra en el inciso tres.

El presente inciso trata sobre la distribución y la difusión de publicaciones pornográfica infantil, he aquí donde los medios digitales tiene su implicancia, pues a través de estos medios como ser Facebook y Whatsapp, se configura la conducta descripta en la norma, por consiguiente es necesario que la sociedad maneje cierto tipos de medidas de seguridad a fin de evitar que sus propios hijos/as sean blancos de ciberataques y que la imagen de estos sean difundidas por toda internet, en este supuesto la pena prevista es de hasta cinco años o multa.

Artículo 146 c.- Interceptación de datos.

Los ciberataques son realizados en el ciberespacio, es así como estos ciberdelicuentes pueden realizar varios hechos punibles en este espacio, la intercepción

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

de datos es la más frecuente, cabe señalar que este hecho se encuentra tipificado en el ordenamiento normativo penal del Paraguay y la conducta castigada en ese supuesto es la obtención a datos de carácter privado y que con ello lo transfiera será castigado con una pena de hasta dos años o multa.

Para evitar este tipo de ciberdelito la posible victima necesariamente debe tener una seguridad robusta en sus contraseñas personales, sean estos de medios digitales o cuentas bancarias, en virtud de ello el ciberdelincuente tardaría años en poder descifrar dichas contraseñas y, por ende, los datos de carácter personal se salvaguardarían.

Artículo 174 b.- Acceso indebido a sistemas informáticos.

En este supuesto penal priman la desautorización y la violación de sistemas de seguridad, aquí el ciberdelincuente, al acceder indebidamente los sistemas e seguridad se alza con una gran cantidad de datos e informaciones privadas, la norma prevé para esta conducta un marco penal de pena privativa de libertad de hasta tres años o multa

Art. 175.- Sabotaje de sistemas informáticos.

El sabotaje de sistemas informáticos es el hecho punible por medio del cual el ciberdelicuente realiza una serie de conductas descriptas en la norma, la obstaculización la destrucción, inutilización, la sustracción o la simple alteración de un sistema informático da lugar a una sanción de pena privativa de libertad de hasta cinco años o multa, también se encuentra prevista la tentativa.

Artículo 175 b.- Instancia

Cabe señalar que, en la presente normativa, la persecución penal depende de la víctima, salvo que la protección de los datos sea de interés público.

Artículo 188.- Estafa mediante sistemas informáticos.

La estafa mediante los sistemas informáticos es hoy en día es uno de los delitos informáticos más cometido en el Paraguay, aquí el ciberdelincuente a través del uso indebido de datos personales y muchas de las veces con el plus de la amenaza crea para un beneficio patrimonial indebido, este tipo de hecho es realizado netamente por los medios digitales como ser Facebook y WhatsApp.

Al presente análisis se debe incorporar el ciberataque conocido como sextorsión. Según Isamara Valeska Vargas Urbina, este delito consiste en la intimidación a través

de las Tecnologías de la Información y la Comunicación (TIC), mediante la cual una persona es extorsionada bajo la amenaza de divulgar imágenes (Urbina, 2019).

4. Conclusiones

Luego de indagar conceptos en referencia al tema y del análisis del ordenamiento normativo penal se evidencia que Paraguay necesita implementar una política criminal cibernética sobre la problemática de ciberseguridad.

Sin dudas el creciente avance de las TIC, Tecnologías de la Información y la Comunicación repercute plenamente a la población mundial y el Paraguay no es la excepción, este tipo de tecnologías impacta de sobre manera a la sociedad paraguaya, esto debido a que la mayor parte de la población se encuentra conectada e interactuando unos con otros.

La utilización de los medios digitales se ha vuelto indispensable para la vida cotidiana, por consiguiente esto crea conductas comunes entre los adultos y los jóvenes en general, esto a su vez ha generado conductas delictivas, por la gran exposición de datos e información de carácter privado, ahora bien, cuando la interacción ocurre en el marco de relaciones afectivas, los datos como ser imágenes personales, permite su vulneración y en el peor de los casos la violación de datos de carácter personal.

En resumen, luego del análisis de la legislación penal en referencia a los delitos informáticos, además de indagar diferentes definiciones y conceptos sobre el tema en cuestión, se concluye que el fenómeno de la ciberseguridad es un tema de actualidad por lo tanto genera la necesidad de adecuar el sistema jurídico nacional a los estándares internacionales, con ello logrará dar respuestas a los ciberdelitos cotidianos, por ejemplo, la Sextorsión.

Como consecuencia de la constante interacción a través de los medios digitales trae consigo una de las mayores vulnerabilidades, y esta a su vez provoca que el ciberespacio sea el ámbito donde se necesita mayor defensa a los datos de carácter personal y la seguridad a la información.

Paraguay necesita la creación de políticas cibernéticas para luchar contra los ciberdelincuentes, la carencia de infraestructura es uno de los principales factores, además es indispensable la creación de una serie de ordenamientos normativos a fin de poder describir conductas al igual que definiciones sobre ciberseguridad, asimismo

Saeta Digital
Tecnología, Diseño e Innovación
ISSN: 2523-241X
Vol. 8 Núm. 1 (2022)

llevar a cabo la implementación de planes, estrategias o medidas preventivas en materia de ciberseguridad.

Recomendaciones para la utilización de la red social de Facebook

- No aceptar perfiles con pocos amigos en común y pocas fotografías.
- No ceder ante la extorción de los ciberdelincuentes que piden sumas de dinero a cambio de no difundir las fotografías de las víctimas.
- Bloquear números que envíen mensajes y no responderlos.
- No ingresar a sitios dudosos.
- No brindar información personal.

Consejos

- No aceptar perfiles en las redes sociales que contengan pocas fotos o amistades, o poca información.
- Proteger los datos personales en las redes sociales, no brindarla en caso de ser posible.
- No publicar fotos del lugar de trabajo, estudio, entre otros.
- No brindar información personal a personas extrañas, como dirección, lugar de residencia, lugar de trabajo, además correo electrónico, contraseñas o códigos de las tarjetas de créditos o cuentas bancarias.
- No ceder ante la extorsión de los ciberdelincuentes y una vez que reciben amenazas, denunciar lo más rápido posible al Departamento de Anticorrupción de la Policía Nacional o a cualquier comisaria de su localidad.
- No ingresar a las páginas que no son certificadas. Los enlaces certificados contienen en el lado superior izquierdo un candadito cerrado, lo que significa que la navegación es segura.
- No descargar videos y no visitar páginas donde se consume pornografía infantil

5. Bibliografía

Carlini, A. (2016). *Ciberseguridad: un nuevo desafío para la comunidad.*

Cristián J. Bravo, P. E. (marzo de 2018). *Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile*. Obtenido de Aceptación del Reconocimiento Facial Como Medida de Vigilancia y

Seguridad: Un Estudio Empírico en Chile: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000200115

Gualpa Cando, E. & Rubio Rubio, D. A. (2011). *ANÁLISIS Y ESTUDIO DE LOS VIRUS Y ANTIVIRUS INFORMÁTICOS DEL MERCADO LOCAL. CASO PRÁCTICO ELABORACIÓN DE UN VIRUS QUE RECOPILE LA MAYOR CANTIDAD DE PROCESOS QUE PUEDEN CAUSAR DAÑOS EN LOS COMPUTADORES.* LATACUNGA, ECUADOR. Obtenido de https://repositorio.utc.edu.ec/server/api/core/bitstreams/c3c62a1b-5b34-4cc8-a9fa-f3ed103a25b0/content

González, J. A., Pérez Meana , H., & Guevara López, P. (2015). Gusanos. Obtenido de https://www.amc.edu.mx/revistaciencia/images/revista/66_3/PDF/Gusanos.pdf

Grillo, O. (2019). Itinerarios de la antropología. *Consejo Latinoamericano de Ciencias Sociales*, 21-31.

Ministerio de Tecnologías de la Información y la Comunicación. (MITIC). (2022). *Estado de la Ciberseguridad en Paraguay.* MITIC chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf

Ley N° 4339/2011. (2011). *Aprueba la carta acuerdo para la donación SFLAC N° TF-096017, proyecto de fortalecimiento de la Contraloría General de la República por UD 330.200 dólares de los Estados Unidos de América, suscrita con el Banco Internacional de Reconstrucción y Fomento (BIRF), que estará a cargo de la Contraloría General de la República, y amplía el presupuesto general de la Nación para el ejercicio fiscal 2011, aprobado por Ley N° 4249 del 12 de enero de 2011.* Cámara de Senadores. https://www.bacn.gov.py/leyes-paraguayas/3709/ley-n-4339-aprueba-la-carta-acuerdo-para-la-donacion-sflac-n-tf-096017-proyecto-de-fortalecimiento-de-la-contraloria-general-de-la-republica-por-ud-330200-dolares-de-los-estados-unidos-de-america-trescientos-treinta-mil-doscientos-suscrita-con-el-banco-internacional-de-reconstruccion-y-fomento-birf-que-estara-a-cargo-de-la-contraloria-general-de-la-republica-y-amplia-el-presupuesto-general-de-la-nacion-para-el-ejercicio-fiscal-2011-aprobado-por-ley-n-4249-del-12-de-enero-de-2011

Lozano, M. B., Uribe Luna, S., Benigno Barragán Sánchez, B., & Vázquez Varga, I. F. (2019). *EL WHATSAPP COMO MEDIO DE COMUNICACIÓN E INTERACCIÓN EN LA COMUNIDAD UNIVERSITARIA*.

Maroto, J. P. (2016). EL CIBERESPIONAJE Y LA CIBERSEGURIDAD. *CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL*, 46-76. Obtenido de https://dialnet.unirioja.es/descarga/libro/548996.pdf

NACIONAL, C. (1992). *CONSTITUCION NACIONAL*. ASUNCION.

NACIONAL, C. (1992). *CONSTITUCION NACIONAL*. ASUNSION .

ONU. (s.f.). *DECLARACION UNIVERSAL DE DERECHOS HUMANOS.*

Pierre, H. L. (2017). Amenaza. Concepto, clasificación y proceso de securitización. *Amenazas globales, consecuencias locales Retos para la inteligencia estratégica actual*, 7-32.

Publico, M. (2020). Obtenido de #DelitosInformaticos ¿Cómo te pueden robar tu cuenta de Whatsapp con llamada de Verificación?: https://ministeriopublico.gov.py/nota/delitosinformaticos-como-te-pueden-robar-tu-cuenta-de-whatsapp-con-llamada-de-5501

Sans, A. G. (2008). Las Redes Sociales como Herramientas para el Aprendizaje Colaborativo: Una Experiencia con Facebook. *RE-Presentaciones Periodismo, Comunicación y Sociedad*, 48-63.

TOSSI, A. A. (2015). CONSIDERACIONES SOBRE LA CIBERAMENAZA A LA SEGURIDAD. *Revista Política y Estrategia*, 83-94. Obtenido de https://www.politicayestrategia.cl/index.php/rpye/article/download/44/162

Urbina, I. V. (2019). “SEXTING Y SEXTORSIÓN SEGÚN LEY No.779, LEY INTEGRAL CONTRA LA VIOLENCIA HACIA LAS MUJERES. *Revista de Derecho de la Facultad de Ciencias Jurídicas y Sociales*. Obtenido de https://revistas.unanleon.edu.ni/index.php/revistadederecho/article/download/167/142/195