

UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO
PETAENG



TRABAJO DIRIGIDO

**“EL PAPEL DEL INTERNET COMO HERRAMIENTAS DE EDUCACIÓN Y
CONOCIMIENTO PARA LA PREVENCIÓN DE DELITOS
INFORMÁTICOS EN LA UNIDAD DE ANÁLISIS EN BOLIVIA DEL
INTERNET**

(Para optar al grado de Licenciatura en Derecho)

POSTULANTE : PAMELA IVLIN PERALTA AREQUIPA

TUTOR : DR. RUDY CHAVEZ SALAZAR

LA PAZ – BOLIVIA
2022

RESUMEN

Ante el avance extraordinario de las nuevas tecnologías, el impacto que ha tenido el Internet y las Redes Sociales, ha conducido que existan nuevas formas de comunicación que podrían encontrarse diferentes partes del mundo este fenómeno mundial otorga grandes beneficios, pero de la misma manera ofrece un aspecto negativo cuando personas inescrupulosas utilizan este medio como instrumento para cometer cualquier tipo de delitos de tal manera viendo la necesidad de dar mayor conocimiento y formación a los estudiantes, ya que la tecnología se ha convertido en una herramienta indispensable en su vida diaria.

A través del desarrollo se explica los riesgos asociados del mal uso de las redes sociales y la influencia que tienen en los estudiantes, el impacto de las TIC en la educación tomando en cuenta una buena formación sobre el uso de las tecnología tanto en la formación del docente sobre nuevos métodos de aprendizaje que deben adoptar los profesores al momento de implementar como una herramienta educativa hacia los estudiantes, dando a conocer con mayor profundidad las ventajas y desventajas que tienen las redes sociales.

La finalidad principal es dar a conocer sobre los usos legales de la información, sobre los diferentes Delitos Informáticos que se podrían cometer al momento de ingresar a diferentes páginas de redes sociales que son prohibidas.

Haciendo una mención principal sobre los principales peligros en la internet que pueden estar en constante riesgo los estudiantes, al tener mayor conocimiento sobre de un buen uso de la Internet se podría prevenir diferentes tipos de delitos informáticos.

ÍNDICE

DISEÑO DE LA INVESTIGACIÓN.....	1
I. TEMA.....	1
II. JUSTIFICACIÓN DEL TEMA.....	1
III. IDENTIFICACIÓN DEL PROBLEMA.....	1
IV. PLANTEAMIENTO DEL PROBLEMA.....	2
A) PROBLEMA GENERAL.....	2
B) PROBLEMAS ESPECÍFICOS.....	2
V. DELIMITACIÓN DEL TEMA.....	2
A) DELIMITACIÓN ESPACIAL.....	2
B) DELIMITACIÓN TEMPORAL.....	2
VI. OBJETIVOS.....	3
6.1. OBJETO GENERAL.....	3
6.2. OBJETIVOS ESPECÍFICOS.....	3
VII. METODOLOGÍA DE LA INVESTIGACIÓN.....	3
7.1. TIPO DE INVESTIGACIÓN.....	3
7.2. MÉTODOS DE INVESTIGACIÓN.....	4
7.2.1. MÉTODO INDUCTIVO.....	4
7.2.2. MÉTODO DEDUCTIVO.....	4
7.2.3. MÉTODO ANALÍTICO.....	5
7.3. TÉCNICAS DE INVESTIGACIÓN.....	5
CAPITULO I.....	6
1. MARCO HISTÓRICO.....	6
1.1. LA INTERNET Y SU ORIGEN.....	6
1.2. <i>INCURSIÓN DE LA INTERNET EN BOLIVIA</i>	7
1.3. Historia de las redes sociales en Bolivia.....	10
1.4. EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS.....	11
CAPITULO II.....	16
1. MARCO TEÓRICO Y CONCEPTUAL.....	16
1.1. INTERNET.....	16
1.2. IMPORTANCIA DE LA INTERNET EN LA EDUCACIÓN.....	18
1.3. DEFINICIÓN REDES SOCIALES.....	19
1.4. CARACTERÍSTICAS DE LAS REDES SOCIALES.....	21

2.	TIPOS DE REDES SOCIALES	21
2.1.	Las redes de tipo generalista	21
2.2.	Redes específicas	22
2.3.	Redes Horizontales	22
2.4.	CLASIFICACIÓN DE LAS REDES SOCIALES	22
3.	VENTAJAS Y DESVENTAJAS DE LAS REDES SOCIALES	25
3.1.	Ventajas de las redes sociales	25
3.2.	Desventajas de las redes sociales	26
4.	RIESGOS ASOCIADOS AL USO DE LAS REDES SOCIALES	27
5.	INFLUENCIA DE LAS REDES SOCIALES	28
6.	REDES SOCIALES COMO HERRAMIENTA DE APRENDIZAJE	31
7.	IMPACTO DE LAS TIC EN LA EDUCACIÓN	32
8.	USO DE LA INFORMACIÓN EN EL INTERNET	33
9.	FORMACIÓN SOBRE EL USO DE LA TECNOLOGÍA	35
9.1.	Formación docente	35
9.2.	Formación escolar	36
9.3.	EL USO DEL INTERNET Y EL USO LEGAL DE LA INFORMACIÓN	37
9.4.	DELITOS INFORMÁTICOS Y USO DE LAS REDES SOCIALES	38
10.	DELITOS INFORMÁTICOS	39
10.1.	CONCEPTO DE DELITOS INFORMÁTICOS	39
10.2.	CARACTERÍSTICAS DEL DELITO INFORMÁTICO	41
10.3.	CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS	42
10.4.	SUJETOS Y RELACIONES QUE SURGEN DEL DELITO INFORMÁTICO	43
11.	PERFIL CRIMINOLÓGICO	45
12.	PRINCIPALES PELIGROS EN INTERNET	44
12.1.	ACOSO CIBERNÉTICO	46
12.2.	ROBO DE IDENTIDAD	44
12.3.	SPAM O CORREO BASURA	47
12.4.	INFORMACIÓN NOCIVA	45
12.5.	PIRATERÍA	48
12.6.	PORNOGRAFÍA	48
12.7.	ACOSO SEXUAL O GROO MING	48
12.8.	AMENAZAS A LA PRIVACIDAD SEXTING	49
12.9.	REVELACIÓN DE INFORMACIÓN	46

12.10. DELITOS ECONÓMICOS Y FRAUDES	49
CAPITULO III	47
1. LEGISLACIÓN NACIONAL.....	48
1.1. CONSTITUCIÓN POLÍTICA DEL ESTADO.....	50
1.2. DECRETO SUPREMO N° 27329 “TRANSPARENCIA Y ACCESO A LA INFORMACIÓN”	51
1.3. LEY N° 164 “LEY GENERAL DE TELECOMUNICACIONES, TECNOLÓGICAS DE INFORMACIÓN Y COMUNICACIÓN”	52
1.4. LEY N° 341 “LEY DE PARTICIPACIÓN Y CONTROL SOCIAL”	50
1.5. DECRETO SUPREMO N°27330 “SIMPLIFICACIÓN DE TRAMITES EN LA ADMINISTRACIÓN PUBLICA”	53
1.6. DECRETO SUPREMO N°1391 “REGLAMENTO 1391 “REGLAMENTO A LA LEY N°164”	54
1.7. DECRETO SUPREMO N° 1793 “REGLAMENTO PARA EL ACCESO, USO Y DESARROLLO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” .	55
1.8. DECRETO SUPREMO N° 2514 “CREACIÓN DE LA AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN”	56
1.9. LEY 777 “LEY DEL SISTEMA DE PLANIFICACIÓN INTEGRAL DEL ESTADO SPIE”	56
1.10. LEY Nª 779 “DESBUROCRATIZACIÓN PARA LA CREACIÓN FUNCIONAMIENTO DE UNIDADES ECONÓMICAS”	56
1.11. DELITOS INFORMÁTICOS CÓDIGO PENAL BOLIVIANO	57
1.12. CÓDIGO NIÑO, NIÑA ADOLECENTE	55
1.13. DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS “ONU”	58
CAPITULO IV	62
MARCO PRACTICO	62
1. RESULTADOS DE LA ENCUESTA	62
CAPITULO V	65
CONCLUSIONES Y RECOMENDACIONES.....	65
1. CONCLUSIONES	65
2. RECOMENDACIONES	66
BIBLIOGRAFÍA	68

DISEÑO DE LA INVESTIGACIÓN

I. TEMA

EL PAPEL DEL INTERNET COMO HERRAMIENTAS DE EDUCACIÓN Y CONOCIMIENTO PARA LA PREVENCIÓN DE DELITOS INFORMÁTICOS EN LA UNIDAD DE ANÁLISIS EN BOLIVIA DEL INTERNET

II. JUSTIFICACIÓN DEL TEMA

El presente trabajo está enfocado como tema inicial el dar a conocer que tan importante es el conocimiento del buen uso del internet con respecto a la prevención de los delitos informáticos en los estudiantes.

La generación que utiliza hoy las nuevas tecnologías de información tiene la suficiente capacidad de comprender, y la habilidad para reconocer cuando se necesita la información adecuada o requerida, por lo que representa un desafío de la educación poder implementar mecanismo de enseñanza o métodos de prevención con respecto a los riesgos que están expuestos los estudiantes al caer en delitos informáticos.

III. IDENTIFICACIÓN DEL PROBLEMA

Con la aparición de las nuevas tecnologías con el uso del internet o redes sociales sin duda ha traído grandes beneficios en el desarrollo e implementación más adentrada a las tecnologías de la información y comunicación en la educación ya que las nuevas generaciones adoptan con mucha naturalidad el uso de las tecnologías en todas las actividades facilitándonos a hacer muchas de nuestros temas, como ser la obtención más fácil de información, la consulta de bibliotecas virtuales de diversas partes del mundo, o solamente para el uso personal de entretenimiento como la creación de plataformas digitales de redes sociales como el Facebook, twitter, Instagram y mensajería instantánea (WhatsApp).

Sin embargo, la delincuencia ha hecho uso de todo el medio informático que, al no tener un conocimiento adecuado de la utilización del internet o redes sociales, se

podría llegar al uso excesivo de páginas de internet prohibidas provocando una serie de delitos informáticos.

IV. PLANTEAMIENTO DEL PROBLEMA

A) PROBLEMA GENERAL

A partir del conocimiento del uso de las tecnologías de la información y la comunicación global y satelital, internet, el correo electrónico, redes sociales etc. Los estudiantes quedaron expuestos por las vulnerabilidades del mal uso del internet, a pesar que ha sido un beneficio enorme en todos los contextos.

B) PROBLEMAS ESPECÍFICOS

¿De qué manera se relaciona el internet y la educación en los jóvenes?

¿De qué manera se relaciona los delitos informáticos con el internet?

¿De qué manera se relaciona el uso de redes sociales en Gral. FACEBOOK, WHATSAPP, TWITTER, INSTAGRAM, ¿para cometer delitos informáticos?

¿Qué aplicaciones tienen las TICS en la sociedad mundial?

V. DELIMITACIÓN DEL TEMA

La presente investigación está focalizada en la educación, conocimiento y prevención de los delitos informáticos más frecuentes en los estudiantes de secundaria.

A) DELIMITACIÓN ESPACIAL

La presente investigación se realizara en la ciudad de La Paz a estudiantes del eje central por ser los que mas uso le dan a las redes sociales.

B) DELIMITACIÓN TEMPORAL

Para la investigación se tomará como punto de partida el sistema actual del conocimiento del delito informático.

VI. OBJETIVOS

6.1. OBJETO GENERAL

Conocer el nivel de educación y conocimiento sobre el uso del internet al momento de la comisión de delitos informáticos y las repercusiones legales que podrían darse.

6.2. OBJETIVOS ESPECÍFICOS

Identificar las causas principales que llevan a los estudiantes a cometer delitos informáticos.

- Analizar de qué manera puede ser utilizado el internet como medio de educación para la prevención de los delitos informáticos.

- Determinar las ventajas y desventajas que tiene el uso del internet en los estudiantes.

- Mencionar los delitos informáticos más frecuentes cometidos por los estudiantes al momento de utilizar las redes sociales.

- Plantear mecanismos de estudio que tomen en cuenta las prácticas educacionales en los estudiantes con respecto a los delitos informáticos.

- Determinar la consecuencia legal que podrían tener al momento de la comisión de un delito informático

VII. METODOLOGÍA DE LA INVESTIGACIÓN

7.1. TIPO DE INVESTIGACIÓN

La presente monografía se trata de un trabajo de investigación científica de carácter educativo, informativo, porque recogerá elementos bibliográficos en los que se abordara diversos puntos de vistas crítico reflexivo sobre el tema en cuestión y hacer

una exposición de los diferentes términos en el área del derecho y el propio de las tecnologías de la información y la comunicación para dar claridad a la hora de aplicar los instrumentos de recopilación de la información y que se pudiera lograr una respuesta eficaz aproximada a la realidad del tema.

La falta de conocimiento y herramientas apropiadas y las buenas prácticas del uso del internet en los estudiantes se debería recurrir a diversas formas de uso de la información y los efectos que tiene el uso inapropiado de las redes sociales.

7.2. MÉTODOS DE INVESTIGACIÓN

7.2.1. MÉTODO INDUCTIVO

Uno de los métodos empleados en el presente trabajo de investigación es el método inductivo. El método inductivo es el “proceso de conocimiento que se inicia con la observación de fenómenos particulares con el propósito de señalar las verdades generales que pueden ser aplicadas a situaciones similares a la observada” (Carlos, 2020).

7.2.2. MÉTODO DEDUCTIVO

Se emplea este método porque se efectúa un estudio de los aspectos teóricos y conceptuales para poder identificar la problemática en cuestión para posterior poder definida la investigación con referente a los adolescentes reclusos de su libertad.

El método deductivo es el “proceso de conocimiento que se inicia con la observación de fenómenos generales con el propósito de señalar verdades particulares que pueden ser aplicadas a situaciones similares a la observada”.

7.2.3. MÉTODO ANALÍTICO

Este método comprende el “proceso de conocimiento que se inicia por la identificación de cada una de las partes que caracterizan una realidad. De esa manera se establece la relación causa-efecto entre los elementos que componen el objeto de investigación” (Carlos, 2020). El trabajo de investigación efectúa un análisis de aspectos teóricos, normativos, históricos relacionados al tema en cuestión.

7.3. TÉCNICAS DE INVESTIGACIÓN

En cuanto al conjunto de instrumentos y medios a través de los cuales se efectuara este estudio, se plantea las siguientes técnicas de investigación que me permitirá ordenar las etapas de la misma, aportar instrumentos para manejar la información, llevar un control de los datos y orientar la obtención de conocimientos:

- **REVISIÓN BIBLIOGRÁFICA.** - Una revisión bibliográfica es, principalmente, una modalidad de trabajo académico para elaborar artículos científicos, trabajos de fin de grado, máster o tesis. El objetivo principal de esta modalidad es realizar una investigación documental, es decir, recopilar información ya existente sobre un tema o problema.
 - Documentos
 - Expedientes
 - Documentales
 - Reportajes

CAPITULO I

MARCO HISTÓRICO

1.1. LA INTERNET Y SU ORIGEN

1.1.1. ORIGEN DEL INTERNET

A finales de los años sesenta es concebida la primera red denominada “ARPANET” en la Agencia para el desarrollo de Proyectos Avanzados de Investigación (ARPA, Advanced Research Projects), que tenía la misión de conectar los ordenadores de diferentes instituciones militares con el fin de que las comunicaciones no se interrumpieran si alguna de ellas era destruida, sino que solamente se perdiera un nodo (Nodo, en informática y redes de área local, un dispositivo conectado a la red capaz de comunicarse con otros dispositivos de la misma), logrando que las comunicaciones estuvieran descentralizadas.

El año 1974 Vinton Cert (Ingeniero Estadounidense), junto con Robert Kahn, publican “Protocolo para Intercomunicación de Redes de paquetes “, donde especifican el diseño de un nuevo protocolo, el Protocolo de control de transmisión (TCP, Transmisión Control Protocol) que ya estaba fuera de ámbito estrictamente militar el cual se convirtió en el estándar aceptado. La implementación de TCP permitió a las diversas redes conectarse en una verdadera red de redes, es decir conectarse a internet.

En 1983 ARPANET se separa de la red militar que la origino, de modo que ya sin fines militares se puede considerar esta fecha como el nacimiento de Internet, su expansión es enorme mejorando los servicios; en 1985 se termina el desarrollo del aún vigente protocolo para la transmisión de ficheros en Internet (FTP, Transfer Protocol), basado en la filosofía de cliente-servidor.

En 1990 Tim Berners-Lee, investigador del Centro Europeo de Investigación Nuclear (CERN), crea una nueva manera de interactuar con el Internet: El Word Wide Web fue aumentando más a fondo por otros que crearon software y tecnologías para hacerlo más funcional. Por ejemplo, Marc Andreessen creo un nuevo navegador llamado

Mosaic en 1993, posteriormente dirigió el equipo que creó Netscape Navigator. Asimismo, Berners-Lee, creó las bases del protocolo de transmisión HTTP, el lenguaje de documentos HTML y el concepto de los URL.

En septiembre de 1993 se inició el primer servidor Web en español. En estos momentos se aumenta la potencia de las redes troncales de EE.UU., y en 1994 se eliminan las restricciones de uso comercial de la red y el gobierno de EE.UU. deja de controlar la información de Internet, constituyéndose en 1995 como el año del gran “boom” de Internet, puede considerarse como el nacimiento de Internet Comercial, contando con aproximadamente 3.8 millones de nodos registrados y más de 30 millones de usuarios.

La Internet es identificada por la mayor parte de usuarios como la gran autopista de la información. Así, la eficaz intermediación de Internet que posibilita reconducir los incontenibles flujos de información y contribuye a que la “sociedad de la información” pueda efectivamente transformarse en “sociedad del conocimiento”, como consecuencia de la posibilidad de extraer conocimientos útiles de la sobreabundancia de información.

Para Llaneza González, Internet es un sistema de comunicación transnacional que, gracias a unos estándares comunes, usando tecnologías y redes de telecomunicación, permite el intercambio y la obtención de información mediante el uso de diversas modalidades de comunicación en línea (listas de correos, USENET, chats, etc.) Internet es información, tecnología y una red física de telecomunicación.

1.2. INCURSIÓN DE LA INTERNET EN BOLIVIA

En Bolivia las telecomunicaciones han estado a cargo de cooperativas telefónicas con un monopolio local, los servicios nacionales e internacionales de larga distancia a cargo de ENTEL, ofreciendo los servicios de telefonía celular TELECEL (1991) que se convertiría más adelante en TIGO , ENTEL (1996), y a fines de 1999 VIVA NUEVATEL monopolios que concluyen con la aplicación de la Ley de Telecomunicaciones, ofreciendo hoy en día no solo de telefonía celular pues también

ofrecen internet inalámbrico utilizando los conocidos módems internet (es un acrónimo de modulador/demodulador. Se trata de un equipo, externo o interno, utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de voz y/o datos), dándose la apertura de mercados para un mejor servicio a precios competitivos.

El proceso de la incursión de Internet en Bolivia, se dio bajo el Programa Regional RLA/031/88 de la Oficina Regional para América Latina y el Criebe del Programa de Naciones Unidas para el Desarrollo, constituyéndose un Proyecto Experimental bajo el nombre de BolNet, pionero de Internet en Bolivia generando servicios inicialmente de transmisión de datos comenzando por el Correo Electrónico (1990-1992). En el año 1991, se dieron los primeros pasos en la Internet, primero con una infraestructura alquilada y posteriormente en 1993, con la instalación de los equipos definitivos en la Facultad de Ingeniería Electrónica de la UMSA, logrando la comunicación de 24 horas al día con 91 países. Se prestaba servicios a más de 1000 usuarios, incluyendo a instituciones académicas y científicas. La primera página web en Bolivia fue www.bolnet.bo. También dieron servicios como acceso a base de datos, listas electrónicas, gopher y otros (1992-1995), los que desaparecieron con el advenimiento de los servicios full Internet y el servicio web.

En 1991 se asignó el código de país Internet para Bolivia “bo”, pero fue recién en julio de 1995 que comenzaron a conectarse a Internet anfitriones con el nombre de dominio .bo. Dicha conexión fue posible gracias a un proyecto entre BolNet (Unidad Especial del Consejo Nacional de Ciencia y Tecnología (CONACYT), Red HUCYT (Red Hemisferica e Interuniversitaria sobre Ciencia y Tecnología) y el Programa de Desarrollo de las Naciones Unidas (PNUD).

ENTEL y BolNet, suscriben una alianza estratégica para la creación de Sistemas de Información y Servicios (1996-1999), es así que Bolnet cooperara en la creación, desarrollo y expansión de la ENTELNET conectando a las cuatro ciudades más importantes del país (La Paz, Santa Cruz, Cochabamba y Sucre) no solo en ingeniería de redes, sino en el desarrollo de sistemas de administración y gestión de redes.

Concluido el convenio entre ENTEL S.A. y BolNeet en diciembre de 1999, el Consejo Nacional de Ciencia y Tecnología, la Vicepresidencia de la Republica y el Ministerio de Educación, Cultura y Deportes, aprueban el nuevo Plan Estratégico de BolNet para construir un Backbone Nacional para el Área Científica y Educativa y cooperación gubernamental.

Hasta mayo de 2000, se habían registrado 16 proveedores VAS en SITTEL, de los cuales 12 eran proveedores de servicios relacionados a Internet, pero esta lista no era fija, debido a que no todos los operadores ISP del país se habían registrado, y solo 10 ISP estaban en pleno funcionamiento.

Antes de la apertura de telecomunicaciones el único ISP que presto servicio de Internet a 8 departamentos es ENTEL, el número de internautas a principios del año 2000 era de unos 90.000 hallándose el mayor número de usuarios de Internet en Santa Cruz, seguramente por el costo telefónico.

Cabe resaltar la palabra del entonces Vicepresidente de la Republica Ing. Jorge Quiroga R. “La incorporación y uso masivo de la Internet en la Republica permitirá otorgar mayor accesibilidad y rapidez a la información a un menor costo, aspirando a salvar las brechas de comunicación y tecnología que aun separan a grandes sectores de la sociedad boliviana, teniendo a facilitar sus demandas inmediatas de información”.

Hoy en día en el Estado Plurinacional que se dice ser netamente inclusivo, es decir, incluir en todo ámbito a los sectores que antes estaban olvidados y que ahora son la gran mayoría, está realizando importantes esfuerzos en procura de modernizar al aparato gubernamental para poder ofrecer servicios en línea al ciudadano, a través del uso de las TIC´s. (Tecnologías de Información y Comunicación).

La construcción de la Agenda Digital Boliviana, contribuirá para dotar al país de un horizonte y una estrategia estatal que permitan sentar las bases para dar un salto cualitativo de la sociedad hacia la Sociedad de la Información.

La actualización de la normativa en telecomunicaciones orientada a las TIC's, permitirá crear un escenario moderno que garantice el uso y acceso eficiente de los recursos digitales, proteja al ciudadano y promueva la modernización.

El Satélite Túpac Katari permitirá ofrecer conexión de Internet y servicios de telefonía de tipo satelital a poblaciones alejadas.

Con la vigencia de la reciente Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación del 08 de agosto de 2011 que entre otras cosas promueve el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos y además garantiza el desarrollo y la comunicación, es decir que el Estado mediante políticas estratégicas está orientado a asegurar una conexión eficiente.

1.3. Historia de las redes sociales en Bolivia

En Bolivia, el paso hacia el uso de las redes sociales ha estado ligado a las comunidades virtuales. Gómez, en Historia de Internet en Bolivia, enumera cuatro etapas sobre internet: una etapa técnico-académico (1989-1994), expansión y comercialización del servicio (1995-2001), el Estado toma el control: Bolivia hacia la sociedad de la información (2002-2005) y la masificación del servicio: internet como derecho (2006-2015) Estas etapas, con excepción de la última, se vinieron sin la presencia de las redes sociales.

Ya entrando en la historia d las redes sociales virtuales, podemos decir que comienza con el cuarto periodo que describe Gómez. A partir de ahí podemos identificar tres etapas en la historia de las redes sociales: una primera etapa técnico social (2008 a 2011), na segunda etapa de expansión y diversifican (2012 a 2015) y una etapa que comienza en 2016 y se mantiene hasta la actualidad. Describamos y caractericemos cada una de estas etapas o hitos de las redes sociales en el país.

Esta primera etapa está caracterizada por la llegada de las redes sociales como innovación tecnológica de la Web 2.0 y d la apropiación social de los usuarios que, en

un principio, vieron en los foros, chats, listas de correos electrónicos y blogs, canales ideales para relacionarse e interactuar en el espacio.

En una segunda etapa está muy relacionada con los esfuerzos para cerrar la brecha digital, el crecimiento de usuarios de internet y la apropiación progresiva de las redes sociales con su consecuente diversificación. Así, la apropiación de las redes sociales conduce a una maduración del activismo digital y junto a la diversificación de actores, se consolidan en espacios los periodistas y medios de comunicación de igual modo que la clase política, las autoridades de gobierno y sus administraciones. Por último, el crecimiento de los usuarios se convierte en una necesidad para los servicios de empresas, que se ven conminados a ofertar productos y servicios mediante estas plataformas. Esta nueva configuración produce cambios de comportamiento en la sociedad red, que deja rezagada a la vida en comunidad.

1.4. EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS

Nuestro país de una economía basada principalmente en la industria petrolera, minera y agrícola, con una área industrial muy reducida en comparación con otros países, concentra un significativo sector de la población dedicado a la administración del estado; que necesariamente debe estar capacitado en el manejo de ordenadores o computadoras, ya que la informática se constituye en una herramienta imprescindible en la actualidad para el correcto y eficaz funcionamiento tanto de las instituciones estatales como de las instituciones privadas Actualmente la informática es una herramienta imprescindible para el correcto y eficaz funcionamiento de las instituciones públicas como privadas.

“Los avances de las tecnologías de la información, comunicaciones y el crecimiento de las operaciones comerciales mediante un medio electrónico han propiciado el surgimiento de nuevas conductas fraudulentas relacionadas con el uso de instrumentos electrónicos.”

Sin embargo, el uso de la informática en nuestro país no es privativo, debido a la baja de ordenadores y de procesadores coloca a grupos importantes de nuestra población a estar en contacto con la tecnología generando diferentes actividades, así

como redes sociales, correo electrónico e incluso juegos electrónicos. Las medidas del estado como la entrega gratuita de ordenadores a bachilleres de nuestro país, la instalación de 2000 antenas Wi Fi, en el área rural para internet, así como telefonía 19 móvil sumándose también la compra del satélite TÚPAC KATARI, así como el crecimiento de nuestras empresas de telefonía las cuales están en constante actualización de tecnología, por estos motivos es necesario la necesidad de contar con una ley específica acerca de delitos informáticos la cual este acorde con el desarrollo de la tecnología.

En nuestro país los delitos informáticos no solo están ligados con las instituciones, sino que están ligados también con el desarrollo de la población y en si de la sociedad ya que, al desarrollo de las tecnologías, nuestra sociedad se encuentra vulnerable ante nuevas formas de delitos cometidos mediante ordenadores, cajeros automáticos tarjetas de crédito etc.

“Los primeros estudios empíricos sobre el delito informático fueron realizados a mediados de la década de 1970, si bien estos estudios sacaron a la luz un limitado número de delitos, simultáneamente indicaron fuertemente que un gran número de estos delitos permanecían sin descubrirse o sin denunciarse. La perspectiva publica y científica acerca de los delitos informáticos cambio radicalmente en los ochenta, una amplia ola de piratería de programas, manipulación de cajeros automáticos y abusos de las telecomunicaciones revelo la vulnerabilidad de la sociedad de la información y la necesidad de nuevas estrategias de control de estos delitos.” (Saenz, 2014, p.57)

Creemos que, en la actualidad, es innegable la existencia de delitos cometidos mediante el uso de instrumentos informáticos ...“más aún, mediante el análisis de las normativas existentes en el derecho 20 comparado,”(9) de donde surge la necesidad de estructurar un nuevo bien jurídico digno de tutela jurídica penal, que entendemos y sostenemos que se trata de la información en todas sus etapas, la cual conlleva en sí un valor, ya sea económico, ideal o de empresa como veremos más adelante, que es relevante y digno de tutela jurídica penal.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que los usos de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. Este tipo de delitos son considerados un aspecto negativo del desarrollo de la informática y se producen debido a las posibilidades que las computadoras ofrecen para infringir la ley.

“En este contexto, aparecen conductas que vulneran bienes jurídicos no convencionales, o comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales.” La regulación jurídica de la criminalidad por o contra el ordenador presenta determinadas peculiaridades debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan. Son evidentes e indiscutibles los beneficios de la informática en la comunidad. Empero, los aspectos negativos comprenden inimaginables formas de cometer delitos. En el plano jurídico - penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías.

Así, como las nuevas tecnologías nos traen destacables ventajas, es importante responder eficientemente a la necesidad de regular las conductas que pueden derivarse del uso indebido de las tecnologías siendo de esta forma el uso indebido de ordenadores, de tarjetas de crédito y débito.

A los efectos de lograr un mayor abundamiento en la investigación a desarrollar, como también una clara y ordenada explicación de la misma, tomaremos distintos parámetros para elaborar un esquema acerca de la evolución de los delitos informáticos:

“En los años 1970 y siguientes fueron los europeos los primeros países en tomar conciencia de los avances de la informática, los cuales generarían mayores peligros,

con relación al bien jurídicamente protegido, en los años setenta se referían al ámbito de la intimidad.” (Saez, 2014,p .178)

Entre 1970 y 1980, se comenzó a regular el tratamiento de datos personales mediante ordenadores, tanto en Suecia, Alemania, así como también en EEUU. Comienza así, la inclusión de diversas normas penales en los ordenamientos europeos a los efectos de proteger la privacidad y la confidencialidad, sin embargo, en los años ochenta a delitos se desarrollaron delitos informáticos de contenido económico y se resguardaba la propiedad intelectual de los programas.

A partir de 1980 comienza un proceso legislativo originado en Estados Unidos luego se extendió a Europa como reacción de la legislación tradicional que solo protegía los bienes materiales. Se legisla sobre protección de bienes intangibles dinero electrónico, soportes informáticos, etc.

En los años 1980 y 1990 por su importancia económica, se incluye a los programas informáticos, como obras protegidas por el Derecho de Autor. Los separa en otra sección, distinguiéndolos en protección para semiconductores, y para las bases de datos y los secretos comerciales.

A partir de 1986 en diversos países se van desarrollando Reformas en el Derecho Penal para combatir esta nueva forma de delitos generando seguridad y derecho

En los años noventa al desarrollo de nuevos paradigmas reguladores del derecho a la información.

HISTORIA DE LA LEGISLACIÓN PENAL CONTRA DELITOS INFORMÁTICOS EN BOLIVIA

En Bolivia, el año 1997, se incluye dentro las reformas del Código Penal, en su Libro Segundo Título XII, capítulo XI, los artículos 363 bis y 363 ter, tipificaciones penales, que buscan regular la manipulación informática y la alteración acceso y uso indebido de datos informáticos.

Podemos mencionar también que, como parte de este esfuerzo regulador, el Poder Legislativo sancionara en 1992 la ley No. 1322 de derechos de autor y el Poder Ejecutivo dicta el Decreto Supremo No. 24582, del 25 de abril de 1997, denominado Reglamento de Soporte Lógico o Software, que velan por la protección de los derechos Autorales en software y conforman una importante base para la formación de nuevas legislaciones en materia de derecho informático.

Las legislaciones penales bolivianas, de la década de los años 90 del siglo pasado, son una muestra de la necesidad de la regulación específica de las acciones, derivadas del uso de la informática, en las relaciones comerciales.

Dentro del ordenamiento jurídico vigente, aún falta mucho que implementar legislativamente, para participar con el mundo y la región latinoamericana, en las operaciones que se desenvuelven en materia informática.

CAPITULO II

MARCO TEÓRICO Y CONCEPTUAL

1.1. INTERNET

Hoy por hoy se vive en un mundo globalizado donde las tecnologías son la fuente de información para la sociedad sobre todo la internet que aporta gran cantidad de datos académicos, culturales, estadísticas, notas, etc. Para lo cual se define a internet como:

Un conjunto de redes de computadoras interconectadas que abarcan el mundo entero mediante cables de fibra óptica, torres de radio comunicación y satélites. También incluye una inmensa cantidad de información y programas dentro de computadoras conectadas entre sí. Cualquier conexión a internet en el mundo puede acceder a grandes cantidades de información (Eck, 2002).

La internet aporta elementos como la sincronía, el anonimato, la capacidad de socializar y de generar un sentimiento de grupo en el usuario, la construcción de identidades, inmediatez, la accesibilidad y la comunicación mediante la escritura, factores que determinan su preferencia, pues resultan menos estresantes que una conversación cara a cara (Sánchez-Carbonell, Beranuy, Castellana, Chamarro, & Oberst, 2008).

La internet es la red de redes o telaraña universal compuesta por un conjunto de computadoras que están interconectadas entre sí, dicha red ofrece diversas herramientas que permiten la comunicación entre las personas que la utilizan, así como también se tiene acceso a música, videos, juegos, e información, e incluso se pueden realizar actividades como pagos de cuenta, transacciones, compras, etc. La internet no solo ofrece beneficios a la sociedad, algunas de las desventajas de la internet es que, se generan algunos riesgos de la cual los usuarios no tienen en cuenta, (Jiménez Rojas) Menciona que:

La Internet es una de las herramientas tecnológicas más utilizadas hoy en día, es la mayor fuente de consulta de información y una de las mayores plataformas

comerciales, lo que ha causado que gran número de actividades antijurídicas se realicen a través de este medio.

CARACTERÍSTICAS DEL INTERNET

INTERACTIVA: El Internet se encuentran en muchos sitios para compartir opiniones, gustos e información, tales como foros, salas de chat, blogs, etc.

INTEGRAL: Gracias a su cobertura mundial, el Internet puede ser utilizado con diferentes fines, como por ejemplo los negocios, ya que permite el contacto entre compañías y personas, facilitando así las relaciones empresariales y de negocios.

INFORMATIVA: Lo más importantes son los diarios y canales de noticias a nivel mundial que cuentan con una página web, a través de la cual los usuarios pueden mantenerse en contacto con las novedades que ocurren en los diferentes lugares gracias a eso la información es conocida de manera casi inmediata y simultánea en cualquier lugar con acceso al Internet.

INTERNET COMO MEDIO DE COMUNICACIÓN

Las posibilidades que brinda el Internet como fuente de acceso a información en múltiples formatos son casi ilimitadas. De ahí que, en las últimas décadas, los medios de comunicación tradicionales se hayan visto impulsados a ofrecer plataformas y soluciones adaptadas a nuevos tiempos y consumidores de información.

En un principio (inicio de los años 90), muchos medios de comunicación usaban la Internet como un apoyo, una herramienta secundaria sobre la que se vaciaba el contenido a través de la web. Poco a poco, los medios comenzaron a ajustar los formatos de sus contenidos para que fuesen más compatibles, en forma y fondo, con las características de Internet y de la web.

Las características propias el Internet permiten la presentación de información en multitud de formatos como, por ejemplo, sonido, video, imágenes y texto. Permite combinar elementos de otros medios de comunicación, como la radio, el periodismo y la televisión. De allí que en las últimas décadas muchos medios no solo hayan logrado

adaptarse al avance tecnológico que el internet supone, sino que además han surgido nuevos medios y plataformas inéditas para la creación y transmisión de información y contenido.

El surgimiento de plataformas como Blogger o Wordpress, que permiten la creación de blogs, la irrupción de plataformas digitales de redes sociales como Facebook, Twitter o Instagram, la evolución de la mensajería instantánea, los servicios de streaming (transmisión de contenido multimedia como películas, series o videos), sino que además han hecho que los usuarios pasaran de ser receptores pasivos a creadores-consumidores de contenidos.

En este nuevo ecosistema comunicacional, los medios tradicionales y los nuevos medios han tenido que considerar a los usuarios como parte activa de este nuevo entramado. Internet cambio las dinámicas de poder entre emisores y receptores y esto se ve reflejado en la cantidad y variedad de contenidos a los que es posible tener acceso hoy en día, así como en la creación y actualización de tecnologías de la información que permitan el acceso de los usuarios a los contenidos digitales.

1.2. IMPORTANCIA DE LA INTERNET EN LA EDUCACIÓN

Una de las herramientas de mayor capacidad de información a distancia que ha traído consigo la tecnología mundial es el Internet, se ha convertido en un medio idóneo para impartir una enseñanza de calidad. A través del uso del internet se posibilita, por primera vez en la historia de la educación que la mente quede liberada de tener que retener una cantidad enorme de información. Solo es necesario comprender los conceptos sobre dinámica de los procesos en las cuales una información está encuadrada, ello permite utilizar métodos pedagógicos con los cuales el alumno puede aprender más.

Actualmente la sociedad está más inmersa en el ámbito tecnológico que nunca, la cultura ha provocado el desarrollo e implementación más adentrada a las tecnologías de la información y comunicación en la educación. Las nuevas generaciones adoptan la tecnología de manera natural y se sienten altamente familiarizados con ella en el

ámbito educativo, así como también se sienten más atraídos en la forma que esta actúa como recurso educativo.

La escuela debe acercar a los estudiantes a la cultura de hoy, no a la cultura al ayer (Marquez 2003). La incorporación de las tecnologías en el ámbito escolar posibilita potencializar las estrategias para el proceso de enseñanza y aprendizaje así también como un medio donde pueden practicar lo aprendido, maximiza el interés del alumno en la clase porque se le hace llamativa pues se utilizan las tecnologías que ocupan en su vida diaria y se sienten a gusto con ella. El Internet como parte esencial de las TIC's funge como herramienta indiscutiblemente útil en el ámbito educativo, permite a los involucrados en el, la obtención de datos, comunicación, acceso a paginas educativas del Internet en el sector educativo todo el personal implicado en el, alumno, profesores, padres, etc. sepan manipularlos correctamente para así tener un proceso de enseñanza y aprendizaje exitoso.

1.3. DEFINICIÓN REDES SOCIALES

Las redes sociales son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos, e ideas de libre expresión. (Hernández, 2013, p. 32).

Las redes sociales son un sistema social con estructura propia y particular de cada individuo. Fueron creadas con la finalidad de que se pudieran establecer relaciones mediáticas a nivel internacional a través de Internet para enriquecer el conocimiento. Cuando una persona decide pertenecer a una red social debe estar preparado para establecer un contacto con una serie de personas que no siempre conoce. Las redes sociales se convierten pues en un espacio donde interactuar con los demás y con quién compartir gustos, música, imágenes, videos e incluso establecer nuevas relaciones de amistad. En estos últimos años, las redes sociales se han convertido en un elemento esencial para los jóvenes, por lo que va teniendo una importante repercusión en la formación de la identidad del individuo. En los

adolescentes esto tiene relación con la búsqueda de la identidad. (Hernández, 2013, p. 32).

De acuerdo a Ramos (2008, p.52), las Redes Sociales son formas de interacción social que consisten en un intercambio dinámico entre personas, grupos e instituciones. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas, y que se organizan para potenciar sus recursos. García (2010) coincide con Ramos y de acuerdo a él, la red social es aquel lugar de la web en el que se pueden compartir mensajes, fotos y vídeos con el grupo de “amigos” y localizar “nuevas amistades”; se crea de forma espontánea entre personas que se invitan para formar parte de ella.

Celaya (2015). Las redes sociales permiten que las personas publiquen y compartan cualquier tipo de información, entre conocidos y desconocidos. Este fue un espacio creado para facilitar la interacción entre personas.

En las redes sociales de Internet tenemos la posibilidad de interactuar con otras personas, aunque no las conozcamos, cada nuevo miembro que ingresa transforma al grupo en otro nuevo. Algunas redes se crean por amistad, otras por trabajo, por un conocimiento específico o un hobby. En ocasiones, dentro de una misma red social se crean diferentes grupos de miembros unidos por una misma característica. (Tamez, 2012, p.28).

“Una red social en el ámbito de internet, son páginas que permiten a las personas conectarse con sus amigos con el fin de compartir contenidos interactuar crear comunidades, o intereses similares el trabajo, la lectura juegos y amistad, relaciones interpersonales es decir un sistema social con estructura propia, dentro del cual existe”. De acuerdo a lo anterior las redes sociales no son más que páginas de internet que permiten a las personas mantenerse en contacto con familiares y amigo además de compartir una gran gama de contenidos que es lo que hace que las redes sociales sean más visitadas por todos sus usuarios. (Mardochowicz. p. 13)

Las redes sociales han revolucionado la manera de comunicarse, sin embargo, los mejores receptores de este cambio han sido los jóvenes para expresarse, por lo

que los jóvenes han experimentado cambios en sus hábitos, ya no es la televisión sino la computadora o el celular, Tablet.

1.4. CARACTERÍSTICAS DE LAS REDES SOCIALES

- Área de participación ciudadana. Medio de comunicación cada vez más utilizado en detrimento del correo electrónico.
- Comunicada o punto de encuentro en el que los usuarios construyen, comparten y desarrollan conocimientos.
- Suscripciones a eventos, noticias y boletines.
- Zona personal, para acceder a servicios personalizados.
- Existencia de Alertas.
- Fácil acceso a las mismas a través del ordenador, móviles, PDA, TDT, etc.
- Tiene un papel facilitador para el logro de resultados.

2. TIPOS DE REDES SOCIALES

En este apartado se explicará los tres tipos de redes sociales como son; redes de tipo generalista, específicas y horizontales. "Cada red social tiene sus propias características o finalidades. La primera distinción que se da entre las redes sociales "generalistas" y las que tienen contenidos o características específicas". (Gonzales, 2016, p.34)

2.1. Las redes de tipo generalista

Están abiertas a la población general, que busca relacionarse, intercambiar información y mantenerse en contacto con otras personas.

Es por ello que las redes sociales generalistas abarcan gran cantidad de usuarios por estar abiertas al público en general, por lo que este tipo de redes sociales son las que más usuarios tiene y sigue aumentando son las que mayor número de

miembros reúnen, en estas redes, de tipo general, los usuarios pueden usar los instrumentos de comunicación que se les ofrece en función de los fines que cada uno tenga. (Gonzales, 2016, p.34)

2.2. Redes específicas

Están definidas” en función de unos objetivos que de alguna forma condicionan y limitan las relaciones entre los usuarios, pueden ser de profesionales relacionadas con algún aspecto de la cultura o la política, o estar dirigidas a determinadas personas en razón de su situación o circunstancias: jóvenes, padres, salud”. Para estas redes el tipo de usuarios que albergan son muy selectivos ya que son personas que comparten intereses particulares, en este tipo de usuarios pueden ser solo profesionales de determinada especialidad o personas que comparten los mismos intereses de ese tipo de usuario. (Gonzales, 2016, p.34)

2.3. Redes Horizontales

“Las redes sociales horizontales equivaldrían a las generalistas y no estarían enfocadas a un grupo de personas o cuestión concreta, sino que en ellas cabría cualquier cosa: trabajo, ocio, amigos, familia, deportes y literatura. De todo puede hablarse y las relaciones pueden ser heterogéneas ejemplos de estas redes: Facebook, hi5, MySpace y WhatsApp.” (Gonzales, 2016, p.35)

2.4. CLASIFICACIÓN DE LAS REDES SOCIALES

Las redes sociales están clasificadas de la siguiente manera:

Instagram: Es una red social y aplicación para compartir fotos y videos. Permite a los usuarios aplicar efectos fotográficos como filtros, marcos, similitudes térmicas, áreas subyacentes en las bases cóncavas, colores retro y vintage, y posteriormente compartir las fotografías en diferentes redes sociales como Facebook, y Twitter (Gonzales, 2016, p.36).

Una característica distintiva de la aplicación es que da una forma cuadrada a las fotografías en honor a la Kodak Instamatic y las cámaras Polaroid, contrastando con la

relación de aspecto que actualmente usan la mayoría de las cámaras de teléfonos móviles. Instagram fue creada por Kevin Systrom y Mike Krieger y fue lanzada en octubre de 2010. La aplicación rápidamente ganó popularidad, con más de 100 millones de usuarios activos en abril de 2012 y superó los 300 millones en diciembre de 2014. (Gonzales, 2016, p.36)

Facebook: El término Facebook pertenece al inglés. Compuesta literalmente por fase cuyo significado es cara y book que significa libro. Es por ello Facebook opera mundialmente como una red social en la cual las personas, luego de crearse un perfil y completar los datos que deseen, pueden realizar diferentes actividades entre las cuales las más populares son buscar y encontrar numerosos contactos de la vida real (muchos de los cuales pertenecen a momentos pasados de la vida de cada uno), expresar sus opiniones y estados de ánimo, subir y comentar fotos, jugar, crear redes y grupos con diferentes objetivos, etc. (Gonzales, 2016, p.36)

Según Matus (2011) Facebook es la red social más grande ha cambiado el mundo desde que nació hasta hoy. Inicialmente, Facebook fue creado como un sitio donde los estudiantes creaban grupos con el fin de compartir resúmenes, noticias, recordatorios de exámenes, trabajos prácticos, etc., hasta que poco a poco, los estudiantes comenzaron a explotar otra faceta hasta el momento no utilizada, dándole un perfil más social, subiendo fotos y datos que comenzaron a darle un perfil más social al sitio web. Facebook está definido como un sitio Web de redes sociales creado por Mark Zuckerberg, originalmente fue un sitio para estudiantes de la Universidad de Harvard, pero en la actualidad está abierto a cualquier persona que tenga una cuenta de correo electrónico. Los usuarios pueden participar en una o más redes sociales en relación con situación académica, su lugar de trabajo o región geográfica (Faerman, 2010).

WhatsApp: Es una aplicación de chat para teléfonos móviles de última generación, los llamados Smartphone. Permite el envío de mensajes de texto a través de sus usuarios. Su funcionamiento es idéntico al de los programas de mensajería instantánea para ordenador más comunes. La identificación de cada usuario es su número de teléfono móvil. Basta con saber el número de alguien para tenerlo en la lista

de contactos. Es imprescindible que, tanto el emisor como el destinatario, tengan instalada esta aplicación en su teléfono. Para poder usar WhatsApp hay que contratar un servicio de internet móvil. (Gonzales, 2016, p.36)

Innovó al digitalizar y, en consecuencia, abaratar el hábito de envíos de mensajes de texto que se lleva a lo implícito los que alguna vez utilizan teléfonos analógicos. Entonces, al ser de uso común, su apropiación fue progresiva y natural. Esta red social también popularizó los emojis o pictogramas, estas pequeñas imágenes digitales o íconos que son ampliamente usados para expresar una idea o emoción en los textos electrónicos. Lo interesante de esta red social es que propaga fácilmente los mensajes a través de la circulación cerrada y limitada. No se puede seguir lo que se publica en un grupo de WhatsApp si es que no está en él. (Morales, 2020, p.19)

Facebook Messenger: Es una aplicación con la que puedes intercambiar mensajes en tiempo real desde tu móvil con tus amigos de esta red social y con los contactos de tu agenda telefónica, aunque no estén dados de alta en Facebook. (Gonzales, 2016, p.36)

Es sin duda la red social con mayor volumen de usuarios, esta fue concebida desde un inicio para establecer relaciones y compartir estados. Con los años, ha logrado desplazar a otras plataformas similares como MySpace o Hi5, principalmente por su sencillez. Facebook resulta más interesante, pero no es fundamentalmente distinto desde el punto de vista del usuario. Por tanto, lo que importa son las herramientas, la flexibilidad y la capacidad de crear y de animar una red. Prima la sencillez. (Pisani y Plotet, 2009, p. 37).

Esta manera intuitiva de publicar estados ha hecho que las personas adopten una narrativa visual y participativa, con gran capacidad de expandir los mensajes. Por lo tanto, lo que se logra con Facebook, básicamente, es la masificación de los mensajes. (Morales, 2020, p.18)

YouTube: Es un sitio web para compartir vídeos subidos por los usuarios a través de Internet, por tanto, es un servicio de alojamiento de videos. El término proviene del inglés "you", que significa tú y "tube", que significa tubo, canal, pero se

utiliza en argot como "televisión". Por lo tanto, el significado del término YouTube podría ser "tú transmites" o "canal hecho por ti". (Gonzales, 2016, p.36)

Nació como un servicio de alojamiento y publicación de videos online. Con el tiempo, fue integrando una versión móvil, la transmisión en vivo y la mensajería instantánea. Según esta red social a diario sus usuarios consumen el equivalente a un billón de horas viendo videos. Asimismo, los pronósticos de consumo son muy prometedores, tanto que para el 2021 el video online representará el 82 por ciento de tráfico global de Internet. A esta popularidad contribuyeron la expansión y cobertura de las conexiones a internet, así como el acceso a los dispositivos móviles. Algo que incentiva la participación de los usuarios es la posibilidad de obtener ganancias por los videos. Cualquier usuario puede acceder a la monetización de sus videos de modo que estos muestren anuncios publicitarios cuya comisión llega al productor, que puede ser un medio o una persona. Estos elementos dieron paso a la aparición de los youtubers, personas que producen videos temáticos, a veces caseros, y que generan en torno a ellos una comunidad y una influencia, por lo que son requeridos no sólo por YouTube, sino por empresas para que promocionen sus productos. (Morales, 2020,18)

Twitter: Es una red social como Facebook u otra red, la diferencia de las demás es la limitación para dejar mensajes y leer texto ya que su longitud máxima es de 140 caracteres denominados como tweets. De modo que los tweets también se pueden realizar por medio de teléfonos celulares twitter se basa en el principio de los seguidores cuando se elige seguir a otro usuario. (Gonzales, 2016, p.37)

3. VENTAJAS Y DESVENTAJAS DE LAS REDES SOCIALES

Según las ventajas y desventajas del uso de las redes sociales, enumeraremos los siguientes puntos, que proponen lo bueno y lo malo que trae abrir un perfil personal. (Gonzales, 2016, p.37)

3.1. Ventajas de las redes sociales

- Reencuentro con conocidos

- Oportunidad de integrarse
- Excelentes para propiciar contactos efectivos nuevos como búsqueda de pareja, amistad o compartir intereses sin fines de lucro.
- Compartir momentos especiales con las personas cercanas a nuestras vidas
- Diluyen fronteras geográficas y sirven para conectar gente sin importar la distancia.
- Tener información actualizada acerca de temas de interés, además permiten acudir a eventos participar en actos y conferencias.

Una de las grandes ventajas de las redes sociales es la vinculación entre los usuarios, al conocer gente nueva e interactuar entre ellos, permitiendo ello el aislamiento de muchas personas, la formación de comunidades, con anonimato y sin discriminación formando espacios de igualdad a través de la red. (Hernández, 2013, p.35).

Las ventajas que las redes sociales nos ofrecen son muy importantes y variadas ya que nos ofrecen un sinnúmero de aplicaciones que hacen que sea más fácil nuestro entorno, independientemente de lo que se quiera realizar en ellas ya sea comunicarse o compartir momentos especiales con familias y amigos o conseguir información referente a algún tema en específico, el poder usar las redes sociales hacen que todo esto se vuelva tan fácil que hace que los usuarios quieran pasar más tiempo conectados. (Gonzales, 2016, p.43)

También permite hacer el intercambio de ideas, formar lazos con personas que comparten los mismos intereses, la creación de movimientos masivos de solidaridad o ideología y la creación de campañas publicitarias de gran éxito.

3.2. Desventajas de las redes sociales

- Son peligrosas sino se configura la privacidad correctamente, pues exponen nuestra vida privada.

- Pueden darse casos de suplantación de personalidad
- Falta en el control de datos
- Pueden ser adictas y devorar gran cantidad de tiempo pues son ideales para el ocio.
- Pueden ser utilizadas por criminales para conocer datos de sus víctimas en delitos: como el acoso y abuso sexual, secuestro, tráfico de personas etc.

Las desventajas que están puedan tener es que las personas al inscribirse a una red social escriban sus datos personales con absoluta fidelidad, han sido muy desastrosas, ya que abunda los casos en que otras personas que tiene acceso a dicha información y que no son amigos, han utilizado esa información para compartirla con personas inescrupulosas que la utilizan para cometer actos delictivos como secuestros, extorsiones, violaciones y otros. Muchas personas que desean renunciar a las redes sociales por los motivos anteriormente mencionados, aunque desean borrar su información personal, ésta queda guardada aún, además de que también son propensas a que los usuarios se puedan volver adictos a las mismas. (Gonzales, 2016, p.44)

La invasión de la privacidad es un gran problema que se presenta en las redes sociales, compañías especialistas en seguridad afirman que para los hackers es muy sencillo obtener información confidencial de sus usuarios. Son peligrosas si no se configura la privacidad correctamente, pues exponen nuestra vida privada. (Hernández, 2013, p.36).

4. RIESGOS ASOCIADOS AL USO DE LAS REDES SOCIALES

Las redes sociales son una evolución de las aplicaciones de internet, y producto de su uso generalizado. Por ello todos los problemas y peligros del uso inadecuado o excesivo de internet pueden aplicarse a las redes sociales que funcionan a través de la red. Sin embargo, es necesario diferenciar entre los peligros y retos genéricos que plantea internet, y que las redes sociales comparten en una medida similar a otras

aplicaciones, y los problemas específicos asociados a las redes sociales. Estos últimos, aun estado también presentes en cualquier uso de internet, se encuentran muy agudizados en las redes sociales por tres motivos. (Ríos, 2017, p. 37)

Puesto que la finalidad específica de las redes sociales es la comunicación e intercambio entre particulares, en ellas se acumula una inmensa cantidad de información y datos privados, e incluso íntimos, de millones de ciudadanos.

Los usuarios de red son en una gran mayoría, jóvenes que no han recibido ningún tipo de formación previa sobre el uso adecuado de las redes sociales, ni advertencia sobre sus peligros. 3. A los padres y educadores de la juventud actual, les ha tocado vivir, respecto a las redes sociales al igual que sobre las nuevas tecnologías en general una situación nueva desde el punto de vista educativo. (Ríos, 2017, p. 37)

“Los usuarios tienen la oportunidad de experimentar un mundo de relaciones virtuales, que no existían anteriormente, pero también que enfrentarse a retos y peligros desconocidos. Ante los problemas que se están planteando, y a los que a continuación haremos referencia, se están preparando y poniendo en marcha medidas legislativas y de otro tipo que probablemente en un futuro pondrán límites y normas que regulen mejor el funcionamiento de las redes sociales”. (Hernández, 2013.p,37)

Por todo ello la importancia de los retos y problemas que plantean estas redes, especialmente en el caso de la privacidad, protección de datos y seguridad, es tal magnitud que actualmente están centrando la preocupación de los investigadores sociales, legisladores, educadores, medios de comunicación, los internautas y la sociedad en general.

5. INFLUENCIA DE LAS REDES SOCIALES

Según Echeburúa y de Corral (2010) la red social puede atrapar a los jóvenes gracias a que el mundo virtual contribuye a crear una falsa identidad y a distanciarse o distorsionar el mundo real. El mismo autor define algunas señales de alarma o características de los adolescentes expuestos a la adicción de las redes, dentro de las cuales destacan la privación del sueño y descuidar otras actividades importantes como

el contacto con la familia y los estudios. En cuanto a los síntomas que presenta el afectado podrían ser:

- ❖ Su mentalidad es filtrar todo a través de la red social, como poder compartir, promocionar, marketear, o propagar información personal, laboral, o social.
- ❖ Actualizar tu estado, perfil, fotos, etcétera, con frecuencia y etiquetas a tus amigos para recibir comentarios.
- ❖ Las horas de descanso se han reducido en dos horas o más.
- ❖ Pasan las horas antes que te des cuenta de que no has hecho nada, excepto navegar en Facebook, Twitter, entre otras más.
- ❖ Los llamados "adictos" (en la gran mayoría menores de 25 años) en un 18% de estos solo pueden estar desconectados apenas un par de horas.

Por su parte Odriozola (2012) en su artículo acerca de los factores de riesgo en la adicción a las nuevas tecnologías y redes sociales en los jóvenes concluye que el abuso de las redes sociales y del internet puede ser una manifestación secundaria de otra adicción principal (como el sexo) u otros problemas psicopatológicos como depresión, fobia social, y otros problemas de tipo impulsivo compulsivo. Es decir que las nuevas tecnologías pueden hacer más llevadera la vida o crear dificultades a las personas especialmente a los adolescentes, a los cuales las redes sociales pueden atraparlos alejándolos del mundo real y creando una falsa identidad, interfiriendo negativamente en su vida cotidiana. (citado en Añari & Valencia, 2017, p.32)

Si hablamos sobre esto, de entrada, se nos viene a la mente la famosa y conocida red social Facebook, esta página es un sitio web de red social, que está abierto a cualquier persona que tenga una cuenta de correo electrónico. Las personas pueden hacer uso de una o más redes sociales a la vez, como el Messenger Facebook y el WhatsApp en relación con su situación académica o puesto de trabajo, ya que solo es necesario tener conocimientos básicos de informática.

Uno de los enormes éxitos por lo cual Facebook ha tenido tanta popularidad a nivel mundial se debe a lo siguiente (Mejía, 2015, p. 38):

- ❖ La facilidad con la que se puede compartir el contenido, sean estos fotos, links o videos. La posibilidad de subir casi sin límites las fotos.

Estos entre otros factores son los que hacen que Facebook sea una de las redes preferida por los adolescentes. (Añari & Valencia, 2017, p.32)

Mientras que Twitter que es otra de las redes más utilizadas entre los adolescentes es una red creada para publicar, compartir e intercambiar información mediante breves comentarios en formato de texto, con un máximo de 140 caracteres. Twitter se ha convertido en la plataforma de comunicación en tiempo real más importante que existe en la actualidad. (Añari & Valencia, 2017, p.32)

Para muchas de las personas, las redes sociales pueden convertirse en una especie de adicción, a punto tal que afectan las actividades que solían realizar, las relaciones con sus amigos y familiares se ponen de mal humor cuando no están conectados e incluso agresivos, entre otras cosas.

Conceptualmente la adicción a internet es un trastorno del espectro compulsivo impulsivo que implica el uso de computadoras en línea y/o fuera de línea y se compone de al menos tres subtipos: juego excesivo, preocupaciones sexuales, y la mensajería email/texto (Bostwick y Bucci 2008). Por su parte (Greenfield, 1999, citado en Añari & Valencia, 2017, p.32) encuentra varios sentimientos que experimentan los usuarios dependientes de Internet y que pueden llevar a la adicción: los adictos informan de una intensa intimidad cuando está conectados, existe un sentimiento de desinhibición, muchos adictos informan también de una pérdida de ataduras, sentimientos de que el tiempo se detiene o que pasa muy rápido y sentirse fuera de control cuando se está conectado.

6. REDES SOCIALES COMO HERRAMIENTA DE APRENDIZAJE

Actualmente las Redes Sociales se presentan como herramienta para intercambiar información, ideologías y hasta creencias de cualquier índole, es así como la vemos inmersa en todos los ámbitos en el campo educativo, pero si bien es cierto existen otros canales para mantener al público al día con la información, esta ha resultado ser el más efectivo.

De manera más específica, las redes sociales, entendidas como servicios web que permiten a los individuos construir un perfil público o semipúblico dentro de un sistema delimitado, articular una lista de contactos y ver y cruzar su lista de conexiones y las hechas por otros dentro del sistema (Boyd y Ellison, 2007), son un medio muy útil para “compartir todo tipo de datos e información y en múltiples formatos: audio, texto y video, y con muchas menos limitaciones que el correo electrónico, cuya capacidad es mucho más limitada” (Abuin, 2009). Estas nuevas herramientas brindan una amplia capacidad de comunicación que facilita el flujo de información de toda clase, ya que, si bien en un principio se utilizaban para publicar, esencialmente, reflexiones o vivencias de los usuarios, hoy en día casi todos los informativos y grandes medios de comunicación cuentan con perfiles en estas redes sociales (Carità et al 2011). Actualmente la web 2.0 y las diferentes herramientas que proporcionan, están ganando cada día más protagonismo en nuestra sociedad. Como parte misma, la trascendencia de estas aplicaciones en la docencia es cada vez mayor. Por ello son muchos los trabajos que se pueden encontrar en los que se propone la incorporación de las Web 2.0 en actividades docentes, con el objeto de favorecer y fortalecer nuevos modelos de enseñanza y aprendizaje.

El uso de las redes sociales, se ha extendido en todos los países; tienen un fin socializador muy potente y se han convertido en la herramienta prioritaria para mantener el contacto con las personas ya conocidas o ampliar el círculo social. Así, de una forma u otra los estudiantes pasan la mayor parte de su tiempo conectados a la Internet.

7. IMPACTO DE LAS TIC EN LA EDUCACIÓN

Los avances y retrocesos se combinan en un entretreído heterogéneo e impredecible, no obstante, el desarrollo de la tecnología es inevitable, irreversible y claramente influyente. De hecho, el conocimiento de la irregularidad de situaciones entre países es accesible mediante la tecnología que, al instante nos pone en contacto con diferentes regiones, situaciones y con buenas y malas noticias.

La sociedad actual salvo una debacle nuclear masiva que nos transporte a la edad de piedra, no será la misma que hace apenas 10 años atrás, el conocimiento circula con gran velocidad, las demandas para el ejercicio profesional se retocan ágilmente los problemas se difunden y extienden, por tanto, la educación en general se ha situado en el centro del debate por cuanto es responsable de la información de recursos humanos que deben poder existir con calidad de vida allí donde corresponda. En consecuencia, los educadores tienen al menos dos claros desafíos que modifican notablemente sus hábitos profesionales:

Investigar para estar al tanto de los cambios y avances en la tecnología y el desarrollo.

Planificar y poner en marcha innovaciones permanentes para posibilitar aprendizajes de calidad, contextualizados, relevantes y estructuralmente útiles (es decir perdurables).

Los estudiantes son parte de esta realidad de formación y tienen igualmente nuevos retos de urgente reconocimiento:

- Vivir en contacto con la sociedad con la realidad nacional e internacional para asimilar

ágilmente los cambios del entorno y las metas de formación necesarias.

- Asumir que su actividad formativa requiere una activa participación en la dedicación,

discusión y búsqueda de aprendizajes sólidos.

Desde esta perspectiva debemos seguir investigando nuevas posibilidades creativas para potenciar la formación integral y la utilidad de las tecnologías de información y comunicación (TIC) de manera que se conviertan en una oportunidad significativa para asumir estos desafíos en el marco de una educación refrescante en contenidos y en oportunidades de aprendizaje permanente para el profesor y el estudiante. Las TIC's en lugar de provocar temor en términos de innovación, permiten abrir el currículo y el aula, permeabilizar la formación sobre la base de un fuerte liderazgo y proactividad del profesor: quien es un docente investigador que revisa de modo permanente los contenidos del programa de curso.

Generando diversas oportunidades de aprendizaje mediante escenarios reales y virtuales potenciados por la investigación como medio de aprendizaje permanente (La Torre 2003, Bisquerra, 2004, Cabero, 2004).

La investigación y la innovación permanente tienen que ser parte de la cultura de trabajo de docentes, profesores y estudiantes; es necesaria una nueva cultura de vinculación real con la información la reflexión y la innovación, por cuanto en un mundo impredecible y riesgoso el pensamiento ágil, flexible, sorprendente, creativo y sensible es necesario ser cultivado desde la escuela, en la universidad y posteriormente en el mundo del trabajo.

8. USO DE LA INFORMACIÓN EN EL INTERNET

La introducción de las nuevas Tecnologías de la Información y Comunicación cambiaron el modelo de los sistemas de todo el mundo en cuanto al manejo y acceso de la información, teniendo un fuerte impacto en el ámbito escolar en el proceso de integración de los recurso tecnológicos y la aparición de las web 2.0 que hicieron posible el tránsito de los escenarios en la internet en el cual se presentaron diversas formas del acceso a la información de diferentes niveles como páginas web comerciales, bibliotecas virtuales, repositorios, proyectos artículos, en fin una cantidad de información que podía ser consultada y descargada promoviendo la facilidad para la infestación y el aporte al conocimiento, sin embargo existe una barrera asociada a las condiciones, prácticas y creencias del manejo de la información.

Con la creación del internet en diferentes aplicaciones en el año 1969, se construyó una red que ha permitido mezclar la comunicación y la tecnología, los computadores ya existían, pero el uso exclusivo era para tareas que facilitaran el trabajo de los seres humanos (Aguilar Rodríguez y Said Hung).

El uso del internet con el tiempo creció de manera excepcional en todo el mundo, convirtiéndose en una herramienta de suma importancia y popularidad, dotada de atributos que han permitido la evolución de las comunicaciones y la tecnología, (Sánchez, 2014).

En este contexto se desarrollarán varias actuaciones que han cambiado profundamente el quehacer pedagógico de los profesores y la forma como los estudiantes aprenden y consolidan el conocimiento desde diferentes perspectivas, que permiten el manejo libre de la información del estudiante.

El concepto del uso de Internet, por si solo tiene sentido pero cuando se observa la relación con los resultados de la acción adquiere relevancia de tal manera que la práctica del uso de la tecnología tiene un fin en particular en el ámbito del aprendizaje, (Anderson, 2008, Empirica, 2007, Rychen & Salganik, 2003) se refieren a las practicas con TIC que demuestran ser efectivas ya sea en la enseñanza de asignaturas o en el desarrollo de nuevas habilidades y competencias relacionadas con la emergencia del Internet y las demandas de la sociedad del conocimiento.

Entonces el buen uso del internet se verá reflejado en lograr mejores aprendizajes, innovación pedagogía y producir un cambio en los ámbitos donde se desenvuelvan con el manejo de la información.

El acceso de la información y el uso que implica un enfoque en el manejo de la información la (UNESCO 2008), hacia lo que llamo la “la Alfabetización digital” para preparar a los estudiantes para utilizar las tecnologías y apoyar el desarrollo social y mejorar la educación.

9. FORMACIÓN SOBRE EL USO DE LA TECNOLOGÍA

9.1. Formación docente

Según Beltrán y Marchesí (2000):

“...el educador es el guía en el proceso de comprensión de la realidad que lleva a cabo el educando. Esto implica que para poder llevar a cabo eficazmente esta tarea, lo primero que tiene que poseer el docente es el conocimiento de dicha realidad y si uno de los aspectos de la misma es la tecnología, es indispensable que la domine para poder desarrollarla”

Al respecto Castañeta (2009) comenta:

“La educación enfrenta uno de los desafíos más interesantes de su historia al responder a los requerimientos de un mundo en proceso de cambio, en donde los conocimientos y habilidades instrumentales con que contaba el docente para desempeñar su rol van quedando a la zaga de las demandas provenientes del adecuado cumplimiento de su tarea”. (Castañeda. 2009: p. 58)

Por su parte Harasim (2000) expone que el dominio del ordenador no es requisito previo, pero los profesores deben ser capaces al menos de manejar el entorno operativo, a fin de acceder y moverse por el sistema.

Desde el punto de vista de Beltrán y Marchesí (2000) la formación docente contribuye al dominio de las habilidades profesionales requeridas, a reducir la inseguridad que el cambio genera y a una actualización permanente.

Debido a la importancia de este tema, Fernández y Sevillano (2002: p. 114) proponen desarrollar las siguientes actividades en beneficio de la formación escolar:

1. Organizar y apoyar programas integrados de educación desde el nivel preescolar hasta el universitario, con vistas a desarrollar los conocimientos, técnicas y actitudes de los docentes en beneficio de la enseñanza.
2. Desarrollar cursos de formación para los profesores encaminados a mejorar su conocimiento y comprensión de los recursos tecnológicos. Así como

a familiarizarlos con métodos de enseñanza apropiados que tengan en cuenta el conocimiento de los estudiantes.

3. Educar para un uso constructivo del tiempo de ocio y al mismo tiempo la educación debe ir convirtiéndose en una actividad placentera.

Cada vez es más evidente el desfase de la educación formal con respecto a los cambios tecnológicos experimentados en el mundo de la comunicación, por lo que es necesario que las instituciones educativas proporcionen las herramientas adecuadas a los docentes para enfrentar este cambio.

9.2. Formación escolar

Desde el punto de vista de Fernández y Sevillano (2002):

“...la incorporación de la tecnología se va introduciendo lentamente en la escuela, sin embargo, se utilicen o no, en las aulas, el alumno accederá a ellas desde instancias no formales educativas”. (Fernández y Sevillano. 2002: p. 114)

La formación de estudiantes respecto al uso de cualquier tecnología puede ser suministrada en principio por el profesor, pero el método más útil para aprender es interactuar de forma continua con la tecnología y ganar habilidad mediante la experiencia. Los educandos necesitan aprender la mecánica del uso del sistema, incluyendo las aplicaciones especiales, la formación cara a cara supone una oportunidad para enseñar acerca del uso de la tecnología.

Según Harasim (2000) las habilidades del sistema y la teoría se pueden adquirir mediante una combinación de materiales impresos, un taller en red de un par de días de duración, pero el método más eficaz es mediante mentores. Añade que resultan útiles los manuales, folletos básicos de una página y enviar a los alumnos documentos o videos que ilustren como utilizar la herramienta.

Dado que estas herramientas no fueron creadas con fines pedagógicos, los docentes deben adaptarlas a las exigencias de los procesos educativos. Entendido así los maestros de escuela tienen un papel extraordinario cuando combinan la enseñanza

cara a cara con actividades en red, pues en esta situación la tecnología no es un sustituto sino una mejora de la enseñanza.

9.3. EL USO DEL INTERNET Y EL USO LEGAL DE LA INFORMACIÓN

El uso legal de la información parte de las políticas, normatividad y derechos de los usuarios que acceden a la información, tiene una fuerte relación con las conductas ética y las buenas prácticas que ella demanda para que la utilidad que proporciona las tecnologías de la información y comunicación no desborde a cometer delitos informáticos por el uso inapropiado.

Según, Sánchez (2001), hace referencia a que el “progreso tecnológico puede ser portador de beneficios o de perjuicios, según como se encauce la voluntad humana, dando origen a nuevas situaciones que han provocado la necesidad de nuevas elecciones y decisiones”, las conductas irresponsables en el mal uso de la información a visibilizado los profundos problemas y consecuencias que estos abarcan cada día más a jóvenes inexpertos o personas inescrupulosas, de ahí que las legislaciones y la jurisprudencia de los Tribunales de la mayoría de países han reconocido la importancia de defender los derechos a la intimidad como valor esencial, a la protección de la información. Es así que los sistemas educativos afrontan hoy problemáticas sobre el uso ilegal de la información por parte de los estudiantes y docentes en delitos informáticos como el plagio, el cyberbullyng, los derechos de autor, la falta de valores atenta contra la seguridad de la información, los derechos humanos, por ello en el proceso de integración de las tecnologías de la información y comunicación tuvieron que adaptar sus políticas frente al acceso y manejo de la información.

La integración de las TIC, implican cambios significativos en la sociedad de la información y como tal en esta nueva concepción el proceso de enseñanza-aprendizaje, (Salinas, 1997, p.7), la atención se centra en las destrezas emocionales e intelectuales a distintos niveles; la preparación de los jóvenes para asumir responsabilidades que demanda el mundo laboral con las competencias necesarias para este proceso de aprendizaje continuo.

9.4. DELITOS INFORMÁTICOS Y USO DE LAS REDES SOCIALES

El concepto de red social según Garton, Haythornthwaite y Wellman, (1998), “una red social es un grupo de personas (organizaciones u otras en entidades sociales) conectadas por diversas relaciones sociales como amistad, trabajo, intercambio de información, etc.”

Este concepto desde la perspectiva social, fue acomodado al uso del internet cuando apareció la interconexión de sujetos hablantes virtuales interconectados a través de los diversos canales abiertos de interacción, con las herramientas de la web 2.0 que a través del tiempo fue “transformándolo en medios de comunicación como consecuencia de las modificaciones y evoluciones propias del desarrollo e interacción de nuevas tecnologías de la comunicación, así como de la convergencia tecnológica entre los medios y particularmente por la irrupción de las tecnologías de redes abiertas” (Arrieta Zinguer , 2014, p.6).

Los jóvenes en su mayoría usan de manera habitual las redes sociales y se identifican desde el factor motivacionales (Colas, González, y De Pablos, 2013, p.15) convirtiéndola en fuente de uso relacional para cubrir necesidad psicológica como sociales, iniciando el contacto con las redes sociales desde aproximadamente los años edad sin ninguna restricción y vigilancia de sus padres convirtiéndose en un uso habitual y de cotidianidad (Colas, González, & De Pablos, 2013, p.21).

El uso inadecuado de las redes visibilizo una problemática respecto a los delitos informáticos originados por la conducta irresponsable del manejo de la información como el ciberlluying delito que en el marco jurídico constriñe la intimidad mediante el acoso y violencia entre dos o varios individuos, según Castells (2001), los nuevos escenarios de interrelación, dieron lugar a fenómenos sociales en las redes, donde el acoso entre estudiantes se hizo una práctica visible para los acosadores como el grooming y sexting, denominándose ciberbullying.

En las redes sociales es relativamente fácil la comisión de delitos debido al acceso a la información y manipulación de está con intenciones de causar daño psicológico según Cea Jiménez (2011) el internet con las redes sociales reúnen una

“serie de particularidades específicas como la eliminación de la barrera del espacio ya que, debido a la utilización de la red de Internet que llega a cualquier lugar del mundo, no es necesario estar presente físicamente en el lugar donde se cometa el delito”.

Estos retos que suponen para la organización del proceso de enseñanza-aprendizaje dependerán en gran medida en la normatividad y políticas que adopte para que la formación con sus recursos se desarrolle con las competencias requeridas para desenvolverse como profesional.

10. DELITOS INFORMÁTICOS

Así, como las nuevas tecnologías nos traen destacables ventajas, es importante responder eficientemente a la necesidad de regular las conductas que pueden derivarse de su uso indebido. Los delitos informáticos son considerados un aspecto negativo del desarrollo de la informática y se producen debido a las posibilidades que las computadoras ofrecen para infringir la ley. En este contexto, aparecen conductas que vulneran bienes jurídicos no convencionales, o comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales. Empero, los aspectos negativos comprenden inimaginables formas de cometer delitos. En el plano jurídico penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías. Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes. Además, los delitos informáticos se caracterizan por las dificultades que entraña descubrirla, probarla y perseguirla, a ello se añade la facilidad de penetrar en los sistemas informáticos.

10.1. CONCEPTO DE DELITOS INFORMÁTICOS.

Es necesario realizar un concepto sobre los llamados delitos informáticos. Al respecto, se han formulado en doctrina diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora. Existe diferentes conceptos acerca de los delitos informáticos, a continuación, citaremos algunos autores que se refieren a los delitos informáticos de la siguiente manera:

“Jimena Leyva define a los delitos informáticos como: toda acción típica antijurídica y culpable para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma.” (Viega, 2003, p. 178)

Miguel Ángel Davara Rodríguez señala que ... “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software” (Davara,2000,p.15)

El Convenio de Ciber delincuencia del Consejo de Europa de 23 de noviembre del 2001 llevado a cabo en Budapest, define los delitos informáticos como ...” actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos.”

Las Naciones Unidas, conceptualiza a los delitos informáticos como “todos los delitos cometidos por medio de tecnologías de información; en contra de cualquiera de sus componentes o los que fueren cometidos por medio de tecnologías de información.”

Julio Téllez Valdés conceptualiza ...” delito informático de forma típica y atípica, entendiendo a la primera como las conductas típicas, antijurídicas y culpables, en las que se tienen a las computadoras como instrumento o fin y a las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.” (Téllez, 1996, p. 103-104)

Ricardo M. Matta y Martín define al delito informático como “toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.” (Matta y Martín, 2001, p. 21)

Los delitos informáticos en sentido estricto vendrían a ser todo comportamiento ilícito que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, para llevar a cabo actos ilícitos, esta es una visión limitada porque existen

muchos delitos que no pueden tipificarse con las leyes vigentes y, ante la ausencia de una normatividad acorde, se habla de lagunas o de falta de regulación.

10.2. CARACTERÍSTICAS DEL DELITO INFORMÁTICO.

De acuerdo a las características que menciona en su libro Derecho Informático el Dr. Julio Téllez Valdés (2004: 163), se podría enunciar algunas de las características fundamentales que revisten este tipo de acciones:

- Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.

- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

- Son muy sofisticados y relativamente frecuentes en el ámbito militar. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

- En su mayoría son imprudenciales y no necesariamente se cometen con intención. Ofrecen facilidades para su comisión a los mentores de edad.

- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

10.3. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

Téllez Valdés (2004: 165-167), clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

10.3.1. **Como instrumento o medio:** en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).

d) Lectura, sustracción o copiado de información confidencial.

e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de cómputo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

10.3.2. **Como fin u objetivo:** en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como, por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a los dispositivos de almacenamiento.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

10.4. SUJETOS Y RELACIONES QUE SURGEN DEL DELITO INFORMÁTICO

10.4.1. SUJETO ACTIVO

“El sujeto activo de los delitos informáticos, puede ser cualquier persona abarca tanto a particulares como funcionarios públicos,”. El sujeto activo simplemente encuentra la manera de ingresar a la información o contenido del área protegida en si ingresa a los sistemas operativos como un intruso, vulnerar sistemas de seguridad es un reto personal en si el sujeto activo de los delitos informáticos tiene habilidades específicas para el manejo de los sistemas informáticos. (Saez, 2014, p. 234)

“Es evidente que el nivel de aptitudes del delincuente informático es hoy un tema de controversia, ya que, para algunos estudiosos del tema, dicho nivel no es indicador

de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pueden encontrarse en un empleado del sector de procesamiento de datos de cualquier organización”.

Los sujetos activos de los delitos informáticos tienen las siguientes características:

- a) Poseen importantes conocimientos de informática.
- b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible se los denomina delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.
- c) A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar un sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de la cuenta de los clientes.
- d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.
- e) Estos delitos se han calificado de cuello blanco, porque el sujeto que comete el delito es una persona de cierto estatus socioeconómico.” (Viega, 2003, p. 180-181)

Al desarrollar todas estas características, es evidente que el sujeto activo de los delitos informáticos son personas que conocen los sistemas operativos, así como conocen como vulnerar dichos sistemas y usar de manera ilícita la información ya sea información personal de algún usuario o información institucional de empresas públicas o privadas.

“Es de destacar que la cifra negra de delitos informáticos es muy alta. No es fácil descubrirlos ni sancionarlos. Los daños económicos son altísimos. Se habla de

pérdidas anuales por los delitos informáticos y otros tecno-crímenes que van de ser los U\$S 100 millones hasta la suma de U\$ 5.000 millones, estos datos de acuerdo a un estudio realizado a finales de los años 1990 hecho por una firma auditora.”

10.4.2. SUJETO PASIVO

“El sujeto pasivo son aquellos sobre los que recae la acción u omisión que realiza el sujeto activo.” (25) en realidad el sujeto pasivo es la víctima del delito es el sujeto en el cual recae la acción u omisión que realiza el sujeto activo, las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, instituciones bancarias etc., que usan sistemas automatizados de información, generalmente conectados a internet. “En el caso el sujeto pasivo es el titular del sistema u ordenador intrusado incluso muchas veces a los proveedores de servicios públicos, sistemas financieros y casos hay de algún servicio de inteligencia de una gran potencia.” (Saez, 2014, p. 235)

El sujeto pasivo puede ser desde una familia, individuos, empresas grandes y pequeñas, instituciones públicas privadas, instituciones bancarias, gobiernos, que utilizan sistemas automatizados de información, los cuales, por lo general se encuentran conectados a internet. La condición relevante a cumplir por el sujeto pasivo, es la de poseer información en formato digital y almacenada en un medio informático pueden ser datos, programas, documentos electrónicos, dinero electrónico, información, etc., y que se encuentra en contacto directo con la tecnología, específicamente con las redes de Internet.

11. PERFIL CRIMINOLÓGICO

“Las tecnologías de la información han facilitado la aparición de nuevas conductas que con independencia del mayor o menor reproche social generado, han obligado a los países avanzados a adaptar sus legislaciones para dar cabida a modalidades comisivas que no existían hace unos años.” (Rivas, 1999, p. 134-135)

Existen diferentes tipos de perfil de delincuentes informáticos y se clasifican de la siguiente manera:

a) Hacker Persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico actúa por curiosidad... “Con el termino hacking nos referimos a la técnica consistente en acceder a un sistema informático sin autorización. Entendemos que existe autorización cuando el sistema está conectado a una red pública y no dispone de un control de acceso mediante el uso de identificadores de usuario y password accediendo a información confidencial del usuario.”

b) Cracker Aquel que rompe con la seguridad de un sistema, hablar de... “craks nos referimos a los programas o rutinas que permiten utilizar o inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática.”

c) Preaker Es aquella persona que intercepta la red telefónica para obtener beneficios personales, “preacking entraría en las técnicas de fraude en materia telefónica analógica y digital.”

d) Phisher...”es aquella persona que se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.”

Habiendo expuesto el concepto de delito informático, y en razón de no extendernos en temas que serán tratados en otros puntos de la presente investigación, pasaremos a desarrollar la teoría del delito con relación a los delitos informáticos.

12. PRINCIPALES PELIGROS EN INTERNET

Las nuevas tecnologías e Internet son una herramienta útil para aprender, comunicarse y divertirse. Sin embargo, como cualquier instrumento o actividad tienen sus peligros, especialmente para los más indefensos: los niños y adolescentes.

12.1. ACOSO CIBERNÉTICO

Uno de los mayores peligros de Internet es el Acoso Cibernético. Muchas personas crean perfiles falsos en redes sociales para amenazar y acosar

anónimamente a una persona en específico. Las víctimas de acoso cibernético tienen que enfrentar problemas psicológicos que interfieren con su vida diaria (trabajo, escuela, etc.)

En la mayoría de los casos las víctimas de acoso cibernético tienen baja autoestima y, en casos más dramáticos, presentan tendencias suicidas. El acoso cibernético hace vulnerable a la víctima, ya que el victimario puede atacar desde cualquier lugar y a cualquier hora.

12.2. ROBO DE IDENTIDAD

El Internet es lugar donde prevalece el cruce desmedido de información, pero debemos ser muy cuidadosos con nuestros datos porque nuestra información personal puede ser fácilmente robada por criminales cibernéticos.

En miles de ocasiones la policía cibernética ha enfrentado casos en los que el robo de identidad consiste en crear cuantas falsas en redes sociales con la información pública de algún usuario. De esta manera los criminales hacen uso de los datos personales a través de cuentas falsas para fines pornográficos. Es otro de los mayores peligros de Internet.

12.3. SPAM O CORREO BASURA

Cuando hablamos de SPAM electrónico, nos referimos a mensajes no deseados o correo basura. El hecho de que un correo electrónico se clasifique como SPAM es porque este tipo de mensajes se envían de forma masiva a un gran número de destinatarios. En ocasiones el SPAM solo se reduce a publicidad que nadie pidió, pero también puede incluir malware, el cual permite la descarga de virus que posiblemente dañe nuestro sistema operativo.

12.4. INFORMACIÓN NOCIVA

En un inicio comentamos acerca de la gran cantidad de datos que podemos encontrar en Internet, asimismo es importante recalcar que esa información puede ser nociva por tener contenido susceptible.

Mucha información en Internet contiene pornografía, crímenes, actos terroristas y suicidas, etc. Muchos adultos podemos optar para mantener una postura analítica ante estos hechos, sin embargo, los niños y adolescentes son más vulnerables ante tal información, por el cual, debemos tener especial cuidado con el uso que los menores de edad hacen sobre el Internet para que no expongamos a los mayores peligros de Internet.

12.5. PIRATERÍA

La piratería es el acto de plagiar o descargar de forma ilegal material con derechos de autor. En Internet el mundo de las piraterías es bastante grande, existe el plagio de obras literarias, cinematográficas, etc. El dinero que pierden los autores de dichos contenidos es inmenso, año tras año, la piratería es uno de los mayores peligros de Internet que sigue en ascenso y las pérdidas económicas son infinitas.

12.6. PORNOGRAFÍA

La pornografía es una de las industrias que más ingresos reporta anualmente en todo el mundo. El fácil acceso a Internet que provoca que los menores de edad estén expuestos a estos contenidos eróticos, los cuales pueden perjudicar su salud mental, ya que no tienen la suficiente madurez para entender los aspectos sexuales que se ciernen sobre el material pornográfico, esta inmadurez puede provocar en los niños una idea errónea de lo que es el sexo.

12.7. ACOSO SEXUAL O GROO MING

Se llama Groo Ming a las acciones deliberadas, realizadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos contra los niños.

12.8. AMENAZAS A LA PRIVACIDAD SEXTING

Proviene del acrónimo formado Sex y Texting. Inicialmente, y como lo indica su nombre, se trataba del envío de mensajes con contenidos eróticos. Posteriormente, dado el avance tecnológico, esta modalidad evoluciono hacia el intercambio de imágenes y videos convirtiéndose en una práctica habitual entre adolescentes y niños. Se produce cuando se envían fotografías, audios o videos de carácter sexual, generalmente a través del teléfono móvil, y redes sociales las que luego posiblemente terceras personas se encargaran de distribuir.

12.9. REVELACIÓN DE INFORMACIÓN

Ya sea de forma consiente, en una conversación de chat o en una red social, o inconsciente a través de engaños (estafas, falsas ofertas, sorteos o regalos), tu hijo puede revelar sus datos personales online sin darse cuenta del peligro que supone. Ignorar correos que piden cualquier tipo de información, no introducir nunca datos como dirección o el teléfono móvil en ninguna web por muy segura que parezca o evitar este problema.

12.10.DELITOS ECONÓMICOS Y FRAUDES

Al utilizar las tecnologías para realizar operaciones financieras estamos expuestos a riesgos si no tomamos las precauciones oportunas como utilizar ordenadores con antivirus actualizados, tener los sistemas operáticos actualizados, entrar en las páginas seguras de plataformas bancarias etc.

El fraude tiene dos consecuencias directas sobre los usuarios: en primer lugar, la pérdida económica tangible en caso de que el ciber delincuente consiga su propósito; en segundo lugar, la posible pérdida de confianza que podemos experimentar ser víctima de una situación de fraude, lo que nos llevara a volver al banco a realizar nuestras transferencias.

CAPITULO III
MARCO JURÍDICO

1. LEGISLACIÓN NACIONAL

1.1. CONSTITUCIÓN POLÍTICA DEL ESTADO

1.1.1. ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Artículo 130.

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

Artículo 131.

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la, Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de

Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

Si bien todo sistema legislativo y normativo referido a un determinado campo, atraviesa por un proceso de construcción que acompaña su evolución; para el caso de la Informática en Bolivia aún se tiene un acompañamiento jurídico poco nutrido.

En esta oportunidad se han identificado varias disposiciones legales que tienen implicancia directa o indirecta con la delincuencia Informática: Decreto Supremo N° 27329 “Transparencia y Acceso a la Información”, Ley N° 341 “Ley de Participación y Control Social”, Decreto Supremo N° 1391 “Reglamento a la Ley N° 164”, Decreto Supremo N° 1793 “Reglamento para el Acceso, uso y Desarrollo de las Tecnologías de Información y Comunicación”, Ley N° 650 “Agenda Patriótica 2025”, Decreto Supremo N° 2514” Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación”, Ley 777 “Ley del sistema de Planificación Integral del Estado SPIE”, Ley N° 779 Desburocratización para la creación y funcionamiento de Unidades Económicas” y el Decreto Supremo 0667 “Código de Procesamiento Penal”.

1.2. DECRETO SUPREMO N° 27329 “TRANSPARENCIA Y ACCESO A LA INFORMACIÓN”

Aunque con una visión de Estado, con el D.S. N° 27329 se inician las pautas hacia el camino de constitución de un cuerpo normativo específico a las Tecnologías de Información y Comunicación (TIC) en Bolivia. En esta disposición se resalta la necesidad de disponer de una ley general de acceso a la información, así también, de procurar una normativa que permita la transparencia y acceso gubernamental por parte de la ciudadanía.

Así como el D.S. N° 27329 se involucra al acceso de información por las personas, también se trata sobre la necesidad de considerar algún tipo de información como clasificada; entre varias como la financiera, y la correspondiente a la delincuencia, lo ilícito y criminal, como para hacer seguimientos y dar con delincuentes los que en este caso pueden ser informáticos.

1.3. LEY N° 164 “LEY GENERAL DE TELECOMUNICACIONES, TECNOLÓGICAS DE INFORMACIÓN Y COMUNICACIÓN”

Constituye una Ley General, y dirigida específicamente a la informática, pero no aborda los delitos Informáticos, en la que se analizan ampliamente los procesos de uso de la tecnología y se regula su aprovechamiento lícito y sus implicancias ilícitas, en resguardo de los derechos y obligaciones de las personas en el país.

Son relevantes las muchas definiciones técnicas sobre informática que se hacen en la disposición, aunque no existe ninguna sobre la delincuencia digital o informática; por lo que llama la atención la falta de enunciación de alguna competencia de Estado respecto a la delincuencia o delitos informáticos. Sin embargo, en la Ley N° 164 se trata de políticas, beneficios y ámbitos de aplicación técnicos de la informática en la vida nacional. Es importante el detalle de aspectos técnicos que se hacen en la disposición como la regulación de espectros radio magnéticos, sin considerar sus posibles acciones ilícitas, presentándose muchos aspectos técnicos de manejo, regulación y alcance de los servicios, por ejemplo.

En el Capítulo Quinto Contratos, se menciona sobre la protección de los derechos de usuarios y de los datos personales. También se trata acerca de la realización de comercio electrónico dentro ambientes técnicamente confiables; evidenciando las posibilidades de pasarse a la justicia ordinaria en caso de controversias.

Por otro lado, se regula sobre los derechos de creación, transmisión, recepción y almacenamiento de correo electrónico; dentro lo que se mencionan sus infracciones y sanciones considerando los criterios de: naturaleza y gravedad de hecho, extensión y magnitud del peligro o daño causado, dolo o culpa en la comisión de la infracción, existencia de agravantes y atenuantes en la comisión de la infracción; y entre las infracciones se encuentra: apercibimiento, secuestro o embargo de equipos y material; multas e inhabilitación temporal para ejercer actividades referidas a telecomunicaciones y TIC, cesación de los actos por el infractor, resarcimiento de daños y perjuicios

establecidos jurídicamente, igualmente medidas de apercibimiento o llamadas de atención por escrito a los infractores si el hecho ilícito y se conmina.

Puntualizando, respecto al secuestro de equipos, componentes, piezas y materiales; dentro de la Ley N° 164 esta acción se considera como una medida precautoria que debe apoyarse en un reglamento, realizarse bajo inventario y siempre y cuando no se afecten a terceros. Al respecto, las clasificaciones de las infracciones son: presentación o ejercicio ilegal de un servicio, accionar contra un sistema general o contra usuarios, proveedores u operadores, contra la autoridad fiscalizadora (Estado); para todos los casos, las sanciones quedan pendientes a tipificarse en un reglamento posterior.

1.4. LEY N° 341 “LEY DE PARTICIPACIÓN Y CONTROL SOCIAL”

Con relación al tema de análisis; en la Ley N° 441 se hace referencia a lo indispensable de apoyar el control social de la administración pública en la informática ejercido por la sociedad. Resaltando la necesidad de coadyuvar con la fiscalización y control en todas las áreas de gestión que hacen a la administración pública los que mediante reclamos o denuncias podrán afectar favorablemente sobre los aspectos ilícitos relativos a informática pudiéndose a exigir la restitución o reparación integral de vulneración de un derecho si esto se da, y si constituye un delito tiene que ser remitido al Ministerio Público para ser investigado.

Asimismo, en la Ley N°341 se encomienda al Estado la creación de redes de información, un gobierno electrónico, telecentros y otros instrumentos similares que permitan el control social, incluso se menciona la difusión de informes utilizando sitios web oficiales aspecto que guarda relación con el Programa Nacional de Telecomunicaciones de Inclusión Social.

1.5. DECRETO SUPREMO N°27330 “SIMPLIFICACIÓN DE TRAMITES EN LA ADMINISTRACIÓN PÚBLICA”

Aunque de forma indirecta, en el D.S. N° 27330 se plantea simplificar los procesos de trámites ordinarios recurrentes a los ciudadanos en la administración

pública, fin que conlleva apoyarse en la tecnología informática. Sin lugar a duda, pese a que es una importante medida de eficiencia abre mayores posibilidades para que los ciber delincuentes puedan resultar una nueva amenaza para sociedad.

1.6. DECRETO SUPREMO N°1391 “REGLAMENTO 1391 “REGLAMENTO A LA LEY N°164”

Toda Ley se operativiza mediante reglamentos, como es el caso del D.S. N° 1391 que complementa la Ley N° 164. En esta disposición que corresponde a un Reglamento General, se regulan y reglamentan todos los aspectos y ámbitos de aplicación de las actividades de telecomunicaciones y TIC que comprende la Ley antes mencionada, no obstante respecto a la seguridad informática se reconocen los derechos jurídicos de los usuarios informáticos. También se hacen definiciones similares y repetitivas a las encontradas en la Ley N°164, entre las que tampoco existe alguna concreta que toque la delincuencia informática.

En esta disposición se considera la interferencia perjudicial como una afectación informática, mencionándose que en ese caso la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT), debe tomar las acciones legales pertinentes. Asimismo, se establece la protección de las operadoras telefónicas en caso de detección de indicios suficientes de fraude o conexiones ilegales, para lo cual el asunto adoptaría una figura legal.

También se aborda algunos inconvenientes posibles a sufrir los usuarios que pueden dar pautas de delito respecto a uso telefónico y de Internet, para los que la medida de protección es la firma de contratos específicos (relación contractual) con los operadores desde una perspectiva de protección al consumidor, no contra amenazas o delitos informáticos.

Adicionalmente en este Decreto Supremo se menciona sobre la inviolabilidad de datos e información personal y de comunicación de las personas, asequible solo por orden judicial mostrándose como delitos:

Suplantación de identidad, sustracción, interceptación, interferencia, obstrucción, cambio o alteración de contenidos, desvío de curso de comunicación, publicación, divulgación, diseminación, utilización de contenidos de comunicación; mismos que están referidos a telecomunicación, son inferibles a la informática. Sin embargo, se hace evidente un contenido normativo fuertemente proteccionista con relación al Estado, pero no así sobre usuarios, quienes son los más vulnerables.

1.7. DECRETO SUPREMO N° 1793 “REGLAMENTO PARA EL ACCESO, USO Y DESARROLLO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN”

Corresponde a un Reglamento Específico de la Ley N° 164 referido a software libre, en el que, entre algunas de sus definiciones de importancia para circunscribir un delito informático, ya se identifican dos principales entendimientos importantes para este artículo:

Seguridad informática, entendida como el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de infraestructura computacional y todo lo relacionada con esta, y especialmente, la información contenida o circulante.

Seguridad de la información, definida como la preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como autenticidad, responsabilidad, no repudio y confiabilidad.

Por otra parte, en este cuerpo normativo se proponen líneas de acción y políticas de seguridad informática; la creación del Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación (COSTETIC), como instancia que trabajé y amplié más reglamentos posibilitando los relacionados con la delincuencia informática.

Por último recalcar sobre la protección de los datos personales; en el D.S. N° 1973 también se dan varias pautas sobre propiedad y derechos de software libre

mediante los certificados digitales, aspecto que constituye un aporte más en términos de seguridad informática.

1.8. DECRETO SUPREMO Nº 2514 “CREACIÓN DE LA AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN”

En el D.S. que dispone la creación de la Agencia Electrónica y Tecnologías de Información y Comunicación, también se inscriben las funciones y atribuciones que este tendría como el establecimiento de información para entidades del sector público.

Por otro lado, en esta disposición también se dispone la existencia del Centro de Gestión de Incidentes Informáticos, instancia que servirá para elaborar planes institucionales de seguridad informática. La desventaja es que todo refleja un beneficio para el Estado y no así para los usuarios.

1.9. LEY 777 “LEY DEL SISTEMA DE PLANIFICACIÓN INTEGRAL DEL ESTADO SPIE”

En este se integran todos los procesos de planificación que se dan en el país, entre los que se incorpora el tecnológico informático.

Corresponde a otra forma de ver la toma de decisiones, concibiéndose una nueva forma de planificar el Estado denominado Planificación Territorial del Desarrollo Integral, en la que ya se considera la tecnología como parte de la vida.

1.10. LEY Nº 779 “DESBUROCRATIZACIÓN PARA LA CREACIÓN FUNCIONAMIENTO DE UNIDADES ECONÓMICAS”

De la misma manera la condicionante de la Ley Nº 779 respecto a la seguridad informática, está en el permitir la creación de mecanismos en calidad de plataformas para mantener controladas todas las Unidades Económicas en el país personales y jurídicas aspecto de relevante relación porque los mecanismos a los que hace referencia son informáticos y de trasfondo económico, lo que implica posibilidades de surgimiento de amenazas informáticas, y por lo tanto ciber delincuencia.

1.11. DELITOS INFORMÁTICOS CÓDIGO PENAL BOLIVIANO

Artículo 363 bis. - (MANIPULACIÓN INFORMÁTICA)

El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Este tipo penal prevé aquella conducta por la cual se modifica información ya sea en el momento de su procesamiento o de su transmisión, es decir en el momento en la que esta información está siendo procesada por un sistema informático o cuando después de haber sido procesada, es transmitida. Para que esta conducta constituya delito, debe producirse una transferencia patrimonial en perjuicio de un tercero y así generar un beneficio indebido

Es importante resalta que este tipo penal no toma en cuenta el hecho de la manipulación del procesamiento o transferencia de datos sea realizada mediante un acceso no autorizado a la información, es decir que en este tipo penal no se toma en cuenta la posibilidad de la violación de los sistemas de seguridad o del acceso sin autorización a los sistemas informáticos, sino que se toma como presupuesto del tipo penal al resultado mismo.

Artículo 363 ter. - (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS)

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Al igual que la tipificación establecida en el artículo 363 bis del Código Penal, que constituye un delito de resultado, es decir que la tipicidad requiere de un resultado

(la transferencia patrimonial en perjuicio de un tercero y generando un beneficio indebido).

En el caso del artículo 363 ter. Se observa que el tipo penal exige que la acción realizadora del tipo (el acceso no autorizado a un sistema informático, para apoderarse, utilizar y modificar información) deba de derivar a un resultado típico (ocasionar un perjuicio a un tercero).

En este tipo penal se está protegiendo la integridad del sistema mismo y de la información procesada o contenida en él, los denominados virus informáticos son precisamente un ejemplo de destrucción o supresión de la información.

En cuanto al contenido general de los artículos son amplios y vagos, pero cubre, de cierta manera, la laguna legal existente hasta ese momento. En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito, una finalidad deseada que causa un perjuicio a otro, o a un tercero.

1.12. CÓDIGO NIÑO, NIÑA ADOLECENTE

En cuanto a dicho código hace referencia al delito que se tiene Tipificado como Acoso Cibernético: Esta es una nueva figura legal que ha sido incluido en el Código Niño, Niña Adolescente aprobado el 2015 en la Asamblea Legislativa Plurinacional.

La pena para quienes incurran en este delito será entre cuatro y ocho años de privación de libertad.

1.13. DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS “ONU”

Los Fraudes cometidos mediante Manipulación de Computadoras que están reconocidos por la ONU. Son:

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.

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 equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo, Es una técnica especializada que se denomina "técnica del salami o salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

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 fotocopadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopadoras 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.

Acceso no autorizado a servicios y sistemas informáticos, 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 uno de los diversos medios que se mencionan a continuación. 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, Esta 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, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

CAPITULO IV

MARCO PRÁCTICO

En este capítulo se presentarán los hallazgos sobre la muestra estudiada y los análisis de los resultados del procesamiento de datos con la herramienta de encuesta. Sin embargo, antes de iniciar con este análisis es importante describir la muestra en cuanto a sus características demográficas iniciales, de tal forma que se puedan tomar en cuenta para el análisis final de los resultados ya que las variaciones de algunas de estas características podrían considerarse como parte de las causas de variaciones en algunos de los resultados analizados.

1. RESULTADOS DE LA ENCUESTA

1. ¿Conoce usted tiene conocimiento de la importancia del internet para los delitos?



FUENTE: Elaboración Propia

2. ¿Usted cree que debería sancionarse aspectos del uso individuo de la información del internet?



FUENTE: Elaboración Propia

3. ¿Usted cree que debe actualizarse nuestro código penal ante delitos informáticos?



FUENTE: Elaboración Propia

4. ¿Cree usted que las redes sociales son la principal herramienta o medio que se utiliza frecuentemente para efectuar los delitos informáticos?



FUENTE: Elaboración Propia

5. ¿Usted cree que el ciberacoso merece la atención de las autoridades de

gobierno?



FUENTE: Elaboración Propia

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES

Si bien el uso del Internet como el uso de las redes sociales es importante para el desarrollo de la Educación de los estudiantes, es una muestra evidente de las formas de interacción que permite a los profesores establezcan una comunicación fluida y dinámica para el mayor conocimiento del manejo de las mismas.

Se puede concluir que las redes se están convirtiendo en una herramienta que permite el desarrollo de las habilidades comunicativas y puede ser utilizada como estrategia de aprendizaje por parte de los estudiantes, ya que la mayoría de ellos las usan siempre, aunque consideran que lo hacen sin ningún beneficio específico, a pesar de que si las incluyen como parte de sus actividades académicas.

Castro y Hernández (2014) plantean que las redes sociales son una nueva forma de interacción y uno de los servicios más utilizados por los internautas actualmente, especialmente por los jóvenes. Constituyen una herramienta de comunicación sin fronteras que nos permite mantener la proximidad poniendo en contacto a amigos y a personas que se identifican con las mismas necesidades, aficiones o inquietudes. Estos medios, inciden más que nunca en la educación de las nuevas generaciones, moldean gustos e incluso influyen en la manera como el individuo se relaciona consigo mismo, con sus semejantes y con el mundo.

Las personas están cambiando, el Internet está modificando los hábitos de vida de la sociedad moderna. La tecnología ha permeado la vida de las personas y herramientas como Internet y las redes sociales ahora son parte de la cotidianidad de las personas, transformando significativamente la forma de comunicarnos. Las nuevas generaciones no han sido ajenas a estas transformaciones. De la misma forma que algunos crecimos en su momento, por ejemplo, influenciados por el auge y el crecimiento de la informática o los videojuegos, los niños y jóvenes de hoy en día, los

dueños del futuro, están haciendo lo propio con Internet: han nacido con la Red, están creciendo con la Red y están viviendo con la Red.

En el ámbito educativo en Bolivia, se evidencia este fenómeno. Los educandos manejan a la perfección las redes sociales, se encuentran registrados en más de una red social, ya que les permite montar fotos, videos y hacer comentarios sobre muchos temas que les interesan, creando así una identidad digital propia.

Es indiscutible resaltar el impacto que ha tenido el uso de la Redes Sociales y el Internet en los estudiantes de secundaria tenemos que considerar que muchos de ellos no solo utilizan para el desarrollo de sus actividades escolares. Sino para estar en contacto con amigos o compañeros generando mas relaciones con otras personas ajenas a ellos. Cabe resaltar que los estudiantes no tienen un conocimiento adecuado sobre los peligros que conlleva al ingreso de diferentes páginas del Internet llevando a muchos de ellos a cometer diferentes tipos de Delitos Informáticos sin darse cuenta de los mismos.

2. RECOMENDACIONES

Si bien, el internet y las redes sociales son de gran importancia en la actualidad, la aplicación de estas nuevas tecnologías de información puede generar también dependencia considerando el uso diario que hacen del mismo.

Por lo tanto, es importante que los profesores puedan tener una formación adecuada sobre el Internet sano de todos los programas de formación de educativa pueden resaltar la importancia del internet en el proceso de enseñanza aprendizaje, también puede ser perjudicial en el ámbito de las redes sociales, porque en realidad no se llega a conocer a las personas con las que están en contacto y se han dado muchos casos que se llegan a generar diversos tipos de Delitos Informáticos.

Los profesores deben hacer notar estos aspectos en los estudiantes de secundaria y poner en conocimiento de los mismos los pro y contras del internet y las redes sociales. Tratando de generar reflexiones pedagógicas sobre el uso adecuado de los contenidos de la Internet en la práctica docente. Se trata de reflexiones y

discusiones entorno al uso adecuado de la Internet tanto en el uso personal y profesional de los docentes, como en la responsabilidad de los mismos en la formación de sus estudiantes.

Informar a los Docentes sobre los peligros presentes en la Internet, para que estos a su vez puedan realizar un acompañamiento efectivo a sus estudiantes.

Realizar prácticas, pedagógicas entorno a la orientación en los estudiantes y padres de familia en el uso sano de la Internet y Redes Sociales. Las practicas Pedagógicas son actividades en las cuales los Docentes se informan e interactúan con los contenidos de un Internet sano, analizan situaciones reales, sobre los peligros de la Internet con sus estudiantes y poder diseñar actividades prácticas en el aula de clases.

También se debería informar a los Docentes acerca de las Autoridades Competentes, y de los medios y procedimientos para denunciar las amenazas presentes en la Redes Sociales.

Por otro lado, el colegio debería incluir los famosos talleres para padres promoviendo la seguridad en Internet de nuestros hijos dando a conocer las ventajas y desventajas que tiene el uso del Internet considerando también los procesos de información sobre el uso excesivo del internet y las redes sociales y contenidos inapropiados y negativos y resaltar los beneficios y perjuicios que estos generan en los estudiantes.

Los estudiantes deben tomar conciencia de los peligros y beneficios que brindan las redes sociales y sobre ello la importancia del internet para la formación en el nivel secundario, así mismo considerando la basta oportunidad que brinda el internet para la investigación.

BIBLIOGRAFÍA

Brandon, S. (2017). La policia y los delitos informaticos . *Razon* , pág. 9.

ESPINOZA, F. P. (2016). *Paz Espinoza Félix C., Derecho del Niñez y Adolescencia*, . La Paz.

FALCONI, J. G. (2009). *El Menor de Edad Infractor y su Juzgamiento en la Legislación*. Ecuador.

FRANCISCO, M. C. (2004). *Derecho Penal. Parte General*. Valencia, España: Tirant Lo Blanch.

GOLDSTEIN, R. (2018). *Diccionario de Ciencias Penales*. España.

HARB, B. M. (2016). *Benjamín Miguel Harb, Derecho Penal Tomo II Delitos en Particular*. La Paz.

HERRERA, W. (2013). *Derecho Procesal, el proceso penal boliviano*. . Cochabamba – Bolivia: 3ra. Edición. Grupo Editorial Kipus. .

HERRERA, W. A. (2010). *El Proceso penal Boliviano*. La Paz : Kipus.

KOLLE, P. D. (2012). *Pacheco de Kolle Sandra, Evolución Histórica del derecho penal juvenil*. España.

LOMBARDÍA, S. (1996). *metodologia de investigacion* . Peru.

MAMANI, M. L. (2012). *Políticas juridicas y pedagogicas para la prevencion de delitos en las unidades educativas del nivel secundario de la ciudad de la ciudad de El Alto*. La Paz.

MARLI, J. (2019). *INFORMACION TECNOLOGICA EN LOS ULTIMOS TIEMPOS* . EEUU.

MÉRIDA, W. A. (2012). *La Adolescencia*. La Paz: UMSA.

- MONTENEGRO, C. (2019). *Políticas para delitos cometido por adolescentes* . Chile.
- Nina, W. (2019). *Metodología de investigación* . La Paz Bolivia: Trabajos de Derecho Bolivia.
- NUÑES, A. J. (2014). *Victimología y violencia criminal Colección Bibliográfica de Ciencia*. Bolivia.
- RETAMOZO, V. H. (2012). *Apuntes de Docencia de Doctrina Jurídica, UMSA*. La Paz.
- RISLE, I. B. (1996). *Manual de Orientación Educacional*. España.
- TOLA, R. (2006). *Diccionario jurídico* . España.
- VARGAS, G. (2002). *metodología*. Bolivia.
- YUGAR, F. R. (2013). *Métodos y Técnicas de Investigación Camino a la Tesis* . Colombia.
- ZAFFARONI, E. R. (2007). *Tratado de Derecho Penal, Tomo IV, EDITAR, Sociedad Anónima*. Argentina.