ISSN. 1690-074X
DEPOSITO LEGAL pp.2002-02ZU1289
REVENCYT RVF007
INDIZADA EN :
CATALOGO LATINDEX
CLASE
BASE DE DATOS REDECONOMIA
DIALNET

UNIVERSIDAD DEL ZULIA
NUCLEO COL
GRUPO DE INVESTIGACIÓN DESARROLLO GERENCIAL
REVISTA ARBITRADA FORMACIÓN GERENCIAL

REVISTA DE GERENCIA EN ÁREAS ECONÓMICAS HUMANÍSTICAS Y TÉCNICAS

REVISTA ARBITRADA FORMACIÓN GERENCIAL

AÑO 21, No.1
Mayo 2022

Formación Gerencial, Año 21. Nº 1, mayo 2022
ISSN 1690-074X

DELITOS INFORMÁTICOS COMUNES EN LAS PYMES DEL MUNICIPIO CABIMAS

Alfredo Díaz Pérez* Youmory Martínez Quiroz ** Franklin Gómez Bejarano***

Recibido: Febrero 2022 Aprobado: Abril 2022

RESUMEN

La presente investigación tuvo como propósito, describir los delitos informáticos comunes en las pequeñas y medianas empresas (Pymes) del Municipio Cabimas, del Estado Zulia. Se fundamentó teóricamente en los postulados de Fernández (2022), Gómez (2018), Loredo y Ramírez (2013), entre otros. La investigación fue descriptiva con diseño de campo, no experimental, transeccional. La población y muestra estuvo conformada por veinticinco (25) directores y jefes de informática de las PyMES de Cabimas. Se utilizó una encuesta en su modalidad cuestionario, con quince (15) reactivos y escala tipo Líkert con cinco (05) alternativas de respuesta. Se recurrió a la estadística descriptiva, obteniendo como resultado que la estafa, suplantación de información, robo o fuga de datos, delitos contra la propiedad intelectual y extorsión sexual, estuvieron presentes en el contexto estudiado.

Palabras clave: Delitos informáticos, PyMES, Cabimas.

* Ingeniero en Informática (URBE, 2005), M. Sc. En Gerencia de Recursos Humanos (URBE, 2008), Doctor en Ciencias de la Educación (URBE, 2018), Postdoctorado en Gerencia para la Educación Superior (URBE, 2019), Desarrollador de software, Docente adscrito al Departamento de Ciencias Formales de la Universidad del Zulia, Núcleo COL. Tutor y jurado de Trabajos de Grado y Tesis Doctorales. E-mail: alfredojosediazperez@gmail.com. Orcid: https://orcid.org/0000-0002-2091-2176

** Estudiante del Programa Humanidades y Educación, Universidad del Zulia, Núcleo Costa Oriental del Lago. E-mail: youmory1996@gmail.com

*** Ingeniero en Computación (UNIOJEDA), Licenciado en Educación, mención Matemática y Física (UNERMB), M. Sc. En Docencia para la Educación Superior (UNERMB). Docente con más de 15 años de experiencia en Educación Básica, Diversificada y Universitaria, Tutor Académico y Metodológico, Especialista en Investigación Educativa. E-mail: franklingomez25@gmail.com

COMMON COMPUTER CRIMES IN SMEs IN THE CABIMAS MUNICIPALITY

ABSTRACT

The purpose of this investigation was to describe common computer crimes in small and medium-sized enterprises (SMEs) of the Cabimas Municipality, Zulia State. It was theoretically based on the postulates of Fernández (2022), Gómez (2018), Loredo and Ramírez (2013), among others. The research was descriptive with a field design, not experimental, transectional. The population and sample consisted of twenty-five (25) IT directors and heads of the SMEs of Cabimas. A survey was used in its questionnaire modality, with fifteen (15) reagents and a Likert-type scale with five (05) response alternatives. Descriptive statistics were used, obtaining as a result that fraud, information supplanting, data theft or leakage, crimes against intellectual property and sexual extortion were present in the studied context.

Keywords: Computer crimes, SME, Cabimas

INTRODUCCIÓN

En los últimos años, el surgimiento de los servicios vinculados a las redes informáticas, han derivado en un conjunto de beneficios de toda índole, los cuales abarcan desde la realización de transacciones bancarias desde el hogar o trabajo, la educación en línea, geolocalización de personas o bienes, compra de artículos a través de tiendas virtuales, comunicarse a través de aplicativos a otras partes del mundo, entre otros.

A partir de lo anterior, ha cobrado auge un concepto emergente, que ha estado presente desde la aparición de las computadoras: La seguridad informática, la cual, es una disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información. Esta protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. (ISOTools Excellence, 2017). En ese propósito, se trata de implementar medidas técnicas con el fin de preservar las infraestructuras de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por ella.

Como complemento a lo anterior, las empresas deben procurar el uso de estrategias dirigidas a proteger sus activos de información, ya que de ellos depende la continuidad operativa de sus procesos. Así mismo, los delitos informáticos son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades (Verney, 2013). De la mano con la globalización, la creación del denominado ciberespacio ha traído consigo de forma paralela, nuevas formas de presentación del delito, que desbordan la territorialidad de los ordenamientos jurídicos (Díaz, 2010).

A la luz de las ideas expuestas anteriormente, se considera un delito informático a toda acción ilícita realizada a través de un computador o dispositivo electrónico por parte de una persona u organización y a través de la cual, se busque vulnerar o violentar la seguridad, obtener beneficios de manera fraudulenta o desencadenar comportamientos inesperados en los sistemas informáticos.

Cabe destacar que, en el mundo, han surgido casos donde los delitos informáticos son frecuentes. En ese sentido, y de acuerdo a lo reportado por la fiscalía general del Estado, en España tuvieron lugar en 2020 más de 16.900 procedimientos judiciales por ciberdelincuencia, un valor que representa un incremento de un 28,69% con respecto a 2019. (Fernández, 2022). De ellos, la mayor parte correspondió a delitos contra el patrimonio o contra la libertad.

Sobre la base de las consideraciones anteriores, en España, se ha incrementado la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas; garantizar y fortalecer la seguridad de los sistemas de información, redes e infraestructuras críticas; potenciar las capacidades para investigar y perseguir las actividades terroristas; e intensificar la colaboración internacional (Consejo de Seguridad Nacional 2013). Sin embargo, siempre existe el factor de riesgo, pues, ante las acciones preventivas, se generan nuevas ofensivas, por lo cual, se requiere crear una cultura de seguridad informática para que las personas estén atentas ante

cualquier comportamiento inusual en los sistemas, aplicaciones o recurso tecnológico utilizado como parte de sus actividades cotidianas.

Ahora bien, en el caso de Latinoamérica, los delitos informáticos más comunes, son el abuso de dispositivos, falsedad informática, fraude o estafa electrónica, interceptación ilícita, atentados contra la integridad de los sistemas, acceso ilícito a los recursos de información, pornografía infantil y atentados contra la seguridad de los datos (Temperini, 2014). En tal sentido, es prioritario que los países adopten decisiones políticas serias a mediano o largo plazo que permitan mejorar los niveles de coordinación, armonización y actualización normativa a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia. Por otro lado, se destaca la necesidad de adopción de decisiones que destinen recursos necesarios para gestionar una estructura adecuada para la detección, investigación, persecución eficaz de los delitos informáticos.

Por otra parte, en Venezuela, existe la Ley Especial contra los Delitos Informáticos (2001), la cual, tiene como objetivo, la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías.

En efecto, al realizar una observación preliminar en algunas Pequeñas y Medianas empresas de la Ciudad de Cabimas, del Estado Zulia, se ha percibido que, en cierta medida, han sido objeto de distintos delitos informáticos, los cuales se relacionan con la suplantación de identidades, el phishing, el espionaje electrónico, la intercepción de correos electrónicos con información sensible y el hackeo de sistemas o software. Esto representa una problemática que debe ser atacada desde la propia conciencia de los ciudadanos, pues, el uso de servicios en la web, el acceso a recursos electrónicos en los distintos roles que desempeñan en la sociedad, reviste un riesgo tácito por el uso de datos sensibles tales como nombres de usuario, contraseñas, datos personales, entre otros.

A la luz de las consideraciones anteriores, surge la necesidad de estudiar los delitos informáticos más frecuentes tanto en el ámbito personal como empresarial, por lo cual, se llevó a cabo la presente investigación cuyo objetivo fue describir los delitos informáticos comunes en las pequeñas y medianas empresas (Pymes) del Municipio Cabimas, del Estado Zulia.

FUNDAMENTACIÓN TEÓRICA

Delitos Informáticos

Los delitos Informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal que hacen uso indebido de cualquier medio informático. Este comprende actividades criminales que en un primer momento se han tratado de encuadrar en las figuras típicas de carácter tradicionales robo, fraudes, estafa, sabotaje, entre otras (Verney, 2013).

Por otra parte, Loredo y Ramírez (2013), indican que el delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma

activa dispositivos habitualmente utilizados en las actividades informáticas.

A los efectos del presente estudio, se consideran los delitos informáticos como el conjunto de actitudes, acciones u operaciones ilícitas, realizadas a través del computador o medios electrónicos con el fin de obtener beneficios de cualquier índole, prioritariamente económicos, aunque también puede ser materiales, o intangibles, como la información relacionada a un proyecto, producto, servicio o similar.

Tipos de Delitos Informáticos

De acuerdo al criterio de Rivas (2021), los delitos informáticos más comunes, son la estafa, suplantación de identidad o phishing, fuga de datos, delitos contra la propiedad intelectual y sextorsión. Así mismo, la Ley Especial contra los Delitos Informáticos (2001), vigente en Venezuela, establece un conjunto de delitos que abarcan desde acceso indebido, sabotaje o daño a sistemas, espionaje informático, falsificación de documentos, hurto, fraude, entre otros. A continuación, se describen los delios considerados por Rivas (2021) como frecuentes o comunes entre los usuarios.

Estafa

La estafa, en palabras de Rivas (2021), se comete usualmente mediante la suplantación de identidad. Los ciberdelincuentes aprovechan sus conocimientos informáticos para engañar a las personas para robarles los usuarios, contraseñas y sus datos personales. Este delito informático se realiza mediante spam, software ilegal o, lo más común, sitios web falsos que imitan de forma casi perfecta a las originales.

El vínculo entre el fraude informático y la estafa, según lo afirman Mayer y Oliver (2020), es bastante evidente, al punto que los ordenamientos jurídicos en distintos países, los regulan de manera sucesiva o conjunta, pues parten de la base de que ambos afectan intereses patrimoniales ajenos, sólo que a través de distintos medios. Así mismo, se puede precisar un nexo entre el fraude y el sabotaje informático, ya que el primero por lo general se asocia con la alteración de datos, mientras que el segundo con su destrucción. En cualquier caso, se puede manejar como una estafa.

Como complemento a lo anterior, la Ley Especial contra los Delitos Informáticos (2001), establece en su Artículo 14 que el todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Sobre la base de las ideas expuestas, se considera la estafa como un delito perpetrado por una persona que emplea el engaño con ánimo de lucro para provocar una conducta de error en la víctima y a través del cual, se le induce a realizar un acto de disposición en perjuicio de sí misma o un tercero. Esto puede lograrse a través de invitaciones fraudulentas a participar en sorteos, correos electrónicos donde se solicitan datos personales o incluso, la falsificación de algunos portales propios de servicios comunes, como bancos u organizaciones gubernamentales.

Suplantación de identidades

La suplantación de identidades, de acuerdo a lo expuesto por Rivas (2021), es el delito informático en que consiste en engañar a las personas para que compartan información confidencial como contraseñas, números de cuenta, números de tarjetas de crédito, entre otros. Normalmente, las víctimas de este delito, reciben un mensaje de correo electrónico, SMS, WhatsApp que copia para suplantar la identidad organización de confianza. Cuando la víctima abre el mensaje encuentra un contenido pensado para asustarle (tiene una multa, se le ha bloqueado la tarjeta de crédito, u otros). Este, mensaje solicita que la víctima vaya a un sitio web y actúe de inmediato. Una vez que el usuario, entre puede descargarse un malware el cual le puede robar información, cifrársela para pedir un rescate, entre otras acciones delictivas.

Como complemento a lo anterior, Mayer y Oliver (2020), indican que el fraude informático suele relacionarse con el phishing o asunción de identidades. En la práctica, este último se vincula con la ejecución de operaciones bancarias, cuya verificación en línea constituye un ámbito idóneo para manipular o alterar datos o programas de sistemas informáticos, a fin de perjudicar el patrimonio de terceros.

Por otra parte, la Ley Especial contra los Delitos Informáticos (2001), establece en su Artículo 14 sobre el manejo fraudulento de tarjetas inteligentes o instrumentos análogos, que toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

Hechas las consideraciones que anteceden, la suplantación de identidades, se puede considerar un delito primario sobre el cual, se erigen otros como la obtención ilícita de beneficios económicos o de cualquier otra índole, mediante la utilización de documentos personales tales como tarjetas de crédito o débito, e incluso, credenciales de acceso a sistemas informáticos.

Robo o Fuga de datos

El robo o fuga de información, según lo indica Rivas (2021), es la pérdida de la confidencialidad, de forma que personal no autorizado accede a información privilegiada. La confidencialidad es uno de los principios básicos de la protección de la información. Por tanto, la fuga de datos es una brecha de datos personales donde la información ha sido accedido por parte de personal no autorizado.

Por su parte, Klusaité (2022), expresa que en internet, el robo de datos puede realizarse de muy diferentes maneras. Algunas de las más frecuentes son los ataques de phishing, que tratan de obtener credenciales de acceso o datos bancarios de sus víctimas mediante la ingeniería social, pero también pueden realizarse mediante una infección por malware o un ataque de fuerza bruta, entre otros métodos.

Así mismo, la Ley Especial contra los Delitos Informáticos (2001), establece en su Artículo 11 que toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de

tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El robo o fuga de datos es entendido en el presente estudio como la sustracción de información confidencial de un tercero, sea persona u organización. En tal sentido, pueden utilizarse distintos medios o técnicas como el phishing, con el fin de engañar al usuario para proporcionar datos sensibles y confidenciales. Así mismo, el robo de información tiene que ver con el uso de dispositivos para apropiarse de información confidencial sin el permiso del propietario de la misma. Es común en organizaciones donde circulan dispositivos portátiles como pen drives o correos electrónicos personales.

Delitos contra la propiedad intelectual

En lo tocante a este aspecto, Rivas (2021), precisa que los delitos contra la propiedad intelectual, consisten en reproducir, plagiar, distribuir o comunicar públicamente una obra sin la autorización del titular del derecho de propiedad intelectual con el objetivo de perjudicar a una persona. En ese mismo orden de ideas, Pérez y Pimentel (2007), indican que el plagio es un delito contra la propiedad intelectual muy común entre las personas, principalmente estudiantes de todos los niveles, el cual, consiste en copiar en lo sustancial obras ajenas, tal como si fueran propias. En ese sentido, resulta un flagelo presente en el ámbito informático, ya que si bien, está vinculado con cualquier tipo de obra, es en el ámbito de los medios electrónicos donde es cometido a gran escala.

Sobre este aspecto, la Ley Especial contra los Delitos Informáticos (2001), contempla en su Artículo 25 que, quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

En franca adhesión con las ideas anteriores, los delitos contra la propiedad intelectual, son aquellos que atentan contra las obras publicadas debidamente por los autores originales, lo cual, incluye productos científicos en formato físico o digital, libros, videos, imágenes o cualquier recurso multimedia protegido por las leyes de derecho de autor y otros tratados internacionales.

Sextorsión

La extorsión sexual o sextorsión, según el criterio de Rivas (2021), es una extorsión sexual y por tanto un delito informático. Este consiste en la amenaza de revelar información íntima sobre una víctima a no ser que esta pague una cantidad a la persona que está extorsionando. Dicha información podría incluir mensajes de texto sexuales, fotos íntimas e, incluso, vídeos. Los delincuentes suelen pedir dinero, pero a veces buscan material más comprometedor. También, en ocasiones, intentan engañar con la posesión de videos cuando realmente no los tienen y esto se realiza con el propósito de obtener dinero a cambio.

Hechas las consideraciones anteriores, Flores, (2015), indica que la sextorsión es un término acuñado para designar un delito cada vez más común y consistente

en la realización de un chantaje bajo la amenaza de publicar o enviar imágenes en las que la víctima muestra en actitud erótica, pornográfica o manteniendo relaciones sexuales. En definitiva, sin matizar entre chantaje o extorsión, son imágenes íntimas que el delincuente amenaza con poner en circulación a través de terminales móviles o subir a la red.

Al realizar una revisión a la Ley Especial contra los Delitos Informáticos (2001), se pudo observar en su Artículo 23 que, toda persona por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

En correspondencia con las ideas anteriores, la sextorsión es una forma de chantaje sexual en la cual los criminales se apropian de material o contenido privado de terceras personas, usualmente fotos o videos y les amenazan con hacerlo público en Internet, a menos que las víctimas paguen con algún favor, en ocasiones de índole sexual, aunque también recurren al ámbito económico.

METODOLOGÍA

En lo tocante al aspecto metodológico, la presente investigación fue de tipo descriptivo y de campo; de acuerdo a lo planteado por Hurtado (2010), ya que consiste en la enumeración de un conjunto de características o atributos de un fenómeno de estudio. Por ende, se abordan los delitos informáticos más comunes en el contexto de las PyMES de la Ciudad de Cabimas. De igual manera, se cataloga como un estudio de campo, de acuerdo con Arias (2012) quien lo define como la recolección de datos directamente de la realidad donde ocurren los hechos sin la manipulación de las variables.

Con base en las ideas anteriores, se afirma que este estudio es de campo, ya que la información se recopila directamente de la realidad donde se encuentra el objeto de estudio; es decir, las Pequeñas y Medianas empresas de la Ciudad de Cabimas, específicamente en los departamentos o instancias relacionadas con la administración de sistemas de información o similares.

En lo concerniente al diseño de la investigación, ésta se clasifica como no experimental, transeccional, según Hernández, Fernández y Baptista (2014), pues, recolectan datos en un solo momento y tiempo único. Su propósito es describir variables y su incidencia o interrelación en un momento determinado. Así mismo, en este tipo de diseños no se manipulan deliberadamente las variables. En virtud de que en el presente estudio no se realizan experimentos donde se establezca una manipulación de las variables, y la aplicación del instrumento de recolección de datos, se realiza en un solo momento durante el transcurso de la investigación; la misma, se ajusta a las características del diseño antes mencionado. A efectos de la presente investigación, se tomó una (01) población finita para la aplicación del instrumento de recolección de datos, tal como se indican los siguientes criterios de selección:

Está conformada por veinticinco (25) directores, coordinadores y jefes de informática, computación o sistemas de

las Pequeñas y Medianas Empresas de la Ciudad de Cabimas. Las mismas se seleccionaron de manera intencional, considerando aquellas que cuentan con un departamento o división de informática. Fueron consideradas por ser accesibles para el investigador y haber sido objeto de algún tipo de delito informático.

El instrumento utilizado para medir la variable en esta investigación, fue el cuestionario, En tal sentido, Arias (2012) plantea que éste, es un instrumento de recolección de información primaria, que contiene un conjunto de preguntas sistematizadas y presentadas en el mismo orden y término para ser aplicado a todos los sujetos de la investigación.

Con el propósito de medir la variable delitos informáticos, se utilizó un cuestionario aplicado a los directores, coordinadores y jedes de informática de 25 empresas de la Ciudad de Cabimas, Estado Zulia (uno por empresa), previamente diseñado por los autores del presente artículo, estructurado en quince (15) proposiciones afirmativas, utilizando la escala tipo Likert, cuyas alternativas van del 1 al 5, siendo: Nunca, casi nunca, a veces, casi siempre y siempre.

Una vez diseñado el instrumento, fue sometido a un estudio de la validez y confiabilidad. De acuerdo a lo expuesto por Hernández y otros (2014), la validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir, mientras la confiabilidad se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce los mismos resultados.

En ese propósito, la validez del contenido del instrumento, se determinó mediante el análisis y evaluación de los ítems que conforman el mismo, a través del juicio de tres (03) expertos en el área, quienes revisaron la pertinencia de los mismos en función de medir las características del fenómeno, llegando a la conclusión de que el mismo es válido para ser aplicado.

Para el cálculo del coeficiente de confiabilidad, se utilizó el software estadístico SPSS, versión 23, el cual, determina esta característica a partir de diversos métodos. Para este caso, se utilizó el coeficiente Alfa de Cronbach, obteniéndose un valor de 0.80, lo cual, representa un instrumento altamente confiable, en correspondencia con el baremo presentado por Hernández y otros (2014). Igualmente, para la interpretación de los resultados, se utilizaron las medias aritméticas, catalogadas en cinco categorías, las cuales fueron: muy baja, baja, moderada, alta y muy alta presencia, de acuerdo a lo expresado en el baremo reflejado en la Tabla 1.

Tabla 1. Baremo de interpretación de las medias aritméticas

Media	Interpretación
1.00 – 1.80	Muy baja presencia
1.81 – 2.60	Baja presencia
2.61 – 3.40	Moderada presencia
3.41 – 4.20	Alta presencia
4.21 – 5.00	Muy Alta presencia

Fuente: Díaz, Martínez y Gómez (2022).

RESULTADOS Y DISCUSIÓN

En esta sección, se muestran los resultados obtenidos a partir de la aplicación del instrumento de recolección de datos. En ese propósito, se elaboró una tabla estadística donde se muestra para cada característica o indicador con sus frecuencias absolutas y relativas porcentuales. Así mismo, se evidencia la media aritmética y su interpretación de acuerdo a lo expresado en el baremo respectivo.

En ese propósito, los resultados corresponden a los diferentes tipos de delitos informáticos, considerados como comunes, entre los cuales se encuentran la estafa, suplantación de identidades, robo o fuga de datos, delitos contra la propiedad intelectual y la sextorsión o extorsión sexual. Los mismos se aprecian en la tabla 2. Estos sirven como base para la contrastación con los aportes de los autores consultados.

Tabla 2
Resultados obtenidos: Delitos Informáticos comunes

	Estafa		Suplantación de identidades		Robo o fuga de datos		Delitos contra la propiedad intelectual		Sextorsión	
	fi	fr%	fi	fr%	fi	fr%	fi	fr%	fi	fr%
S	6	8,00	20	26,67	3	4,00	4	5,33	9	12,00
CS	8	10,67	0	0,00	10	13,33	2	2,67	5	6,67
AV	2	2,67	10	13,33	27	36,00	18	24,00	24	32,00
CN	42	56,00	37	49,33	32	42,67	36	48,00	30	40,00
N	17	22,67	8	10,67	3	4,00	15	20,00	7	9,33
Media	2,25		2,83		2,71		2,25		2,72	
Interpretación	Baja presencia		Moderada presencia		Moderada presencia		Baja presencia		Moderada presencia	

Fuente: Díaz, Martínez y Gómez (2022).

En primer lugar, la estafa reportó una baja presencia en las PyMES de Cabimas, denotándose con una media de 2,25. Así mismo, la mayor concentración de respuestas correspondió a la opción Casi Nunca (56%), sin embargo, al considerar las alternativas siempre, casi siempre y a veces, suman 20%, lo cual, sugiere una tendencia incremental de este delito entre las empresas consultadas.

Cabe destacar que esto se aproxima a las ideas expuestas por Rivas (2021), pues, se presenta en primera instancia mediante la suplantación de identidad, recurriendo a medios de contacto diversos para acceder a las víctimas. El uso de mensajes de Whatsapp que promueven una conversación es frecuente, así como los correos electrónicos o redes sociales donde se solicita la transferencia de dinero hacia determinadas cuentas bancarias por concepto de donativos o ayudas a terceros, se encuentran dentro de esta tipología de delitos.

En otro orden de ideas, la suplantación de identidades, se ubicó en una moderada presencia, con una media de 2,83. Así mismo, se precisa una mayor concentración de respuestas en la categoría Casi nunca (49,33%), sin embargo, se denota una tendencia a incrementarse, de allí un puntaje de 26,67% en la opción Siempre. Esto coincide con las ideas abordadas por Rivas (2021), quien expresa que es el delito informático en que consiste en engañar a las personas para que compartan información confidencial como contraseñas, números de cuenta, números de tarjetas de crédito, entre otros.

En el contexto, los usuarios han reportado la recepción de mensajes o correos donde se les ha invitado a actualizar datos bancarios, ingresar los números de tarjeta de crédito y acceder a sitios o páginas con aspecto similar a las entidades bancarias u organismos gubernamentales, incluso con el mismo diseño y juego de colores. Algunos han sido objeto de estos delincuentes, pero otros han notado sutilezas como la ausencia del protocolo de transferencia de hipertexto seguro (HTTPS) o los certificados de seguridad, e incluso, errores ortográficos en los mensajes, por lo cual, asumen que se trata de un fraude.

Por otra parte, el robo o fuga de datos, reportó una moderada presencia con una media de 2,71 y una concentración de respuestas en las opciones a veces y casi nunca con 36% y 42,67%, respectivamente, lo cual, implica una tendencia incipiente a cometer este tipo de delitos en las organizaciones, por cuanto, coincide con los aportes de Rivas (2021), quien asegura que es común encontrar empleados que acceden a información confidencial sin los debidos permisos en las empresas, e incluso, en el ámbito personal. También las personas menos aventajadas con el uso de las tecnologías, recurren a familiares que, en ocasiones, abusan de estos accesos para cometer faltas como apropiación indebida de dinero u otros bienes. Así mismo, en las organizaciones resulta común, detectar empleados que filtran información confidencial a sus correos personales o en dispositivos portátiles como memorias USB.

Ahora bien, los delitos contra la propiedad intelectual, se presentan en una baja presencia dentro de las organizaciones, observándose una media de 2,25 y una concentración de respuestas en las categorías Casi nunca, A veces y Nunca, con unos valores de 48%, 24% y 20%, respectivamente, por lo cual, se infiere que las empresas se cuidan de incurrir en delitos contra la producción intelectual, tales como el uso de software ilegal o recursos obtenidos mediante la piratería o acciones similares. Esto coincide con las ideas de Rivas (2021), cuando indica que éstos comprenden la reproducción, plagio o distribución de una obra sin la autorización del titular del derecho de propiedad intelectual. En tal sentido, resulta pertinente acotar que existe una porción de organizaciones que incurren en este delito, debido a los costos asociados al software o falta de cultura en cuanto a las regulaciones de la propiedad intelectual.

Por último, la sextorsión o extorsión sexual, reportó una moderada presencia con una media de 2,72 y una mayoría de respuestas en las categorías Casi nunca, A veces y nunca, con un 40%, 32% y 9,33%, respectivamente. Esto coincide con las ideas de Rivas (2021), cuando afirma que este tipo de delito, consiste en la obtención de material íntimo, como fotografías, mensajes o recursos

similares con el propósito de extorsionar a la víctima a cambio de dinero o bienes materiales. Si bien, las empresas no reflejan gran incidencia de este delito, en el ámbito personal, se infiere mayor frecuencia, al observar los valores de las frecuencias en las alternativas positivas (siempre y casi siempre). Cabe destacar que una de las razones por las cuales este delito es menos frecuente en las empresas, puede ser la existencia de políticas de seguridad y restricciones acceso a las redes sociales con fines personales.

A la luz de las ideas anteriores, resulta conveniente precisar algunas medidas de seguridad para prevenir los delitos informáticos en las empresas, los cuales se muestran a continuación:

a. Se deben mantener al día las actualizaciones de software. En ese sentido, resulta importante utilizar programas o sistemas licenciados. Es menester recordar que el software ilegal o pirata es sinónimo de riesgos, ya que los cracks o herramientas similares pueden ser conducentes a la contaminación por virus o ataques por parte de personas inescrupulosas.

b. Se deben implementar políticas de acceso a los servicios empresariales debido al auge sobrevenido del teletrabajo surgido a raíz de la pandemia. En ese propósito, las organizaciones deben proveer enlaces, accesos, credenciales y herramientas seguras para garantizar a las personas, la confidencialidad de sus transacciones a través de las redes, ya que se maneja información sensible y de interés privado.

c. Las actualizaciones de los sistemas operativos y software en general son fundamentales. Se debe prestar especial atención a las actualizaciones del navegador web. A veces, los sistemas operativos presentan vulnerabilidades, que pueden ser aprovechados por delincuentes informáticos. Son comunes las actualizaciones que solucionan dichos problemas. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

d. El uso de antivirus y firewalls es necesario para proteger los equipos contra intrusiones, o ataques perpetrados por hackers o delincuentes informáticos. En efecto, diversos sistemas operativos incluyen por lo menos un antivirus intrínseco para evitar la contaminación de un sistema debido a un software virulento. Así mismo, los firewalls ayudarán a restringir accesos no autorizados mediante la habilitación de puertos o servicios de red, así como la implementación de herramientas que permiten la preservación de la seguridad informática dentro de las empresas.

e. El uso de contraseñas seguras, es decir, aquellas compuestas por combinaciones de caracteres, números y símbolos especiales, coadyuva a proporcionar seguridad a los sistemas. En ese propósito, resulta pertinente modificar las contraseñas con frecuencia. Es preciso cambiar las claves de las cuentas de correo electrónico afiliadas a servicios bancarios, los patrones de acceso a los teléfonos móviles, computadores de escritorio o portátiles, entre otros recursos. También debe considerarse evitar las contraseñas derivadas de datos personales como fechas de nacimiento, números de identificación, entre otros.

f. La utilización de certificados de seguridad y protocolos de acceso a sitios seguros, permitirá las comunicaciones cifradas y por ende, confiables entre los

proveedores de servicios y los usuarios. En ese sentido, es necesario que al momento de acceder a portales bancarios, pasarelas de pago o portales gubernamentales, se verifique la existencia del protocolo HTTPS. Así mismo, se deben utilizar versiones actualizadas de los navegadores compatibles en virtud de minimizar los riesgos de phishing o suplantación de identidad.

g. Es conveniente evitar la propagación de mensajes de correo o cualquier otro medio con contenido dudoso y donde se solicita acceso a la lista de contactos o el ingreso de información inusual como los números de tarjetas de crédito. Así mismo, el ingreso a portales o aplicaciones donde se debe permitir publicidad con comportamiento viral, representa un factor de riesgo para los usuarios. Por tal razón, deben aplicarse filtros web, bloqueadores de ventanas emergentes o complementos similares a fin de garantizar una navegación segura a los usuarios.

h. Los usuarios de redes corporativas, deben evitar compartir sus credenciales de acceso a sistemas, tales como nombres de usuario y contraseñas, permisos especiales, tarjetas de identificación electrónicas, entre otras. Es necesario recordar que una vez otorgada una credencial de acceso a un sistema o servicio, el usuario es el único responsable de las acciones realizadas con ella, por lo cual, cobra una importancia de segundo nivel por las implicaciones legales o morales intrínsecas.

i. En el caso de las aplicaciones móviles que utilizan acceso a la ubicación, debe cuidarse en primera instancia, sólo habilitar este servicio en casos donde realmente sea necesario, ya que los hackers pueden interceptar los datos enviados o recibidos. Se debe recordar que numerosas entidades bancarias, empresas e instituciones, han implementado aplicaciones nativas y en la web, las cuales, facilitan la ejecución de ciertos procesos y para ello, requieren acceder mediante un Software de Posicionamiento Global (GPS) a cierta información sobre la localización del usuario.

CONCLUSIONES

Al finalizar el presente artículo, se puede precisar que los delitos informáticos están presentes en el contexto de las PyMES, pero también en el ámbito personal. Por consiguiente, se debe prestar una especial atención al momento de utilizar cualquier servicio o activo informático debido al riesgo intrínseco a los mismos. En tal sentido, es necesario crear conciencia entre los ciudadanos para consolidar una cultura en cuanto al uso de información sensible al acceder a cualquier herramienta o servicio.

En lo tocante a los delitos comunes, se pudo identificar en primera instancia la estafa, entendida como una acción a través de la cual, se busca la obtención de ganancias mediante el engaño efectuado hacia terceras personas, aprovechándose de su confianza. Cabe destacar que se reportó una baja presencia en este aspecto. Por ende, en el ámbito informático, se recurre a mensajes, correos electrónicos o el acceso a portales fraudulentos donde se pretende obtener datos de acceso a servicios bancarios para desviar fondos o en otros casos, utilizar esa información de forma indebida en perjuicio del afectado. Si bien, se han observado pocos casos en el entorno empresarial,

esto puede estar incrementándose entre las personas naturales.

Ahora bien, la suplantación de identidades reportó una moderada presencia, es decir, se han generado situaciones en las cuales, personas inescrupulosas se hacen pasar por otras para acceder indebidamente a servicios online en virtud de obtener algún beneficio. En tal sentido, tanto las entidades naturales como jurídicas, deben operar con cautela los distintos servicios informáticos a los cuales tienen acceso. En tal sentido, es necesario estar atentos ante cualquier solicitud inusual de información, tal como ocurre en los correos recibidos para actualizar datos bancarios, aprobar la domiciliación de servicios, entre otros.

Por otra parte, el robo o fuga de datos se presentó en una moderada presencia en el contexto empresarial, esto en virtud de los controles establecidos por las distintas gerencias para garantizar la preservación de información confidencial. Sin embargo, los sujetos indicaron que se han suscitado algunos casos donde se ha intentado vulnerar información crítica o sensible, así como la copia o distribución indebida de datos a través de soportes móviles o correos personales, por lo cual, se requiere revisar las políticas de acceso a la información en estas organizaciones.

Como complemento a lo anterior, los delitos contra la propiedad intelectual reportaron una baja presencia en el ámbito empresarial, por cuanto, se afirma que estas entidades utilizan software licenciado o realizan convenios para legalizarlo. Esto puede deberse a las políticas implementadas por los gobiernos, regulaciones y leyes existentes. Se pudo observar que la mayoría de las empresas consultadas, utilizan software adquirido mediante compra o alquiler, lo cual, les obliga a estar dentro de la ley, pues, de lo contrario, no podrían realizar procesos críticos como la facturación o en el peor de los casos, acceder a ellos. Ahora bien, en el ámbito personal, es necesario profundizar en este aspecto, pues, los estudiantes y profesionales en general, utilizan la herramienta copiar-pegar sin atender a las normas de citado, lo cual, pudiese traducirse en la comisión de un plagio o delito similar.

Por último, la sextorsión o extorsión con fines sexuales, estuvo presente en una moderada presencia, lo cual, permite afirmar que las personas han sido objeto en algún momento de agentes que buscan contacto íntimo con el fin de obtener fotografías u otro material comprometedor para luego, chantajearlos en virtud de conseguir un beneficio económico o de cualquier otra índole. Es preocupante que esto se haya observado en el entorno empresarial, ya que esto se traduce en que los empleados pudiesen estar utilizando software de mensajería o redes sociales durante las horas de trabajo para realizar actividades de ocio.

REFERENCIAS BIBLIOGRÁFICAS

Arias, Fidias (2012). El Proyecto de Investigación. Introducción a la Metodología Científica, 6ª. Edición. Editorial Epísteme. Caracas, República Bolivariana de Venezuela.

Consejo de Seguridad Nacional (2013). Estrategia de Ciberseguridad Nacional de 2013, (Documento en línea). Disponible en: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf.

Díaz, Andrés. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest, Revista electrónica del Departamento de Derecho de la Universidad de la Rioja, 8, 169 – 203

Fernández, Rosa (2022). Cibercrímenes en España - Datos estadísticos. (Documento en línea). Consultado el 09/08/2022. Disponible en: https://es.statista.com/temas/3166/ciberdelitos-en-espana/#dossierKeyfigures

Flores, Jorge (2015). Sextorsión, prácticas arriesgadas y fallos de seguridad al servicio del delito. (Documento en línea). Consultado el 11/08/2022. Disponible en: https://www.pantallasamigas.net/sextorsion-practicas-arriesgadas-y-fallos-de-seguridad-al-servicio-del-delito-2/

Gómez, Carlos (2018). Sexting y sexualidad de los jóvenes de la Universidad Técnica de Ambato, Facultad de Jurisprudencia y Ciencias Sociales. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/28891/1/FJCS-TS-286.pdf

Hernández, Roberto. Fernández, Carlos. y Baptista, María. (2014). Metodología de la Investigación, 6ª. Edición. Editorial Mc. Graw Hill Education 2014. pp. 600.

Hurtado Jacqueline. (2010). Metodología de la investigación Holística. Fundación Sypal. Caracas Venezuela.

ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? (Documento en línea). Consultado el 05-08-2022, Disponible en: http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Klusaitė, Laura (2022). ¿Qué es el robo de datos? (Documento en línea). Consultado el 11/08/2022. Disponible en: https://nordvpn.com/es/blog/robo-de-datos/

Ley Especial contra los Delitos Informáticos (2001). Gaceta Oficial de la República Bolivariana de Venezuela. No. 37.313. 30 de Octubre de 2001.

Loredo, Jesús y Ramírez, Aurelio (2013). Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo. Facultad de Ciencias Físico Matemáticas. Universidad Autónoma de Nuevo León. San Nicolás de los Garza, Nuevo León, México.

Mayer, Laura y Oliver, Guillermo (2020). El delito de fraude informático: concepto y delimitación. Revista Chilena de Derecho y Tecnología |Volumen 9 Número. 1. Disponible en: https://rchdt.uchile.cl/index.php/RCHDT/article/view/57149/61949

Pérez, Patricia y Pimentel, Jesús (2007). El Plagio Electrónico, ¿Necesidad del Alumno Promedio?. Revista Polibits, Número 35, pp. 6. Instituto Politécnico Nacional. Distrito Federal, México. Disponible en: https://www.redalyc.org/pdf/4026/402640448001.pdf

Rivas, José (2021). ¿Cuáles son los tipos de delitos informáticos más comunes? (Documento en línea). Consultado el 11/08/2022. Disponible en: https://www.laboratoriodeinformaticafor

ense.com/estos-son-los-tipos-de-delitos-informaticos-mas-frecuentes/

Temperini, Marcelo (2014). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 2da. Parte. 14º Simposio Argentino de Informática y Derecho, SID 2014. Disponible en: https://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

Verney, Silvina (2013). Curso presencial y/o virtual Derecho Penal Contemporáneo. Delitos informáticos. (Documento en línea). Consultado el 05-08-2022. Disponible en: https://www.terragnijurista.com.ar/doctrina/informaticos.htm