Año 25 No. 89
Enero - Marzo 2020

RVG

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 25 N° 89, 2020, 351-368
ISSN 1315-9984

Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios

Acosta, Maria Gabriela[1]
Benavides, Merck Milko[2]
García, Nelson Patricio3

Resumen

Los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets. El objetivo de la investigación es determinar los principales tipos de delitos informáticos existentes y, los riesgos que estos generan para la sociedad, las empresas y los gobiernos. Es una investigación de tipo mixta, apoyados en estudios confirmatorios y estudios exploratorios, resaltando teorías y Leyes que tienen relación con el estudio. Los resultados de la investigación, arrojan la importancia de determinar los diferentes tipos de delitos informáticos existentes. Así como, el reconocimiento de los puntos álgidos respecto a la seguridad de las redes, para contrarrestar su expansión. Finalmente, los delitos informáticos representan toda acción anti-jurídica, vía cibernética,

Recibido: 23-09-19 Aceptado: 05-12-19

[1] Licenciada en Ciencias Públicas y Sociales, Doctora en Jurisprudencia y Abogado de los Tribunales y Juzgados de la República del Ecuador, Magister en Derecho Penal y Procesal Penal. Magíster en Docencia Universitaria. En el ámbito laboral se ha desempeñado como Abogado en libre ejercicio. No obstante, en el ámbito de la docencia es Docente Titular de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato. En la actualidad, ejerce la función de Coordinadora de la Carrera de Derecho en la misma institución. ORCID: https://orcid.org/0000-0002-7200-1446.

[2] Doctor en Estado de Derecho y Gobernanza Global por la Universidad de Salamanca (ESP). Doctor en Jurisprudencia y Abogado de los tribunales y juzgado por la Universidad Central del Ecuador (ECU). Estudio derecho porque su objetivo es que la justicia brille en toda su extensión sobre todo cuando los derechos y garantías de las personas son violentados. Las obras más significativas son "La reparación integral a la víctima en el proceso penal" y "Derechos garantías y principios de los intervinientes en el proceso penal", entre los más importantes. Actualmente es docente investigador de la Universidad Central del Ecuador y dicta catedra de posgrados en la Universidad de Otavalo y Universidad Técnica de Ambato. ORCID: https://orcid.org/0000-0003-2771-1104.

[3] Licenciado en Ciencias Políticas y Sociales y Doctor en Jurisprudencia y Abogado de los Tribunales y Juzgados de la República del Ecuador por la Universidad Central del Ecuador, Especialista en Derecho Penal y Justicia Indígena, Magister en Derecho Penal y Criminología por la Universidad Regional Autónoma de los Andes, en el ámbito laboral ejerce como Abogado en libre ejercicio, además, en el ámbito judicial es Oficial Mayor de la Segunda Sala de lo Civil de la Corte Provincial de Justicia de Tungurahua, Juez del Tribunal Primero de Garantías Penales de Tungurahua, Presidente del Tribunal Primero de Garantías Penales de Tungurahua, Juez de la Unidad Multicompetente del cantón Pillaro, Juez del Tribunal de Garantías Penales con sede en el Cantón Ambato, profesor y expositor en universidades locales, formó parte del banco de elegibles para juez de Corte Provincial y Corte Nacional. ORCID: https://orcid.org/0000-0001-9980-9958.

con la intención de destruir y, en algunos casos, desprestigiar y chantajear a usuarios de medios electrónicos y de redes de Internet.

Palabras clave: almacenamiento de datos; delitos informáticos; normas jurídicas; riesgos informáticos; seguridad cibernética.

Cybercrime: Impunity organizational and its complexity in the business of the world

Abstract

The cyber-attacks are unlawful acts committed through the inappropriate use of technology, attacking the privacy of third-party information, damaging or extracting any type of data stored on servers or gadgets. The objective of the research is to determine the main types of cyber-attacks and the risks they generate for society, companies and governments. It is a mixed type research, supported by confirmatory studies and exploratory studies, highlighting theories and laws that are related to the study. The results of the investigation show the importance of determining the different types of cyber-attacks that exist. As well as, the recognition of the high points with respect to the security of the networks, to counteract their expansion. Finally, cyber-attacks represents any anti-legal action, via networks, with the intention of destroying and, in some cases, discrediting and blackmailing users of electronic media and Internet networks.

Keywords: Storing data, cyber-attacks, legal rules, cyber risks, cyber security.

1. Introducción

La importancia de determinar los diferentes tipos de delitos informáticos existentes, permite tener una herramienta de vanguardia en el ámbito de la seguridad informática, para enfrentar de manera efectiva, las consecuencias personales, económicas y sociales, al momento de ser víctimas de este acto delictivo (Escobar, 2017). Con referencia a lo anterior y, como usuarios diarios de este tipo de tecnología, es necesario conocer los riesgos que significa, el confiar información de primer nivel (personal, financiera, empresarial), a sitios o aplicaciones que pueden ser vulnerados, por profesionales de oficios (hacker, cracker, phracker y piratas informáticos), para convertir, a estos usuarios, en víctimas de fraude, extorción y chantaje.

El crimen informático, ha llegado a niveles organizacionales, de hecho Fernández (2013) destaca la importancia que reviste la complicidad interna, por intermedio del personal que labora en la misma, quienes sin importar los valores de respeto y lealtad, perjudican la vulnerabilidad de la información de la organización, volviéndose inclusive en algunos casos, en algo codiciado que, además, es muy bien remunerada por los delincuentes cibernéticos, que buscan el desprestigio o robo de información confidencial, con la intención de chantajear o liquidar las empresas.

Por intermedio de esta investigación, se determinan los tipos de delitos informáticos, para conocer las debilidades de las organizaciones en este sentido, y accionar una serie de controles necesarios para resguardar la información cibernética e ir combatiendo mediante claves, encriptaciones y niveles de seguridad todo lo concerniente al plagio de información.

También se analiza la impunidad desde el punto de vista legal y, sus consecuencias hacia terceras personas (implicados), que se ven involucradas en el hecho delictivo. Y finalmente las posibles correcciones necesarias, para resguardar la información, mediante la implementación de acciones en cuanto a la seguridad y poder contrarrestar este problema. El propósito, es salvaguardar su patrimonio y, conocer las vías legales para poder enfrentar los delictivos tomando en consideración, las Leyes y, recuperar el peculio y la identidad afectada.

Desde la perspectiva metodológica, se evidencia un diseño metodológico va en función a los resultados obtenidos producto de la misma investigación. Por intermedio del estudio confirmatorio, se toma en consideración el marco teórico, los resultados exploratorios y las Leyes y Normativas existente y necesarias para soportar el estudio. El método empleado es el mixto (cualitativo y cuantitativo), el cual es el adecuado debido a las variables e hipótesis recogidas durante la investigación, apoyándose al mismo tiempo, en estudios exploratorios cualitativos que sirvieron para confirmar patrones u opiniones comunes y concurrentes (Hernández-Sampieri y Mendoza, 2018).

Los insumos científicos que se utilizaron durante el desarrollo del artículo, fueron artículos indexados tomados de revistas científicas certificadas; Leyes y Normativas jurídicas que tienen relación directa con la investigación; comparaciones en países Latinoamericanos, donde el estudio ha arrojado resultados que aportan a la investigación; teorías, conceptos y discusiones de autores relacionados con el estudio, que permiten de manera hermenéutica aclarar todo lo relacionado con los ejes temáticos.

Ahora bien, dentro de los procesos esenciales para poder obtener de manera clasificada y efectiva la información, se toma en consideración lo siguiente1) Comparabilidad hermenéutica: importante para adentrarse científicamente en la investigación, tomando en consideración estudios que se relacionan entre sí, para evaluar resultados y adaptarlos con los obtenidos; 2) Observación directa: necesaria para apreciar el panorama actual desde el mismo lugar donde ocurren los hechos, permitiendo la presencia de la objetividad y la indagación del investigador; 3) Descripción: en combinación con la hermenéutica, permita la comprensión de los temas que deben ser analizados e interpretados, para poder entender las diferentes posiciones y fundamentaciones que se requieren para soportar la investigación; 4) Método cualitativo-cuantitativo: mide los datos recogidos referentes a los delitos informáticos, en cuanto a los tópicos que se relacionan, dando al mis tiempo, un estatus cualitativo tomando en cuenta los riesgos existentes en este tipo de delitos y, su impunidad ante los hechos.

Para la obtención de la información, se identificaron y analizaron los riesgos inherentes en los delitos informáticos, su importancia en cuanto al conocimiento de los tipos de delitos existentes y más utilizados en las organizaciones, así como la normativa legal en algunos países latinoamericanos. Se realizaron búsquedas en diferentes bases de datos (artículos científicos y en fuentes web confiables), permitiendo soportar los resultados y las

conclusiones del estudio.

2. Delitos informáticos: conceptos, prevención y riesgos

El uso de la informática a nivel mundial, ha tenido un repunte y una importancia relevante frente a la sociedad. El solo hecho de ofrecer servicios que permitan que los usuarios se les simplifiquen las cosas en un momento determinado, sobre todo para comunicarse e informarse, lo hace una herramienta útil y en muchos casos, necesaria (Márquez y Mousalli, 2016).

En efecto, expresa Trejo (2006) que resulta increíble la posibilidad de acceder a tanta información, tan diversa y tan pública, a la mano de cualquier usuario, en la historia de la humanidad. Hoy en día, existe una gran variedad de contenidos al respecto, tales como wikis, bibliotecas virtuales, chat, correo electrónico, videoconferencias, firmas electrónicas, foros, blogs, robótica, entre otros, que facilitan cualquier tipo de interacción masiva, sin tomar en consideración edad, género o nivel económico, que se apoyan en estos contenidos para entretenerse, socializar, buscar información desde la comodidad de la casa, oficina o cualquier ambiente donde exista la conexión (Márquez et al, 2016).

Ahora bien, hablar de delito es hablar de un estado criminal o ilegalidad de una acción, que compromete la integridad del otro (Tundidor, Nogueira y Medina, 2018). Bajo este contexto, el delito organizado se ha fortalecido a través de los años, debido a la misma evolución del sistema en general y, a la transnacionalización de sus redes delictivas. Son innumerables las actividades delictivas existentes, variando solamente según los entornos, localidades, oportunidades, entre otros, logrando expandirse a numerosos países. Según Torres, (2015) existe una fuerte tendencia a que los hechos delictivos se concentren hacia la parte empresarial, siendo este un blanco elegido por los antisociales, en muchos casos, por descuidos en cuanto al sistema de seguridad de las mismas organizaciones.

La modernización ha traído consigo, que el manejo de la información, se realice mediante procesadores informáticos, que permiten almacenar una cantidad considerable de información y, que, al mismo tiempo, se pueda acceder de manera rápida y efectiva a esos datos. La información puede ser de cualquier tipo (personal, empresarial, financiera-bancaria, societaria), siendo esta apetecida por los llamados delincuentes informáticos con la intención de sacar provechos de tipo oneroso, por intermedios del chantaje, desprestigio y hasta secuestro de la información sustraída.

Se vive una época, donde los cambios se presentan de manera vertiginosa. Al respecto explica España (2010), que en tiempos pasados se podía tener la seguridad que muy pocas personas o, casi nadie, podía acceder a información sobre nuestras vidas privadas por intermedio del Internet. Respecto a esto, destaca Riestra (2016), que la información de la informática se convirtió en la cotidianidad en la vida personal de algunos seres humanos. Esto ha producido que se convierta en una información muy bien cotizada. Esto sin duda alguna, hace crecer la amenaza de los mismos. Existen personas que se dedican exclusivamente a este tipo de delitos, con la intención de enriquecerse o, de generar cualquier revuele

noticiosos de un caso específico.

Tomando en consideración el tema central de la investigación, en la actualidad la informática es utilizada generalmente no solo como herramientas de apoyo, que tengan relación con las actividades del hombre, más bien se usa como un medio efectivo y eficaz para obtener y conseguir información (Oxman, 2013). De esto se desprende, que la misma se utiliza como medio persuasivo, en algunos casos, como nuevo medio de comunicación.

Cuando se habla de delito informático, Fuentes, Mazún y Cancino (2018) la definen como el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos. Es necesario aclarar, que este tipo de delitos suceden en el ciberespacio. En este mismo orden y dirección, Ruiz (1996), expresa una definición apegada a la Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014) donde expresa que el delito informático viene dado al comportamiento de manera ilegal que es contraria a la ética y, no es autorizada si divulgación y transmisión de datos de la red.

Es importante conocer que no existe un consenso en cuanto al término como tal, ya que también el delito informático puede ser conocido como delitos telemáticos, crímenes virtuales, cibercrímenes, ciberterrorismo, entre otros. Lo importante en todo esto, es conocer la manera de proteger y resguardarse de manera efectiva, sea de forma Legal o por intermedio de programas de seguridad interna, la información que se tiene en los servidores y en la red. El simple hecho de perder la privacidad en este sentido, aumenta notablemente el riesgo de un ataque cibernético, por intermedio de técnicas que permiten el acceso a la información.

A todas estas, ¿Cómo se podrían disminuir los riesgos, en el caso de estar expuestos ante estos delitos informáticos? En primer resulta interesante el conocer Leyes, Decretos y Regulaciones que buscan legalizar el uso de la información tecnológica. Un ejemplo de todo esto, se encuentra en Venezuela, donde las regulaciones en esta materia, permiten desarrollar habilidades y nuevos conocimientos, en cuanto al uso del Internet. Existe una política de Estado bajo el Decreto N° 825 (2000) el cual se refiere al acceso y uso de Internet en el territorio nacional. Así mismo, en la Constitución de la República Bolivariana de Venezuela (2009) en sus los artículos 108 y 110, expresa el uso de los servicios para ofrecer acceso universal en la búsqueda del conocimiento en la investigación científica, humanística y tecnológica.

En ese mismo sentido, en la Ley Orgánica de Educación (2009) y la Ley Orgánica de Telecomunicaciones (2000), se destacan las bondades y diferentes fases, para la utilización y para la formación de personal calificado para fortalecer el mercado de la enseñanza y modernización urbana. A pesar de lo anterior y sobre la base de las consideraciones mencionadas, los riesgos pueden provenir de cualquier fuente maligna, aplicaciones falsas, o virus, que se alojan de manera camuflada mediante fotos, juegos, entre otros, en el corazón de la información cibernética [servidor] (Perkel, 2010). Cabe agregar, que el simple crecimiento con relación a todas las formas de comunicación y de redes sociales existentes, y que cada día

aparecen en el mundo de la informática, también son causas de que aumente el riesgo de ser atacados en la Internet o Web (Cobb, 2009).

Con relación a los riesgos que condiciona a los delitos informáticos, los mismos provienen de combinaciones de situaciones y generalmente se conocen como atentados y amenazas a los sistemas de información. Entre los tipos de riesgos más conocidos se nombran: riesgos de integridad, riesgos de relación, riesgos de acceso, riesgos de utilidad, riesgos en la infraestructura, riesgos de seguridad general, concentración de procesamiento de aplicaciones más grandes y de mayor complejidad, dependencia en el personal clave y desaparición de los controles tradicionales. Todos cumplen roles según el tipo de delito que se cometa.

En definitiva, el delito informático es una forma de delinquir extrayendo información personal directamente del ciberespacio, el cual abarca el problema amenazando los entornos privados de la sociedad en general, además de adicionar posibles daños patrimoniales tanto personales como empresariales, producidos por el abuso de datos extraídos. Generalmente tiene carácter transfronterizo, que exige una respuesta adecuada y rápida y, por lo tanto, se necesita actualizar una debida adaptación de las Leyes según la naturaleza del delito y la seguridad adecuada para el resguardo de la información y la defensa del territorio cibernético.

3. Delitos Informáticos: Tipología

Podrían existir distintas definiciones acerca el tema de detallar o clasificar los tipos de delitos existentes en las redes. Sin embargo, Lara, Martínez y Viollier (2014), hacen una clasificación interesante (diagrama 1) para entender de manera más didáctica, los tipos de delitos informáticos.

- **El acceso no autorizado:** no se tiene acceso sin derecho a un sistema o a una red cualquiera, violándose todas las medidas de seguridad existentes. Generalmente son operadas por genios de la informática conocidos como Hackers.
- **El daño a los datos o programas informáticos:** es la eliminación o barrado total, descomposición, deterioro o erradicación de los datos o de los programas informáticos, sin que la persona ejecutante tenga derecho o acceso a realizar esa acción.
- **El sabotaje informático:** va direccionado a la alteración y eliminación total de datos o programas. Producen una interferencia, para bloquear los sistemas informáticos con la finalidad de obstruir el funcionamiento de las redes en su totalidad.
- **La interceptación no autorizada:** se refiere a la captación que se realiza sin autorización previa, tomando en consideración mecanismos tecnológicos tradicionales.
- **El espionaje informático:** es la adquisición, revelación y transferencia de información cibernética, de tipo confidencial, comercial; sin permiso o autorización del propietario de la información, con el propósito de causar pérdidas económicas o de obtener algún beneficio oneroso.

En una investigación realizada por Luna (2018), uno de los delitos de informática más utilizados por los

Diagrama 1
Tipos de Delitos Informáticos

Fuente: elaboración propia

ciberdelincuentes, es el espionaje informático. Explica el autor, que el mismo actúa como acechador, instigador y vigila de manera disimulada, a una persona clave para luego abordarla y obtener información sobre alguien o de una empresa o del gobierno. El espionaje industrial, ha cobrado mucho auge mediante la tecnología y, representa una buena plaza donde los cibercriminales pueden obtener mejores ganancias metálicas.

Sigue exponiendo Luna, que a pesar de la existen todavía de herramientas que se utilizan para aplicar el espionaje, tales como: tintas invisibles, micrófonos, grabadoras y micro cámaras, son las computadoras y sus aplicaciones, entre ellos los móviles, las herramientas más utilizadas actualmente para llevar a cabo este delito. Hay dos tipos de espionaje que sobresalen de los demás. Uno es el industrial y otro el informático.

El industrial es la obtiene de forma ilícita, información sobre la proyectos internos, investigación de mercados, desarrollos tecnológicos, con la intención de obtener ventaja, en este caso de su competidor, mientras que mediante el informático, se obtienen los datos personales (gustos, preferencias, intereses, proyecciones, etc.) del usuario por medio de internet y de las redes sociales, para ser utilizados en su contra y pedir rescates (chantaje), o desprestigiar al alguien.

Finalmente, Luna expone que de no tomar con seriedad el tema de la seguridad para proteger las informaciones, el espionaje informático ganará más terreno, aumento el riesgo de que las informaciones confidenciales

se filtren. Una vez que una persona, o una empresa en general entran al mundo de las redes sociales, o por lo menos navegue en el Internet, da la posibilidad de ser identificado y plagiado mediante este procedimiento. Se observa como a nivel organizacional, el tráfico de información se vuelve un problema axiológico, al momento de vender los datos a otros competidores o al gobierno. Nos encontramos a un clic, de perder nuestra identidad y nuestra visión de negocios, por culpa de la codicia, la deslealtad y la falta de valores éticos y morales.

4. Impunidad en la administración de justicia sobre los delitos informáticos

La impunidad es conocida como falta de castigo, así como impune es lo que queda sin castigo (Oliva y Escobedo, 2013). Para Le Clercq, Cháidez y Rodríguez (2016) la impunidad es la falta de castigo; no es más que la libertad que se le otorga a un delincuente para logra quedar absuelto de una pena que ha incurrido. Por lo tanto, se afirma que la impunidad es la causa más común en su ámbito. Generalmente es el accionar que más hiere la sensibilidad colectiva por no castigar a los verdaderos culpables de un hecho delictivo.

En algunos casos, recae en personalidades conocidos, que son perseguidos por razones políticas, siempre abusivas y propias de organismos del Estado, donde la libertad ha sido cercenada, la prensa en todas sus modalidades amordazada, los tribunales sesgados y el poder entregado en manos de una minoría sostenida por la coacción, el miedo y la cobardía general.

Respecto a la impunidad en la administración de justicia y su relación con los delitos informáticos, se dice que se encuentra en un estado de deterioro, producto de la falta de entendimiento por parte del legislador de que al ciberespacio, no le son aplicables las mismas reglas dadas para lo físico-territorial (Chinchón, 2014). Para Negronte (1995), existen leyes que se conciben para ciertos estratos sociales, es decir, pareciera que no aplica para todo el mundo, más bien para los menos fuertes y conocidos.

El delito informático, como se ha indicado en otros puntos anteriores, es un tipo de delincuencia producto de las nuevas tecnologías, el cual se da en diferentes campos de la vida diaria y muy especial en las organizaciones y corporaciones, el cual deben pagar cuantiosas cantidades de dinero para resguardar la información. Sin embargo, no se puede descuidar todos los vacíos jurídicos que surgen a través de estos temas, donde la integridad, ética e intelecto de una persona u organización empresarial se pueden ver afectados. Para Le Clerq (2015), dichos vacíos legales solo logran crear los conocidos y mal llamados «paraísos informáticos» o «cibernéticos», los cuales nacen cuando un ente específico aprovecha la deficiencia de una Normativa o Ley que sea relativa, en este caso, al delito de informática.

En relación con este último, Duva (2014) afirma que mediante Madrid (España) el 95% de los delitos que tienen relación directa con el ciberespacio, quedan impunes. La afirmación se apoya en los registros emitidos por el Ministerio del Interior de ese país, donde además destacan que este fenómeno conocido como cibercriminalidad tiene gran importancia nacional e internacional, ya

que no sólo representa una amenaza social y económica, sino que está llegando a gran parte de población poniendo en peligro lo personal, lo económicos y sobre todo sobre la infraestructura críticas.

Una vez más queda en evidencia que uno de los factores comunes encontrados en la investigación, el cual permite que sucedan este tipo de delitos, es la falta de seguridad en los datos cibernéticos, poniendo en riesgo de que ocurra el hecho. Esto ha traído la atención a nivel mundial, a tal punto que estas actividades cibercriminales han causado alarma en todos los Gobiernos y mercados del mundo, el cual han tomado en serio la importancia que reviste la data informática y sobre todo medidas de seguridad que permita contrarrestar el problema.

El esfuerzo mundial para prevenir y castigar este tipo de criminalidad, ha llevado a elaborar un convenio de cibercriminalidad, el cual fue suscrito en Budapest (Hungría) en 2001, y que España ratificó a partir del 1 de octubre de 2010. Dicho convenio destaca la necesidad de descubrir delitos tales como: el acceso ilícito a los sistemas informáticos, la interceptación de las redes comunicacionales, la producción y venta de dispositivos y programas que permitan la intrusión en un sistema, la alteración o borrado de datos, los fraudes por internet, el espionaje cibernético, y los ataques a la propiedad intelectual y a los derechos afines.

En definitiva, la impunidad de los delitos informáticos es una situación que se debe abordar desde los puntos de vistas legales, axiológicas y de seguridad. Las organizaciones, han tenido ciertos problemas acerca de la seguridad de su base de datos, el cual los coloca en una situación no privilegiada para salvaguardar su data. Por supuesto como se ha indicado, esto favorece en cierta forma, el aumento de la cibercriminalidad, pues el delincuente se apoya en esa falencia, para cometer el delito. Darle relevancia a cumplir con las normas y parámetros legales, permitirá en cierta forma, respaldar a todos aquellos que se encuentran desprotegidos de esta situación.

5. Delitos informáticos en las empresas: discusión

Como se indicó anteriormente, uno de los delitos informáticos más recurrente, es el espionaje informático, ya sea con programas específicos, con datos de salida (Loredo, 2013). Este delito es uno de los más siniestrados y privilegiados para los que cometen su extracción. A raíz de este interesante delito, se desprenden una serie sucesivas de acciones, tales como, robo de identidad y de fondos bancarios, que atentan con la integridad de la sociedad, dándole paso a extracción de información, borrado de archivos, espionaje industrial, entre otros.

Otro de los delitos más cometidos en las empresas son los sabotajes informáticos (Hernández, 2009). Estos se hacen mediante la interrupción de las líneas telefónicas, conjuntamente con el suministro de electricidad. Todo se hace de forma intencional mediante programas de tipo fraudulentos. Ahora bien, también existen los llamados virus, que forman parte de una larga lista de delitos informáticos y suelen ser muy habituales. Estos virus son programas que se crean y se incrustan en los procesadores, para infectar cualquier archivo documentación o sistema informático de seguridad (Zambrano-Mendieta, Dueñas-Zambrano y Macías-

Ordoñez, 2016).

Otra forma de penetrar en el mundo de los delitos informáticos, es mediante la implantación de los virus, siendo los gusanaos los más famosos en estos casos (Temperine, 2013). Estos virus se infiltran en programas originales, con la intención de modificar, destruir y borrar información. Los datos infectados son eliminados en su totalidad afectando todos los procesos internos y externos de las organizaciones. Para poder infiltrar estos virus, las organizaciones se enfrentan a piratas informáticos conocidos como hackers o crackers quienes suelen tener la capacidad y los conocimientos para adentrarse en los sistemas.

Estos piratas de la informática, hacen sus delitos con el **único** objetivo de obtener una recompensa económica, sin medir las consecuencias que se puedan presentar (Quiroga, 2018). Como una forma de incentivarse, los piratas realizan estos delitos como nuevos desafíos personales y para evaluar sus conocimientos frente a otros. Lo que buscan es fama y reputación a expensas de cualquier declive financiero que puedan ocasionar. La ideal del desafío es entrar en un sistema prohibido y ver hasta donde se puede llegar.

Con el auge que han tenido estos piratas de la informática, las organizaciones se han visto en la necesidad de blindar sus sistemas, creando inclusive departamentos de peritos informáticos de auditoría, que son prácticamente unos informáticos forenses, que ayudan a combatir o burlar este tipo de situaciones donde la empresa salga perjudicada (López, 2007).

Por ejemplo, existen empresas de producen programas y aplicaciones que ven como a partir de sus propios programas, sin la debida autorización o sesión de derechos de autor **«**patente**»** son plagiados y clonados sus productos. Cada día este tipo de delitos crecen, inclusive algunas empresas deben acudir a procesos legales para ver la posibilidad de hacer cumplir la ley y poder recuperar daños onerosos que pudieron haberse causado a raíz de este tipo de delitos informáticos.

Definitivamente cada año, estas organizaciones sucumben ante esta problemática, perdiendo su patrimonio. En este conjunto de delitos hay algunos que causan un mayor impacto en la economía de las organizaciones (L**ópez,** 2013). Existen delitos que resultan complicados detectarlos, ya que posiblemente tengan cómplices claves dentro de la organización que no permite que se descubran con facilidad. Lo cierto es que la imagen de la organización se puede ver empaña por situaciones de delitos de informáticos presentados.

Existen delitos informáticos que son complicados detectarlos, generalmente existe complicidad dentro de la misma organización, es decir, que son situaciones producidas por las personas que trabajan en las mismas empresas (Estrada, 2008). Por ejemplo, el sabotaje es uno de ellos, donde algunos empleados, sobre todo aquellos, cuyas conductas dejan mucho que desear, intentan no solo sabotear a su compañía, sino a su compañero de al lado.

Entonces, tratando de destruir la reputación del compañero, al mismo tiempo daña cualquier proceso dentro de la organización. La competencia desleal de ciertos empleados y la ceguera por ser más competitivos hace que pudieran cometer un delito informático que termina perjudicando totalmente a la empresa. Por eso la recomendación de que los

sistemas contengan contraseñas de seguridad sea para destruir o modificar cualquier tipo de data y que quede registrado su trayectoria para poder detectar los responsables del hecho (Azaola, 2010).

De esto parte la importancia de los peritos informáticos, dentro de la organización, y poder descubrir la mano negra que está haciendo todo y así resolver el conflicto, que se había planteado. Aunque esto parezca cosa de inmadurez, algunos trabajadores creen que sus lugares de trabajos son parques infantiles. En lugar de ponerse a trabajar en proyectos productivos, pierden su tiempo dedicándole gran parte del mismo a destruir el trabajo de otros y, por ende, a la empresa.

Hay que destacar que con relación a los delitos informáticos muchas empresas son víctimas sin darse cuenta (García, 2015). Cuando logran detectar la irregularidad o fraude, ya es demasiado tarde. Por todo esto las organizaciones se ven en la necesidad de tener procesos de auditorías para soportar las pruebas e ir a procesos judiciales para exigir una indemnización por el perjuicio recibido.

La realización de auditorías temporales logra la prevención de problemas futuros (Gervilla 2014). Se han escuchado casos donde la inclusión de dispositivos de audio, por ejemplo, en una reunión de alto nivel, puede permitir que la competencia se adelante a ciertos proyectos y los mismos sean robados y puesto en marcha primero que sus verdaderos creadores. Los delitos informáticos que se dan más en las empresas y compañías hacen que cada año, pierden mucho dinero.

No obstante, la imagen de dicha corporación queda evidentemente dañada. Mostrándola como nada profesional y vulnerable ante cualquier incidente que pase. Esta brecha de seguridad no es más que hundir todo el trabajo realizado. La importancia de poder controlar y prevenir estos ataques es lo primordial a la hora de seguir adelante. Con profesionales que sepan y puedan solventar estas injerencias, harán que las empresas salgan adelante.

Al discutir los resultados, se describen los tipos de delitos informáticos analizados, tomando en consideración, Leyes y normativas existentes para encontrar similitudes y diferencias entre cada una de ellas, y así se analiza como los afectados enfrentan la lucha contra los delitos informáticos. Luego un estudio de las causas que producen la aparición de delitos informáticos, describiendo las debilidades ante este flagelo. En el cuadro 1, se presentan los tipos de delitos informáticos en conjunto con sus infractores, recomendaciones y riesgos implícitos que se conjugan al momento de realizar la ciberdelincuencia.

Los delitos informáticos se están haciendo muy comunes en la actualidad; los delincuentes encuentran debilidades que las mismas personal u organizaciones (privadas y públicas) muestran, para activar de manera efectiva una red de actividades ilícitas, para incurrir en hurtos, estafas o interferencias por medio de las redes hacia terceros o cualquier entidad.

El cuadro 1, detalla de manera específica los diferentes tipos de delitos informáticos y los infractores que intervienen en la misma. Por lo tanto, se afirma que, según el tipo de delito, también existe un especialista en esa área que hace posible, que se activen los riesgos inherentes, llevando a cabo su acto ilícito.

Este es uno de los principales

Cuadro 1
Tipos, infractores, recomendaciones y riesgos de delitos informáticos

DELITOS	INFRACTORES	RECOMENDACIONES	RIESGOS
Acceso no autorizado	Hacker/Cracker	▪ Utilizar contraseñas seguras. ▪ Mantener como política auditoría de accesos y niveles de seguridad en los usuarios.	Riesgo de acceso
El daño a los datos o programas informáticos	Phracker	▪ Poner especial atención en el tratamiento de correos electrónicos. ▪ Tener una política en cuanto a la inserción de dispositivos (flash, cd…). ▪ Disponer de un programa que respalda la data diariamente.	Riesgo en la infraestructura
El sabotaje informático	Piratas informáticos	▪ Navegar por páginas web seguras y confiables. ▪ Instalar Antivirus.	Riesgo de seguridad general
La intercepción no autorizada	Hacker	▪ Utilizar firewall. ▪ Instalar indicadores de usuarios no autorizados.	Riesgo de desaparición de los controles tradicionales
El espionaje informático	Cracker/Piratas informáticos	▪ Actualizar regularmente el sistema operativo. ▪ Ser cuidadoso al utilizar programas de acceso remoto. ▪ El manejo de la data debe estar custodiada por personal de confianza.	Riesgo de dependencia en el personal clave. Riesgo de utilidad.

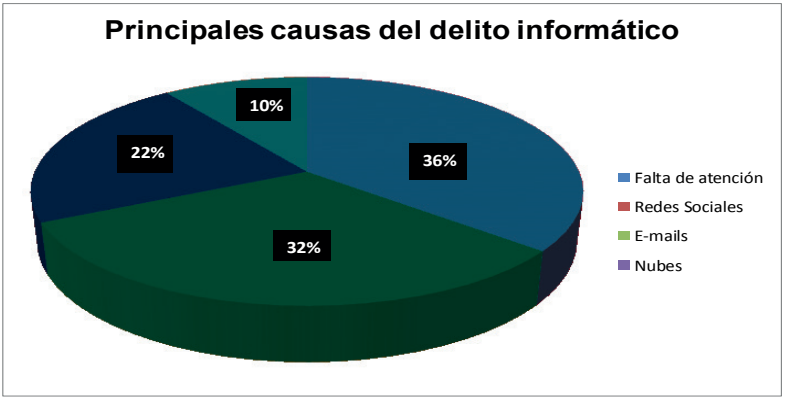
Fuente: Elaboración propia

motivos por los que se han llegado a diseñar innumerables mecanismos de recomendaciones y prevención, con la intención de contrarrestar este tipo de actividades, de forma tal, que todo afectado active políticas ante actividades que resulten sospechosas. Cuando se detalla a fondo la información, se crea la necesidad de que los afectados implanten controles en todas las actividades que se realicen. Sobre las empresas que manejan personal, no solamente para salvaguardar lo que existen, también para escoger a los empleados en cuanto a la documentación que ingresa y referencias de trabajos anteriores, correos electrónicos y en el uso de las redes sociales. Un elemento importante a tomar en cuenta, es la seguridad de las organizaciones en cuanto a los usuarios y password, a fin de evitar cualquier tipo de interferencia y uso no autorizado de información que es considerada confidencial.

Otro punto interesante que resaltar, es lo referente a las principales causas del delito informático (gráfico 1), donde se observan las más empleadas (falta de atención, redes sociales, E-mails y nubes de información), que en la mayoría de los casos son las ventanas abiertas que los usuarios, de manera irresponsables permiten para que los infractores puedan cometer el delito. El desconocimiento es el factor preponderante de todo esto, ya que por

el simple hecho de que el uso de redes es muy, permite a los ciberdelincuentes buscar y obtener la forma de emplear sus capacidades y conocimientos para cometer los delitos.

Gráfico 1
Principales causas del delito informático



Fuente: Elaboración propia

La falta de atención (descuido) y las redes sociales, resultan las causas más notorias en cuanto a la activación de los delitos informáticos. Por algún motivo, ambas se encuentran interconectadas con el tipo de delito más empleado como lo es, el espionaje informático. En algunas ocasiones, el factor común que se presenta en estas ocasiones es la confianza depositada en una persona, y la misma no es capaz de mantener ese sentido de lealtad que se necesita para que la información no salga a la luz pública y mucho menos, que sea empleada como medida de extorción, chantaje e información industrial clasificada.

La seguridad cibernética es primordial para proteger y salvaguardar esa información. Hacer una política de resguardo de la data es un mecanismo de defensa que sirve para enfrentar esta problemática, así como programas internos de auditoria de sistemas, que permitan informar a la hora de cualquier irregularidad poco inusual, respecto a la entrada de datos externos o violaciones de seguridad por parte de cualquier usuario de la red.

En relación a la figura 2, el cual tiene que ver con algunas Leyes que existen en algunos países latinoamericanos, lo más resaltante es que todos, a pesar de tener diferentes aristas, buscan sancionar, evitar y procesar este tipo de actos ilícitos. Por ejemplo, en Venezuela el decreto Nro. 825, es considerada una de las más completas en este ámbito

de delitos informáticos. Sin embargo, al igual que las demás, su finalidad jurídica es proporcionar seguridad, resguardo a los posibles afectados y pena a los infractores de la misma. Por otro lado, Colombia en su Ley de Protección de la información y de los datos, también se enfoca hacia la penalización sobre estos actos vandálicos cibernéticos, priorizando la proyección de los datos e información personal.

En el caso del Perú, el objetivo primordial es la prevención y las sanciones a los que infringen dicha Ley. Algo interesante que resaltar en Perú, es que el organismo encargado de hacer valer esta Ley, se apoya en su totalidad en programas cibernéticos, es decir, aplican de una vez las recomendaciones para disminuir los riesgos y demostrar que una de las mejores armas en este sentido, es la prevención y la seguridad. Finalmente, Costa Rica, que al igual a las anteriores la Ley va prácticamente direccionada a hacer valer el derecho de resguardo y fidelidad de la información cibernética, en contra de aquellos infractores que de manera inescrupulosa atentan contra los usuarios de ducha información.

Tabla 2
Leyes, Decretos y Normativas en Latinoamérica

LEYES/NORMATIVAS/DECRETOS	PAÍS	DESCRIPCIÓN
Decreto N°825 May/2000: Acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político.	República Bolivariana de Venezuela.	Ofrece definiciones y conceptos ante delitos informáticos, es una de las Leyes más completas y complejas. El resguardo de la identidad y de la información es la prioridad que proporciona esta Ley.
Ley N° 1273 Ene/2009: Protección de la información y de los datos.	República de Colombia.	La Ley se creó para penar las acciones relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión y multas en general, según la gravedad del hecho.
Ley N° 30096 Oct/2013: Delitos informáticos.	República del Perú.	El objetivo es prevenir y sancionar conductas ilícitas que afectan los datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.
Ley N° 8148 Oct/2001: Delitos informáticos.	Costa Rica.	Se creó leyes para tipificar violaciones cibernéticas. Privativa de libertad para los infractores, sin clasificar el tipo de delito y su uso ilícito.

Fuente: Elaboración propia

Todos los países necesitan concientizar a los usuarios de la información cibernética, al buen uso y resguardo de la data. De esta forma se disminuirán los riesgos que representa el simple de hecho de ser víctima de una situación irregular como el delito informático. Hay que tomar en serio, las consecuencias que esto conlleva, no solo a nivel personal ni económico, sino en el desempeño mismo de la sociedad que es altamente vulnerable a golpes delictivos en el ciberespacio, debido a las debilidades y en muchos

casos descuidos, en sus sistemas de seguridad y la falta de accionantes para contraatacar a este tipo de delincuencia.

6. Conclusiones

Los delitos informáticos representan un acto ilícito existente en las redes de información (web), que atenta contra la propiedad privada intelectual de la sociedad, las organizaciones y el Estado en general. Cada día se observa, como los delitos informáticos van en ascenso, y parte del mismo, se debe en muchos casos, al descuido en cuanto a la protección de la data por parte de los usuarios. De esta forma, los delincuentes cibernéticos encuentran oportunidades para extraer información que atenta con la integridad y con la estabilidad organizacional de los dueños de la información.

La cautela, el escepticismo y la prevención, deben ser los elementos que permitan a los propietarios de la información, a resguardar la misma. Más aún cuando se trata de data que pueda dañar de manera directa, una identidad o una organización. La contratación de expertos en seguridad cibernética, no debe ser vista como un gasto agregado, más bien, es un valor intangible que necesaria para salvaguardar la información, ante la cantidad de ciberdelincuentes que bordean la web, donde su única intención es perjudicar a terceros y enriquecerse de manera ilícita, apoyados en muchos casos por el descuida, la confianza en cuanto al manejo de la data.

Respecto a la información con los países investigados, a pesar de los esfuerzos por parte de legisladores para abarcar todos los puntos relacionados a este tema de delitos informáticos, aún persisten algunos vacíos legales que son buenos abordar. Delitos como la piratería, propagación de la pornografía infantil y el desvío desproporcionado de la data a nivel general, hacen que los infractores cibernéticos, vayan ocupando un espacio importante para delinquir. Los delitos informáticos no se pueden eliminar de manera perentoria, pero si se puede ir accionando de manera efectiva, las Leyes actuales, inclusive apoyados en la misma tecnología, para poder combatir estos actos ilícitos en la web. Los elementos legales que se están presentando hoy en día, no son relevantes ni suficientes para atribuirles responsabilidades judiciales directas a los infractores.

Cada día los delitos informáticos van tomando auge en todos los niveles cibernéticos. Los infractores crean y activan diferentes modalidades que les permitan delinquir tales como, el hurto, estafas, chantajes, entre otros, perjudicando de manera fehaciente la privacidad e identidad de cualquier persona o entidad. La necesidad de instaurar sistema de seguridad, que permita el resguardo de la información, cada día toma más relevancia, sobre toda cuando la información que se maneja es de primera línea.

Referencias bibliográficas

Azaola, L. (2010), *Delitos informáticos y Derecho Penal*. México: Editorial UBIJUS.

Cobb, M. (2009), Risk of social networking: preparing for e-discovery issues, threats". **Search Security**. Recuperado de http://search security.techtarget. co.uk/tip/0, 289483,sid180_gci1366092,00.html . Fecha de consulta: 26 de Agosto de 2009

Constitución de la República Bolivariana

de Venezuela (2009), Gaceta Oficial No. 5.453. Venezuela.

Chinchón, Á. (2014), Impunidad, sistema de justicia, estado de Derecho y democracia. **¿Es peor la inmunidad que el crimen en sí mismo. Revista del Centro de Investigación y Estudios Judiciales**. Año 20/2014, Nro. 22, pp 18-22.

Duva, J. (04 de mayo de 2014). El 95% de los ciberdelitos cometidos quedan impunes. *El País*. Recuperado de https://elpais.com/politica/2014/05/03/actualidad/1399117342_852720.html

Escobar, A. (2017). Delitos informáticos. Seguridad de la información y criptografía. **UANL-Facultad de Ingeniería Mecánica y Eléctrica***, 15*(1), 1-6.

España, C. (2010), TIC: seguridad e Internet en la Educación. Recuperado de Internet: http://www.eumed.net/libros/2011d/1051/index.htm Consultado 10-12-2018.

Estrada, M. (2008), Delitos informáticos. Recuperado de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf 05-12-2018.

Fernández, J. (2012). Internet y seguridad: los nuevos retos de un mundo globalizado. *Paakat:* **Revista de Tecnología y Sociedad**. *Año 2*(3), 1-8.

Fuentes, T.; Mazún, Rodrigo y Cancino, G. (2018), Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. **Revista Advance in Engineering and Innovation [AEI]**, Año 2, No.4, Yucatán, México, pp 1-8.

García, J. (2015), Informe sobre el peritaje informático. [Trabajo de Maestría] Universidad Carlos III de Madrid.

Gervilla, C. (2014), Metodología para una Análisis Forense. [Trabajo de Maestría] Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC).

Hernández, L. (2009), El delito informático. **Revista Eguzkilore**. Cuaderno del Instituto vasco de criminología. Año V, Nro. 23, pp 227-243.

Hernández-Sampieri, R. y Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. México: McGrawHill Education.

Lara, J.; Martínez, M. y Viollier, P. (2014), Hacia una regulación de los delitos informáticos basada en la evidencia. **Revista Chilena de Derecho y Tecnología**, Año 3, No. 1, pp 101-137.

Le Clercq, J. (2015), Crisis de impunidad en México". **Revista Bien Común**. Año 33, Nro. 2, pp 35-41.

Le Clercq, J.; Cháidez, A. y Rodríguez, G. (2016), Midiendo la impunidad en América Latina: Retos conceptuales y metodológicos. **Revista de Ciencias Sociales**, Facultad Latinoamericana de Ciencias Sociales-Sede Académica de ecuador, Año 1, No. 55, pp 69-91.

López, M. (2007), Análisis Forense Digital. Universidad Nacional de Educación a Distancia. Recuperado de http://www.gnu.org/copyleft/fdl.html.

López, R. (2013), Delitos informáticos, ciberterrorismo, terrorismo y delincuencia organizada. Recuperado de https://haddensecurity.wordpress.com/2013/06/17/delitos-informaticos-iberterrorismo-

terrorismoy-delincuencia-organizada/amp/ 05-12-2018.

Loredo, J. (2013), Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo. **Revista Celerinet**, Año 3, Nro. 2, pp 44-51.

Luna, V. (2018). Espionaje informático, robo de identidad e información. *Quanti Solutions, 2*(1), 6-14. Recuperado de https://www.quanti.com.mx/2018/03/05/ espionaje-informatico-robo-identidad-e-informacion/

Márquez, N. y Mousalli, G. (2016), Internet, usos y riesgos. **Revista Teuken BidiKay**, Año 9, No. 12, Medellín, Colombia, pp 177-191.

Negronte, N. (1995), *El mundo digital*. Barcelona, España: Ediciones BSA.

Perkel, J. (28 de abril de 2010). Cybersecurity: how safe are your data? Nature. Recuperado de http://www.nature.com/news/2010/100428/full/46412 60a.html

Oliva, J. y Escobedo, A. (2013), *El concepto impunidad, su abordaje en los instrumentos del Derecho Internacional de los Derechos Humanos, Derecho Internacional Humanitario y Derecho Penal Internacional*. [Trabajo de Maestría] Universidad Carlos III de Madrid.

Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014), Recomendación del Consejo de la OCDE relativa a la Cooperación Internacional en el marco de investigaciones y procedimientos en materia de competencia. Aprobada por el Consejo el 16 de septiembre de 2014, México.

Oxman, N. (2013), Estafas informáticas a través de Internet: acerca de la imputación penal del phishing y el pharming, *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, Año 1, No. 41, pp 211-262.

Quiroga, A. (2018), La seguridad informática: Un negocio en auge. El clarín 10/06/2018, Piedras, Argentina.

República Bolivariana de Venezuela (2009), Asamblea Nacional, Ley Orgánica de educación, Gaceta Oficial N° 5.929 de 2009. Caracas, art. 3, 4

República Bolivariana de Venezuela (2000), Asamblea Nacional, Ley Orgánica de Telecomunicaciones, Gaceta Oficial N° 36.920. Caracas, art. 5, 12

República Bolivariana de Venezuela (2000), Gaceta Oficial No. 36.955, Decreto 825. Art 1,5,8, Caracas, Venezuela.

Riestra, E. (2016), Derecho a la intimidad y a la informática. ***Revista Lus et Praxis***, Año 11, No. 26, pp 69-76.

Ruiz, E. (1996), Responsabilidad penal en materia de informática: **Revista Informática y Derecho Año 9. No. 10 y 11**, UNED, Centro Regional de Extremadura, Mérida, pp 25-36.

Temperine, M. (2013), Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Recuperado de http://conaiisi.unsl.edu.ar/ 2013/82-553-1-DR.pdf 21-09-2016

Torres, D. (2015), La información y la comunicación del riesgo de origen tecnológico en la empresa Puerto Moa. **Revista Ciencia y Futuro**, Año 5, No. 1, pp 104-122.

Trejo, R. (2006). Viviendo en el Aleph. La sociedad de la información y sus laberintos. España: Gedisa.

Tundidor, L.; Dianelys, N. y Medina, A. (2018), Organización de los sistemas informáticos para potenciar en control de la gestión empresarial. **Revista Cofín Habana**, Año 13, No. 1, Universidad de Matanzas, Cuba, pp 88-110.

Zambrano-Mendieta, J.; Dueñas-Zambrano, K. y Macías-Ordoñez, L. (2016), Delito informático: Procedimiento penal en el Ecuador. **Revista Científica Dominio de las Ciencias**, Año 2, Nro. esp., ago, pp 204-215.