Las opiniones y los contenidos de los trabajos publicados son responsabilidad de los autores, por tanto, no necesariamente coinciden con los de la Red Internacional de Investigadores en Competitividad.

Esta obra por la Red Internacional de Investigadores en Competitividad se encuentra bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 3.0 Unported. Basada en una obra en riico.net.

Ciberseguridad 4.0: Factores que propician el delito de robo de identidad digital por medios informáticos

Laura Angélica Guzmán-Cedillo[1]

Werner Horacio Varela-Castro[2]

*María de los Angeles Briceño-Santacruz**

Resumen

Con el desarrollo de la informática se establecieron diversos instrumentos financieros digitales, que limitan el manejo de efectivo monetario, pero también llego lo que se llama Robo de la Identidad Digital Personal, para fines ilegales y fraudes informáticos, Ciberseguridad. El objetivo de la investigación es conocer los factores que influyen en el robo de identidad digital. Para lo cual se revisó la literatura relacionada y la aplicación de un instrumento de elaboración propia, encontrándose que la aplicación de las TIC para prevenir el fraude informático es más común a nivel internacional, a nivel nacional es más común que las instituciones financieras promuevan instrumentos digitales financieros que por sí mismo limiten el fraude informático y el robo de identidad digital, existe mucha confianza en el uso de instrumentos digitales financieros (IDF), a pesar de la existencia de hackers con alta impunidad al realizar actividades ilícitas y poco apoyo jurídico y normativo.

Palabras clave: Ciberseguridad**,** instrumentos digitales financieros (IDF), robo de identidad digital y fraude cibernético.

ABSTRACT

With the development of information technology, various digital financial instruments were established, which limit the handling of monetary cash, but what is called Personal Digital Identity Theft also arrived, for illegal purposes and computer fraud, Cybersecurity. The objective of the investigation is to know the factors that influence the theft of digital identity. For which the related literature and the application of an instrument of own elaboration were reviewed, finding that the application of ICT to prevent computer fraud is more common at the international level, at the national level it is more common for financial institutions to promote Financial digital instruments that by themselves limit computer fraud and theft of digital identity, there is a lot of confidence in the use of financial digital instruments (FDI), despite the existence of hackers with high impunity when carrying out illegal activities and little legal support and normative.

Keywords: Cybersecurity, digital financial instruments (FDI), digital identity theft and cyber fraud.

[1] Universidad Autónoma Agraria Antonio Narro

[2] Universidad Autónoma de Coahuila Unidad Torreón

Introducción

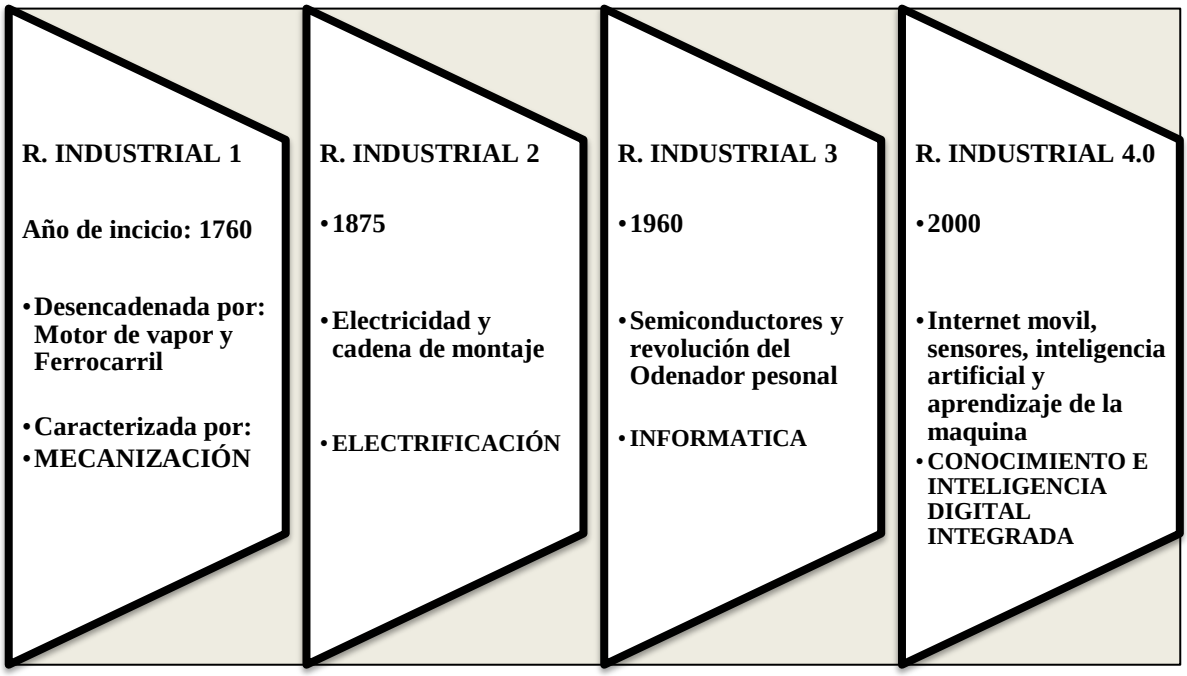
Haciendo un poco de historia, la frase delito informático como término se empezó a usar a finales de los años noventa en Lyon Francia, ya que se funda un grupo denominado G8 con la intención de estudiar todos los problemas emergentes de criminalidad que eran propiciados por la migración a Internet, así se empezaron a diseñar Tratados sobre Delito Informático. Este tratado describía las diferentes disposiciones por las que se requería una legislación sobre la criminalidad informática que incluye una amplia variedad de delitos informáticos entre otros Sabotaje informático, Piratería informática, Robo de identidad y Phreaking entre otros. Por otra parte desde 2006 a la fecha se han presentado diversas proposiciones con puntos de acuerdo para exhortar a las autoridades del sector financiero mexicano a la adopción de medidas que tiendan a prevenir y combatir las prácticas de suplantación de identidad, y ya para 2016 se firma el documento titulado Bases de Colaboración para inhibir la suplantación de identidad a través del sistema financiero mexicano, donde se establece ejercer acciones conjuntas para la prevención de este delito. Las instituciones firmantes fueron el Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales, Instituto Nacional Electoral, Asociación del Banco de México, la PRODECON, la CONDUSEF, y el SAT. Cabe destacar que durante 2017, se registraron 4.8 millones de reclamaciones de posible fraude en el sector financiero, según estadísticas de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef). Al respecto, sobresale que cerca de la mitad de los casos (49%) tuvieron origen en el comercio electrónico. En comparación con reportes anteriores, presentó un incremento del 109%, puesto que en 2011 sólo representaba el 8% del total de las reclamaciones. Tal disparidad en los indicadores demuestra la preocupación e interés creciente por conocer a fondo los diferentes tipos de fraude financiero que asechan principalmente en internet. De acuerdo con la Condusef, las actividades delictivas más frecuentes en el comercio electrónico son la suplantación de identidad, el robo de datos personales, las campañas falsas de afiliación, las compras trianguladas y el *hackeo* de cuentas.

Revisión de la literatura

La cuarta revolución industrial. Contexto histórico. La palabra "revolución" indica un cambio abrupto y radical. Las revoluciones se han producido a lo largo de la historia cuando nuevas tecnologías y formas novedosas de percibir el mundo desencadenan un cambio profundo en los sistemas económicos y las estructuras sociales. Dado que la historia se utiliza como un marco de referencia, la brusquedad de estos cambios puede tardar años en desplegarse. A partir de lo anterior Klaus Schwab (2017), describe el contexto histórico de los cambios profundos en el proceso de industrialización de la humanidad: El primer cambio profundo en nuestra manera de vivir fue la

transición del forrajeo a la agricultura y esto ocurrió hace alrededor de diez mil años y fue posible gracias a la domesticación de animales. La revolución agrícola combinó los esfuerzos de los animales con los de los seres humanos con vistas a la producción, el transporte y la comunicación. Poco a poco la producción de alimentos mejoró, estimulando el crecimiento de la población y facilitando asentamientos humanos más grandes. Esto condujo a la postre, a la urbanización y el surgimiento de las ciudades. La revolución agrícola fue seguida por una serie de revoluciones industriales (Figura 1) que comenzaron en la segunda mitad del siglo XVIII. Estas marcaron la transición de la energía muscular a la mecánica y evolucionaron hasta lo que conocemos hoy, con la cuarta revolución industrial: un mayor poder cognitivo que aumenta la producción humana (Schwab, 2017).

Figura 1. Evolución histórica hacia la cuarta revolución industrial



Fuente: Elaboración propia tomado de Schwab (2017).

La primera revolución industrial abarcó desde aproximadamente 1790 hasta más o menos 1840. Desencadenada por la construcción del ferrocarril y la invención del motor de vapor, marcó el comienzo de la producción mecánica. La segunda revolución industrial, entre finales del siglo XIX y principios del XX, hizo posible la producción en masa, fomentada por el advenimiento de la electricidad y la cadena de montaje. La tercera revolución industrial se inició en la década de 1960. Generalmente se la conoce como la revolución digital o del ordenador, porque fue catalizada por el desarrollo de los semiconductores, la computación mediante servidores tipo "mainframe" (en los años sesenta), la informática personal (décadas de 1970 y 1980) e internet (década de 1990). Habida cuenta de las diversas definiciones y argumentos académicos utilizados para describir las tres

primeras revoluciones industriales, estamos en los albores de una cuarta revolución industrial. Esta comenzó a principios de este siglo y se basa en la revolución digital. Se caracteriza por un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina. Las tecnologías digitales que en su núcleo poseen hardware para computación, software y redes no son nuevas, pero, a diferencia de la tercera revolución industrial, son cada vez más sofisticadas e integradas y están, de resultas de ello, transformando las sociedades y la economía mundial. Esta es la razón por la que los profesores Erik Brynjolfsson y Andrew McAfee (en Schwab, 2017), afirmaron que el mundo está en un punto de inflexión en que el efecto de estas tecnologías digitales se manifestará con "toda su fuerza" a través de la automatización y la creación de cosas "sin precedentes".

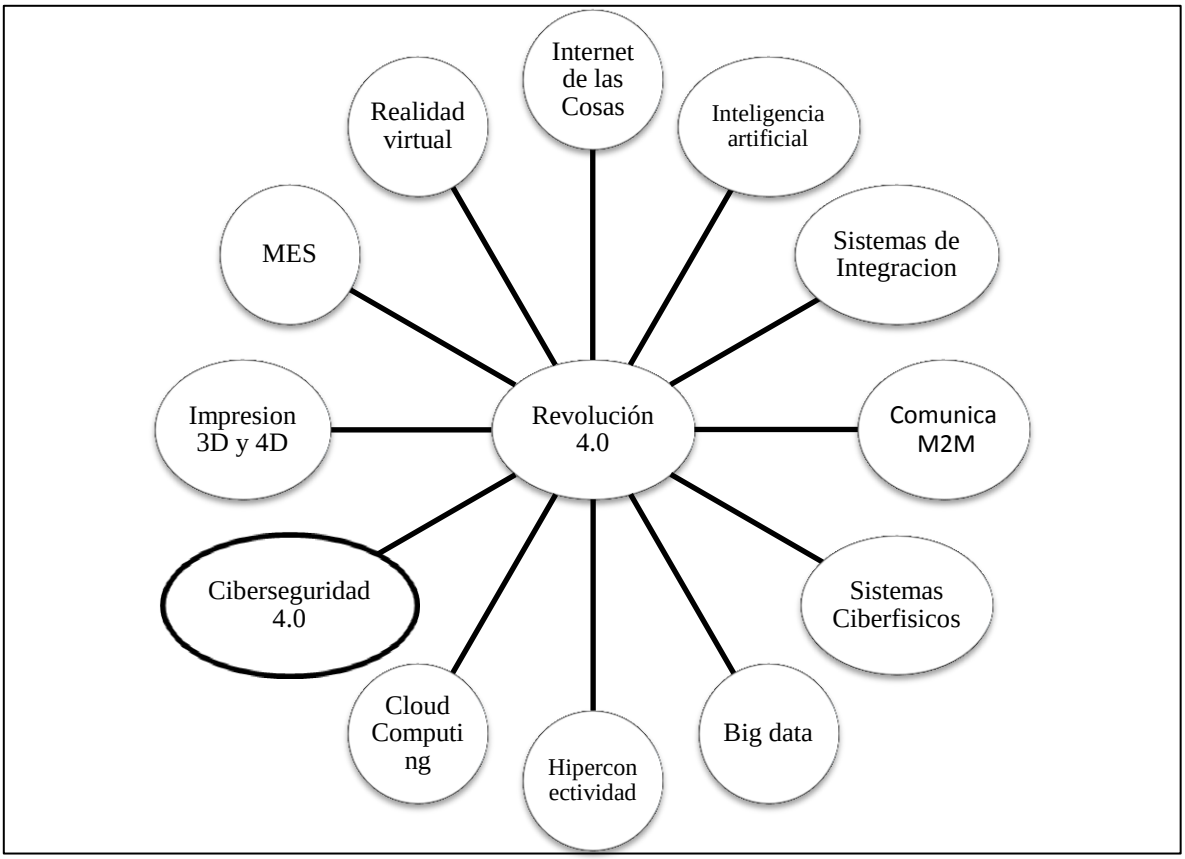
En Alemania se debate sobre la "industria 4.0", un término acuñado en la Feria de Hannover de 2011 para describir cómo esta revolucionará la organización de las cadenas de valor globales. Mediante la creación de "fábricas inteligentes", la cuarta revolución industrial genera un mundo en el que sistemas de fabricación virtuales y físicos cooperan entre sí de una manera flexible en todo el planeta. Esto permite la absoluta personalización de los productos y la creación de nuevos modelos de operación. La cuarta revolución industrial, no obstante, no solo consiste en máquinas y sistemas inteligentes y conectados. Su alcance es más amplio. Al mismo tiempo, se producen oleadas de más avances en ámbitos que van de la secuenciación genética hasta la nanotecnología, y de las energías renovables a la computación cuántica. Es la fusión de estas tecnologías y su interacción a través de los aspectos físicos, digitales y biológicos lo que hace que la cuarta revolución industrial sea fundamentalmente diferente de las anteriores. En esta revolución, las tecnologías emergentes y la innovación de base extendida se están difundiendo mucho más rápido y más ampliamente que en las anteriores revoluciones, todavía en desarrollo en algunas partes del mundo. La segunda revolución industrial todavía debe ser plenamente experimentada por el 17 por ciento de la población mundial, pues casi 1,300 millones de personas carecen de acceso a la electricidad. Esto también es válido para la tercera revolución industrial, con más de la mitad de la población mundial, 4,000 millones de personas, la mayoría en el mundo en desarrollo, sin acceso a internet. El huso (el sello de la primera revolución industrial) tardó casi 120 años en difundirse fuera de Europa. Por el contrario, internet permeó todo el mundo en menos de una década. Todavía válida hoy en día es la lección de la primera revolución industrial, según la cual la medida en que la sociedad abraza la innovación tecnológica es un factor crucial del progreso. El gobierno y las instituciones públicas, así como el sector privado, tienen que cumplir su parte, pero también es esencial que los ciudadanos vean los beneficios a largo plazo. Schwab (2017) está convencido de que la cuarta revolución industrial será en cada detalle tan poderoso, impactante e históricamente importante como las tres

anteriores. Sin embargo, tiene dos preocupaciones fundamentales acerca de los factores que podrían limitar el potencial de la cuarta revolución industrial para que sea eficaz y coherente. En primer lugar, piensa que los niveles necesarios de liderazgo y comprensión de los cambios en marcha, en todos los sectores, son bajos en comparación con la necesidad de rediseñar nuestros sistemas económicos, sociales y políticos para responder a la cuarta revolución industrial. Como resultado de ello, a escala tanto nacional como mundial el marco institucional (y legal) requerido para dirigir la difusión de la innovación y mitigar la disrupción es inadecuada en el mejor de los casos y, en el peor, completamente inexistente. En segundo lugar, el mundo carece de una narrativa consistente, positiva y común que describa las oportunidades y los desafíos de la cuarta revolución industrial, una narrativa que es esencial si queremos empoderar a un conjunto diverso de individuos y comunidades, y evitar una violenta reacción popular contra los cambios fundamentales en curso.

¿Qué es y qué aporta la Industria 4.0? El concepto Industria 4.0 o su homólogo Cuarta Revolución Industrial, supone un nuevo hito en el desarrollo industrial aspirando a la digitalización de los procesos productivos aumentando su eficiencia, calidad y seguridad a partir de la introducción de tecnologías digitales en las plantas industriales renueva la forma de operar y producir transformando productos, cadena de suministro y expectativas con clientes. Cuatro avances constituyen el motor que favorece el impulso de la transformación digital: Información digital, automatización de procesos, fabricación inteligente y cliente conectado. El alcance de estos grandes avances en la integración digital de la información proporciona acceso en tiempo real a los datos nos hacen vislumbrar grandes mejoras en los puestos de trabajo, productos personalizados para cada cliente, mayor interacción con los proveedores, convirtiendo a las organizaciones en entes más predictivos. Lo que conlleva a un aumento de la productividad y competitividad y una significativa reducción de los costes, y un interesante aumento de la rentabilidad. Por otra parte revolución Industria 4.0 ofrece una nueva visión apoyándose en unas bases tecnológicas (Figura 2) que se encuentran actualmente cada vez más desarrolladas y que permitirán transformar y garantizar un sobresaliente apoyo al usuario, entre otros tales como: Internet de las cosas, robótica e inteligencia artificial, sistemas para la integración vertical y horizontal, comunicación M2M (Machine to Machine), sistemas ciberfísicos, Big Data, hiperconectividad, cloud computing (nube), fabricación digital (Impresión 3D/4D), MES, así como la realidad virtual y aumentada (Garatu, 2018).

Así mismo se requiere destacar el elemento en la Figura 2, **Ciberseguridad**: Es la práctica de proteger los sistemas informáticos de las empresas de ataques malintencionados que pudieran poner en riesgo la adecuada actividad de dichos sistemas, utilizándolos o perturbando su funcionamiento.

Figura 2. Tecnologías clave de la revolución industrial 4.0



Fuente: Elaboración propia tomado de Garatu (2018)

En resumen, la incorporación de alguno de estos elementos en la cadena de valor de la empresa facilita el flujo de información desde el mundo físico a las decisiones de negocio en tiempo real. Como ya lo mencionamos es por esto que la convergencia entre la automatización de los procesos relativos y las Tecnologías de la Información permiten mejorar las operaciones (automatización, flexibilidad, velocidad y productividad), reducir costes, así como mejorar la calidad de dichos procesos.

Ciberseguridad: La colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus Ciberseguridad 4.0). El movimiento Industria 4.0 comenzó en Alemania, (Schwab, 2017) y continua creciendo esta digitalización de los procesos productivos notablemente también en todos los países desarrollados donde se presentan beneficios que lo propician aunque también existen obstáculos que están ralentizando la digitalización: La falta de cultura digital y formación adecuada, resistencia al cambio, la ausencia de una visión clara de las operaciones digitales y el liderazgo de la alta dirección, un conocimiento confuso de los beneficios económicos de invertir en tecnologías digitales, talento insuficiente, fiabilidad de la seguridad digital y el más importante de todos la Ciberseguridad. Las sofisticadas amenazas a la propiedad intelectual y a la

privacidad, a los sistemas y los productos conectados, requieren estrategias y herramientas de Ciberseguridad (Aguilar, 2017). De esta manera se desarrolló una clasificación bajo el concepto de si están preparados para la siguiente revolución. Para ello la Unión Internacional de Telecomunicaciones (2015) presenta una clasificación mundial (Tabla 1) donde muchos países tienen la misma clasificación, lo que indica que se encuentran en el mismo nivel de preparación. Este índice tiene un bajo nivel de detalle, ya que su objetivo es representar la preparación de los países para la Ciberseguridad o su compromiso con ésta, y no el detalle de sus capacidades ni sus posibles vulnerabilidades.

Tabla 1. México en la Clasificación mundial de los países por índice de Ciberseguridad

Posición	País	Índice	Clasificación mundial
1	Estados Unidos de América	0,824	1
2	Canadá	0,794	2
3	Australia	0,765	3
4	Malasia	0,765	3
5	Omán	0,765	3
6	Nueva Zelandia	0,735	4
7	Noruega	0,735	4
8	Brasil	0,706	5
9	Estonia	0,706	5
10	Alemania	0,706	5
11	India	0,706	5
12	Japón	0,706	5
74	México	0,324	18
75	Perú	0,324	18

Fuente: Unión Internacional de Telecomunicaciones (2015).

El Índice Mundial de Ciberseguridad (IMC) surge de la asociación de colaboración entre el sector privado y una organización internacional, con el fin de impulsar la cuestión de la Ciberseguridad hasta el primer plano de las agendas nacionales. El IMC es un proyecto conjunto emprendido por ABI Research y la Unión Internacional de Telecomunicaciones (2015), que contribuye a una mejor comprensión del compromiso de los estados soberanos con la Ciberseguridad. El IMC no pretende determinar la eficacia ni el éxito de una medida particular, sino simplemente la existencia de estructuras nacionales para implementar y promover la Ciberseguridad. La base del IMC tiene sus raíces en la agenda sobre Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (2015) y considera el nivel de compromiso en cinco ámbitos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional. Que como resultado se observa que México ocupa el lugar 74 de más de doscientos estados miembros (Tabla 1), y a pesar de ello está dentro de los tres mejores índices y clasificación en américa latina. El propósito del IMC es ofrecer una instantánea de la situación de los países en cuanto a su compromiso con la Ciberseguridad a nivel nacional y junto a os gobiernos mejorar la salvaguardia de la integridad del ciberespacio debe conllevar el desarrollo de la Ciberseguridad.

La Ciberseguridad: tema de negocios. En la actualidad, ninguna empresa es inmune a un ataque cibernético. La inquietud no reside en saber si existe la posibilidad de que les suceda, sino en cuándo va a sucederles (Gutiérrez, 2019). Se trata de que una compañía conozca los procedimientos que debe seguir, a quién avisar y cómo hacerlo, entre otros puntos, tras ser víctima de un ciberataque y al final de cuentas, toda la organización debe entender que para enfrentar a una nueva amenaza se necesita tener una visión que vaya más allá de controles y temas tecnológicos, pues un ataque de esta naturaleza afecta no solo a esa área de la empresa, sino a toda la organización. Lo anterior está provocando que las empresas asignen cada vez un mayor presupuesto para protegerse De acuerdo a Gutiérrez (2019), la industria del Cibercriminal ha crecido de tal manera que es improbable prever una disminución de sus ataques, debido a las grandes cantidades de dinero que este delito genera y sigue generando. Este fenómeno seguirá sucediendo mientras las empresas continúen abriéndose al mundo digital, una tendencia que no va a parar y que se ha impulsado con iniciativas como el Internet de las Cosas, que ha engrandecido el terreno sobre el cual hoy los atacantes actúan. En ese sentido, las organizaciones deben aprender a mejorar sus niveles de protección, detectando cuáles son las áreas en donde necesitan invertir más tiempo, dinero y esfuerzo para protegerlas de mejor manera.

Ciberseguridad en México, ¿dónde estamos parados? México se encuentra entre los tres países más desarrollados en temas de Ciberseguridad en América Latina. Nuestro país está llevando a cabo diversas iniciativas en esta materia, tanto en el sector privado como en el público e incluso el ciudadano. La Ciberseguridad es un tema que llegó para quedarse y, en ese sentido, las organizaciones deben ser capaces de anticiparse al impacto de una amenaza, esto implica progresar en capacidades de Ciberinteligencia, y reaccionar correctamente cuando el incidente se manifieste (Gutiérrez, 2019).

Ciberseguridad en México ¿cuáles serán los desafíos del nuevo gobierno? Uno de los principales retos de acuerdo a lo expresado por Robles (2018) que tendrá la nueva administración gubernamental será convertir a la Ciberseguridad en una prioridad en las estrategias y proyectos que decida poner en marcha, en otras palabras posicionar a la Ciberseguridad como una prioridad que esté presente desde el inicio de los proyectos, será, sin duda, uno de los retos principales que tendrá que afrontar el próximo gobierno. De igual forma, será primordial que se comprenda que la Ciberseguridad es un tema de seguridad nacional, que afecta tanto al ciudadano, como al sector público y privado, por lo que tiene que ser visto como una prioridad en los planes y proyectos que el gobierno entrante decida poner en marcha, al final de cuentas, también los ciudadanos participan de manera activa en el ecosistema digital y, por ende, están expuestos a diversos riesgos cibernéticos. Como se mencionó anteriormente la base del IMC tiene sus raíces en la Agenda sobre

Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (2015) y considera el nivel de compromiso privado y gubernamental en cinco ámbitos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional las cuales buscan contrarrestar el delito informático, criminalidad informática, robo de identidad

Delito informático. Utilización de la informática o de las tecnologías de la información y de las comunicaciones para a producción de un hecho delictivo. Es complejo hablar del tema de seguridad al definir un delito informátic**o, y**a que son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático implicando actividades criminales. Haciendo un poco de historia, éste término se empezó a usar a finales de los años noventa, en Lyon Francia, donde se funda un grupo denominado G8 cuya finalidad es estudiar todos los problemas emergentes de criminalidad por la migración a Internet.

Criminalidad informática. Incluye una amplia variedad de delitos informáticos: Sabotaje informático, piratería informática, robo de identidad, phreaking entre otros las afectaciones financieras que son delitos de Ciberseguridad relacionados con la empresa: Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, intercepción ilegal de datos. Especialistas en delitos informáticos indican las dificultades en las investigaciones de delitos propiciados por el uso de la tecnología de la información cruzada de redes sociales o correos electrónicos que no se encuentran en el país. Tampoco se cuenta con convenios internacionales que faciliten el cruce de datos por lo que se dificulta detectar las direcciones IP desde la que se habrá realizado el ataque por lo que los procesos pueden tardar meses.

Robo de identidad. Consiste en la apropiación o usurpación de datos y documentos de identificación de una persona para fabricar con ellos documentos de identidad, o bien, generar, condiciones mínimas de identidad que sirvan como plataforma para realizar en perjuicio de la víctima todo tipo de operaciones delictivas.

Datos relevantes sobre la Ciberseguridad en México y el mundo. Los delitos cibernéticos tienen un valor para la economía mundial de 445,000 millones de dólares, de acuerdo con el especialista en Tecnologías de la Información de IBM Eduardo Palacios (en Riquelme, 2017) ademas establece que la seguridad cibernética es una práctica que debe estar integrada a la estructura organizacional de las empresas y de cualquier tipo de organización. La seguridad de la infraestructura digital es un elemento que debe ser considerado si es que una organización quiere vincularse con el proceso de transformación digital que están viviendo muchas entidades a nivel mundial.

De acuerdo con información de Julio Sánchez Onofre (en Riquelme, 2017), la industria del secuestro de información alcanzó un valor de 1,000 millones de dólares en el 2016. El ataque de WannaCry que impactó a más de 200,000 equipos a nivel mundial en mayo pasado puso en

evidencia la vulnerabilidad de las organizaciones frente a los ataques de rápida propagación. Para hacerle frente a este tipo de ataques o intrusiones a la seguridad de una organización, es necesario que las organizaciones protejan toda su información sensible; incrementar el alcance de la Ciberseguridad a todos los dispositivos que forman parte de la red de la organización; así como proteger toda la infraestructura digital. Estos son algunos datos relevantes sobre la ciberseguridad en México y en el mundo. 1) 4,000 millones de registros digitales comprometidos en el 2016. Del 2015 al 2016, hubo un aumento de 566% en el número de archivos comprometidos por amenazas de crímenes cibernéticos en todo el mundo, el cual pasó de 600 a 4,000 millones 2) 445,000 millones de dólares al año es el costo del cibercrimen para la economía mundial. Los delitos cibernéticos tienen un valor para la economía mundial de 445,000 millones de dólares, 3) El tipo de fraude cibernético más frecuente es el phishing, con 41%. 4) 39 días es el tiempo promedio para contener una intrusión cibernética.. 5) Para 46.7% de las organizaciones en México existe solo una probabilidad media de que sus archivos digitales sean robados o dañados. 6) Gobierno, banca y finanzas son los sectores más propensos a recibir ataques cibernéticos. Debido a la apertura y alcance de Internet, prácticamente todos los sectores económicos y sociales son vulnerables de sufrir un ataque si no tienen la infraestructura y una estrategia adecuada para contrarrestar este tipo de amenazas. De acuerdo con VU Labs, 29% (en Riquelme, 2017). de las organizaciones de América Latina consultadas en su estudio Ciberseguridad en entornos digitales dijo que además de la banca y el sector financiero, el sector gubernamental es el más propenso a sufrir este tipo de ataques. Le sigue, con 27%, telecomunicaciones; luego salud, con 16%; educación, con 13%; minería, 8%, y construcción, con 7 por ciento.

Definición del problema

En base a la literatura revisada se encontró una restricción a la Ciberseguridad de la revolución industrial 4.0, dicha restricción es el robo de la Identidad Digital personal que propicia el fraude informático en los procesos financieros mediante el uso de instrumentos digitales.

Objetivo general

Conocer que factores influyen en el robo de Identidad Digital Personal

Objetivo específico

Conocer como la tecnología influye en la protección de la identidad digital de las personas.

Hipótesis

HT: Existen factores que influyen en el robo de identidad digital

Justificación

Este trabajo de investigación es útil y se justifica en la búsqueda de conocer y explicar los factores que influyen en el robo de identidad digital, así como conocer como las legislaciones y la tecnología influye en la protección de la identidad digital de las personas.

Método

Limitantes y alcances de la investigación

Dentro de los alcances de esta investigación de tipo explicativa se busca conocer que factores influyen en el robo de identidad digital. Es una investigación no experimental, porque no se manipuló deliberadamente ninguna de las variables ni se desarrollaron condiciones o estímulos a los cuales se expusieran los sujetos de investigación y/o ni se construyó ninguna situación para ver sus efectos. Es de campo y no aleatorio puesto que las encuestas se realizaron en una muestra a conveniencia. Es transversal, ya que la investigación nos dio a conocer los factores que mas influyen en el robo de identidad digital y no se llevó a cabo un estudio a través del tiempo.

Diseño de investigación

Se aplicó un instrumento de medición de elaboración propia a 90 sujetos, este instrumento está compuesto por 54 variables de intervalo con escala de Likert de 0 a 6, cinco nominales, se encontró un Alfa de Cronbach de 90% lo que nos proporciona un nivel de validez y confiabilidad muy bueno con un error de estimación de 2.7%

Resultados

Características de los sujetos

De los sujetos entrevistados el 54% pertenece al sexo femenino y 46% al sexo masculino. También se observa que de los sujetos entrevistados el 0% tienen un nivel de estudios de primaria y secundaria, el 20% tiene un nivel de preparatoria, el 54% tienen un nivel de profesional, el 20% tiene nivel de posgrado y el 5% tiene otro nivel de estudio no especificado. En relación con los instrumentos digitales que manejan se observa que el 54% de los entrevistados manejan tarjetas de crédito, 18% manejan tarjetas de débito, 13% pagos por aplicación móvil, 10% hacen transferencias bancarias y 4% utiliza otro instrumento digital no especificado, en relación a las Instituciones Bancarias que utilizan los entrevistados se observa que el 69% utiliza Bancomer,22% Banamex, 3% utiliza Banorte, 3% Santander Serfin, 0% Scotiabank, 2% el banco HSBC y 0% otro banco no especificado. También se observa que en relación a la edad de los entrevistados el 10% son menores de 18años, el 58% tiene entre 19 y 38 años y el 32% tienen mas de 39 años de edad.

Análisis de datos univariables (Descriptivos)

Una vez analizados los datos que caracterizan de manera nominal la muestra, pasamos a realizar una descripción de las variables más importantes de la investigación mediante la utilización de diversas técnicas estadísticas.

Tabla 2. Variables comúnmente más correlacionadas con las nuevas TIC´s que modifican la Cultura de la prevención del fraude informático

Variable	Media	Des Std.	Media Total	Des Std.	Corr. Total	R^2
Expertos20	3.40	1.63	197.17	32.42	0.60	0.85
Convenios21	3.49	1.59	197.08	32.45	0.60	0.83
Tratados23	3.51	1.54	197.07	32.55	0.56	0.80
Tecnicas47	4.29	1.28	196.28	32.70	0.55	0.73
Financiera9	3.73	1.71	196.84	32.48	0.54	0.76
Procedimientos37	3.30	1.47	197.27	32.62	0.53	0.84
Convenios19	3.34	1.58	197.24	32.57	0.52	0.79
Normativas11	4.17	1.54	196.40	32.61	0.51	0.81
Automatizados38	3.35	1.39	197.22	32.69	0.51	0.76
Tecnologias53	4.25	1.37	196.33	32.71	0.51	0.85

Fuente: Elaboración propia

Como se observa en la Tabla 2, basados en la correlación de cada una de las variables bajo estudio, se encontró que las nuevas tecnologías de información y comunicación modifican la cultura de prevención del fraude informático. (Tecnologias53), a partir de dos vertientes, en primer lugar se observa que a nivel internacional se desarrolla una actividad inusitada, en la cual existen expertos internacionales que trabajan en pro de un nuevo orden internacional de los derechos jurídicos contra el robo de identidad (Expertos20), lo que genera un conjunto de convenios y tratados jurídicos internacionales que se llevan a cabo para prevenir el robo de identidad (Convenios21), el fraude informático (Convenios19),y el uso indebido de los instrumentos digitales financieros (Tratados23). Además, como variables más correlacionadas por otra parte; a nivel nacional y regional las empresas financieras generan una cultura de prevención de robo de identidad digital (Financiera9), a partir de los apoyos proporcionados por estas tales como procesos automatizados que toman decisiones para evitar el fraude. (Automatizados38), así mismo al aplicar con antelación técnicas informáticas adecuadas (Tecnicas47), recomendaciones Normativas al utilizar instrumentos financieros (Normativas11), de esta manera buscan dichas empresas financieras, garantizar con la aplicación de procedimientos de informática jurídica evitar el fraude informático (Procedimientos37).

Análisis factorial Multivariante

Para determinar si el estudio contenía variables validas se realizaron tres pruebas iniciales: Determinante de la matriz de correlaciones, KMO y Esfericidad de Bartlett. En la prueba se muestra que la validez del estudio (Tabla 3) se fundamenta en el coeficiente del determinante de la matriz de correlaciones con valor casi cero (3.20E-017), donde se observa una correlación en un nivel regular de adecuación muestral de las variables en 60.6% inicial en KMO.

Tabla 3. Prueba del determinante, prueba de KMO y prueba de Esfericidad de Bartlett

Determinante de Matriz de Correlaciones		3.20E-017
Medida de adecuación muestral de Kaiser-Meyer-Olkin.		.606
Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	2626.9
	Grados de Libertad	1431
	Significancia.	.000

Fuente: Elaboración propia

Además la Chi cuadrada (2626.9) se encuentra en un nivel aceptable por lo cual al correlacionar las variables se obtuvieron datos significativos a través de los cuales se aprobó la hipótesis inicial, el factor mínimo de validez en la prueba de esfericidad de Bartlett es de 1431 cuya significancia se aproxima a 0.000 lo cual indica que es significativa al 95% de confianza ($\alpha < 0.05$).

Tabla 4. Eigenvalues y porcentaje de varianza explicada total.

	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma de las saturaciones al cuadrado de la rotación		
Factor	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	9.75	18.05	18.05	9.40	17.42	17.42	3.58	6.62	6.62
2	5.01	9.28	27.33	4.67	8.65	26.06	3.54	6.55	13.18
3	3.28	6.07	33.40	2.93	5.43	31.49	3.38	6.25	19.43
4	2.40	4.44	37.84	2.04	3.77	35.26	2.20	4.08	23.52
5	2.29	4.24	42.08	1.94	3.60	38.86	2.19	4.06	27.57
6	2.16	3.99	46.07	1.80	3.34	42.20	2.06	3.81	31.38
7	1.91	3.54	49.61	1.54	2.84	45.04	2.04	3.77	35.15
8	1.78	3.29	52.90	1.40	2.59	47.63	1.99	3.69	38.84
9	1.71	3.17	56.07	1.37	2.53	50.16	1.82	3.37	42.21
10	1.61	2.99	59.06	1.25	2.31	52.48	1.78	3.30	45.51
11	1.47	2.73	61.79	1.11	2.06	54.53	1.77	3.28	48.79
12	1.40	2.59	64.38	1.03	1.91	56.44	1.63	3.02	51.81
13	1.24	2.30	66.67	.90	1.67	58.11	1.56	2.89	54.71
14	1.18	2.18	68.86	.82	1.53	59.64	1.33	2.47	57.17
15	1.13	2.10	70.95	.77	1.42	61.06	1.27	2.35	59.52
16	1.11	2.06	73.02	.74	1.36	62.43	1.14	2.11	61.64
17	1.02	1.90	74.91	.64	1.19	63.62	1.07	1.98	63.62

Fuente: Elaboración propia

En la Tabla 4, se muestra la varianza explicada total de 63.6 en donde las variables se reducen a comunalidades y se determina el nivel máximo de explicación de la encuesta para la investigación; un nivel mínimo aceptable es de 50%, el resto se explica con la teoría contenida en la literatura y con ello se complementa el modelo para la aplicación en las organizaciones de las medidas preventivas relevantes para evitar el fraude informático
a partir de del robo de identidad.

Análisis factorial

Como se observa en la Tabla 5, para efectos de significancia de los factores a estudiar se realizó un Re-Test tomando en cuenta un valor mínimo de 0.6 para efectos de explorar la significancia de los factores individuales. Fundamentado en la tradición: el valor de fiabilidad en investigación exploratoria debe ser igual o mayor a 0.6; entre estos autores Nunnally (1995): establece inclusive que en las primeras fases de la investigación un valor de fiabilidad de 0.6 o 0.5 puede ser suficiente.

Tabla 5. Re-Test exploratorio de confiabilidad de los factores unitarios

Factor no.	Nombre Factor	Variables	Alfa de Cronbach
1	Incremento y prevención del delito informático	Previene10 Delito12 Normativas11 Influencia39	0.745
2	Tratados Internacionales	Convenios21 Expertos20 Convenios19 Tratados23	0.828
3	Informática Jurídica	Estafa36 Acciones34 Internet35 Procedimientos37	0.815
4	Castigos legales a delitos informáticos	Proceso22 Penas40 Castigos41	0.717
5	No significativo	Internet52 Vulnerabilidad 54	0.528
6	No significativo	Características31 Juridicamente42 Intromisiones50	0.559
7	Conceptualizar “Robo de identidad Digital”	Conceptualizar29 Legislacion28	0.768
8	Crimen Informático internacional	Fraudes24 Criminales25 Expertos26	0.662
9	Impunidad delictiva informática	Falta13 cometer14	0.738
10	Minimizar Robo de identidad Digital	Peligro4 Preventivos5	0.668
11-17	No significativo	Variables no significativas	Menor de .60

Fuente: Elaboración propia

En base a lo anterior se describen en las partes subsecuentes los ocho (8) factores significativos en términos de confiabilidad y validez individual, como se observa en al Tabla 10, que refiere al Re-Test del alfa de Cronbach, los factores: 1 Incremento y prevención del delito informático (0.745), 2 Tratados Internacionales (0.828), 3 Informática Jurídica (0.815), 4 Castigos legales a delitos informáticos (0.717), 7 Conceptualizar “Robo de identidad Digital” (0.768), 8 Crimen Informático

internacional (0.662), 9 Impunidad delictiva informática (0.738), 10 Minimizar Robo de identidad Digital (0.668), todos con alfa de Cronbach mayor a 0.6 exploratorio con Eigenvalues mayor a uno.

Tabla 6. Incremento y prevención del delito informático

FACTOR 1	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Previene10	.720	90	0	6	4.10	4	1.49	2.75	36%	30	-0.48	2.35	0.05
Delito12	.700	90	0	6	3.76	4	1.42	2.65	38%	29	-0.23	2.41	0.27
Normativas11	.640	90	0	6	4.18	4	1.53	2.73	37%	31	-0.64	2.63	0.04
Influencia39	.503	90	0	6	4.46	5	1.42	3.13	32%	22	-0.86	3.12	0.01

Fuente: Elaboración propia

Como se muestra en la Tabla 6, del Factor 1 que refiere a la prevención del delito informático: Los encuestados consideran que casi siempre (Md=5) la influencia del uso de la computadora ha incrementado el fraude informático (Influencia39), aunque por otra parte están de acuerdo en que muchas veces (Md=4) la utilización de los Instrumentos Digitales Financieros (IDF) por si mismos de manera consciente (Previene10), así como la aplicación de disposiciones legales existentes (Delito12) y la la aplicación de recomendaciones Normativas bancarias (Normativas11) al utilizar dichos instrumentos financieros, previenen el delito informático.

Tabla 7. Tratados Internacionales

FACTOR 2	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Convenios21	.780	89	0	6	3.49	4.00	1.59	2.20	45%	32	-0.42	2.63	0.21
Expertos20	.692	90	0	6	3.41	3.00	1.62	2.10	48%	43	-0.19	2.48	0.42
Convenios19	.633	90	0	6	3.34	3.00	1.57	2.13	47%	43	-0.37	2.55	0.23
Tratados23	.567	90	0	6	3.52	3.00	1.54	2.29	44%	43	-0.15	2.29	0.16

Fuente: Elaboración propia

Como se muestra en la Tabla 7, del factor 2 que refiere a tratados internacionales: Los sujetos entrevistados consideran que muchas veces (Md=4) existe un conjunto de convenios jurídicos internacionales que se llevan a cabo para prevenir el robo de identidad (Convenios21), desarrollados regularmente (Md=3) por expertos internacionales que trabajan en pro de un nuevo orden internacional de los derechos jurídicos contra el delito de robo de identidad (Expertos20), además de que dichos acuerdos y tratados internacionales existen contra el fraude informático (Convenios19) y buscan actualmente contrarrestar el uso indebido de instrumentos digitales financieros (Tratados23).

Tabla 8. Informática Jurídica

FACTOR 3	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Estafa36	.706	90	0	6	3.21	3.00	1.43	2.24	45%	36	-0.03	2.81	0.99
Acciones34	.700	90	0	6	3.30	3.00	1.52	2.16	46%	38	-0.08	2.82	0.95
Internet35	.690	90	0	6	3.36	3.00	1.73	1.94	52%	46	-0.19	2.38	0.26
Procedimientos37	.577	90	0	6	3.29	3.00	1.47	2.24	45%	37	-0.44	3.02	0.19

Fuente: Elaboración propia

Como se observa en la Tabla 8, del factor 3 que refiere a la informática jurídica: Los sujetos muestreados consideran que Regularmente (Md=3) las leyes contrarrestan la estafa informática derivada del uso del internet (Estafa36), ya que además de las acciones judiciales basadas en informática jurídica que evitan la propagación del robo de identidad digital (Acciones34), la computadora (Internet35), y los procedimientos de informática jurídica (Procedimientos37), son herramientas de apoyo que aprovecha el internet para minimizar el robo de identidad digital y en su aplicación evitan el fraude informático

Tabla 9. Castigos legales a delitos informáticos

FACTOR 4	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Proceso22	.657	90	0	6	3.49	3.00	1.62	2.15	47%	44	-0.22	2.4	0.27
Penas40	.603	90	0	6	3.34	3.00	1.31	2.56	39%	31	-0.35	3.56	0.15
Castigos41	.545	90	0	6	3.51	4.00	1.43	2.45	41%	29	-0.16	2.79	0.79

Fuente: Elaboración propia

Como se lee en la Tabla 9, del factor 4 que refiere a Castigos legales a delitos informáticos: Los entrevistados consideran que muchas veces (Md=4) los castigos que ha impuesto la autoridad a quienes cometen delitos informáticos han ido incrementándose (Castigos41) ya que regularmente (Md=3) se observa que al día de hoy se somete a proceso legal y se han establecido penas jurídicas. (Penas40) a un número mayor de aquellas personas que cometen delitos informáticos internacionales (Proceso22) y/o acciones informáticas contrarias a la ley.

Tabla 10. Conceptualizar "Robo de identidad Digital"

FACTOR 7	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Conceptualizar29	.857	90	0	6	3.28	3.00	1.56	2.10	48%	40	-0.33	2.69	0.38
Legislacion28	.590	90	0	6	3.33	4.00	1.56	2.14	47%	31	-0.57	2.87	0.09

Fuente: Elaboración propia

Como se lee en la Tabla 10, del factor 7 que refiere a Conceptualizar "Robo de identidad Digital": Los sujetos entrevistados consideran que muchas veces (Md=4) que la falta de una correcta conceptualización del término "Robo de identidad digital", dificulta su legislación (Legislacion28), de tal manera que limita las propuestas legislativas acertadas que prevengan el fraude informático (Conceptualizar29)

Tabla 11. Crimen Informático internacional

FACTOR 8	Carga	N	Min	Max	Me	Md	DesvSt	Z	COV	COD	SK	K	K2
Fraudes24	.692	90	0	6	4.00	4.00	1.61	2.48	40%	33	-0.5	2.53	0.10
Criminales25	.621	90	0	6	3.62	4.00	1.57	2.31	43%	33	-0.13	2.2	0.07
Expertos26	.534	90	0	6	3.62	4.00	1.50	2.42	41%	36	-0.23	2.47	0.35

Fuente: Elaboración propia

Como se muestra en la Tabla 11, del factor 8 que refiere a Crimen informático internacional: Los sujetos entrevistados consideran que muchas veces (Md=4) los expertos internacionales sobre

crímenes informáticos actualizan sus propuestas de acuerdo a casos de fraude informático que transitan en la red (Expertos26), aunque estos fraudes informáticos internacionales sobrepasan la capacidad de las autoridades mexicanas (Fraudes24) al igual que sobrepasan las capacidades jurídicas de los gobiernos internacionales para contrarrestarlos (Criminales25).

Tabla 12. Impunidad delictiva informática

FACTOR 9	Carga	N	Min	Max	Me	Md	DesSt	Z	COV	COD	SK	K	K2
Falta13	.754	90	0	6	4.28	5.00	1.57	2.73	37%	25	-0.8	2.96	0.01
cometer14	.690	90	0	6	4.02	4.00	1.67	2.41	41%	33	-0.63	2.66	0.04

Fuente: Elaboración propia

Como se observa en la Tabla 12, del factor 9 que refiere a la Impunidad delictiva informática: Donde los sujetos entrevistados consideran que casi siempre (Md=5) existe una falta de legislación que castigue el delito informático (Falta13), lo que permite muchas veces (Md=4) a cualquier persona cometer delitos informáticos (cometer14)

Tabla 13. Minimizar Robo de identidad Digital

FACTOR 10	Carga	N	Min	Max	Me	Md	DesvSt	Z	COV	COD	SK	K	K2
Peligro4	.744	90	0	6	3.34	3.00	1.57	2.14	47%	42	-0.16	2.54	0.56
Preventivos5	.659	90	0	6	3.24	3.00	1.46	2.22	45%	39	-0.39	2.54	0.20

Fuente: Elaboración propia

Como se muestra en la Tabla 13, del factor 10 que refiere a minimizar el robo de identidad Digital: Los sujetos muestreados consideran que regularmente (Md=3) el uso de los Instrumentos Digitales Financieros (IDF) minimiza el peligro de robo de identidad digital (Peligro4), además de ser su uso preventivo contra los llamados robos digitales (Preventivos5).

Conclusiones.

Este trabajo mostro que entre otros factores los que promueven e influyen en el robo de identidad digital son: Por un parte, la falta de un concepto de "Robo de identidad digital" que no se ha definido correctamente en su proceso de actualización constante, lo que conlleva que las propuestas legislativas que prevengan el fraude informático son poco acertadas. En segundo lugar lo anterior provoca la incidencia de una impunidad ante el delito informático derivado de una falta de legislación que lo castigue justamente y que permite que cualquier persona lo pueda cometer. Así mismo, cuándo se habla de crimen Informático internacional encontramos que los expertos internacionales sobre crímenes informáticos actualizan sus propuestas de acuerdo a casos de fraude informático que transitan en la red aunque estos fraudes informáticos internacionales sobrepasan las capacidades jurídicas de los gobiernos internacionales y las autoridades mexicanas para contrarrestarlos y mediante los tratados Internacionales los expertos Internacionales actualmente trabajan en pro de un nuevo orden internacional de los derechos jurídicos contra el robo de

Identidad, de donde surgen acuerdos y tratados que además de contrarrestar dicho robo de identidad, también desarrollan medidas contra el fraude informático y el uso indebido de Instrumentos Digitales Informáticos. De tal manera que los castigos legales a delitos informáticos que ha impuesto la autoridad Mexicana y en base a dichos acuerdos a quienes cometen delitos informáticos han ido incrementándose, ya que se someten a proceso legal y por ende a penas jurídicas a un mayor número de personas que cometen delitos y acciones informáticas contrarias a la ley.

Este estudio también mostro cómo la tecnología influye en la protección de la identidad digital de las personas, ya que a pesar de que se incrementa el delito informático también se previene. En otras palabras, de alguna manera la influencia del uso de la computadora ha incrementado el fraude informático pero el público en general acepta y utiliza los instrumentos digitales financieros en el entendido de que por sí mismos; legal y normativamente protegen y previenen el delito informático y por ende su patrimonio económico. De esta manera la Informática Jurídica, que refiere el establecimiento de leyes que contrarresten el Robo de identidad digital es regularmente necesaria, pero es mejor si se apoya en procedimientos de informática y computadoras como tecnología de sustento para evitar la estafa y/o el fraude informático, con lo cual se logra minimizar robo de identidad digital, con lo que la utilización de Instrumentos digitales financieros minimizan el robo de identidad digital y previene con ello los robos digitales. Lo anterior explica en mucho como mejorar el desempeño de los procesos financieros mediante instrumentos digitales.

Como parte de la conclusión de las relaciones funcionales obtenidas se dice que para mejorar la aplicación y uso de las nuevas tecnologías de la información y comunicación para que modifique la cultura de la prevención del fraude informático se necesita partir de cuatro vertientes:

En primer lugar es más común observar que a nivel internacional se desarrolla una actividad inusitada que busca prevenir el fraude informático, en segundo, a nivel nacional y regional es más común que las instituciones financieras busquen que sus instrumentos digitales financieros por sí mismo limiten el fraude informático y el robo de identidad digital, en tercer lugar, existe mucha confianza en el uso de instrumentos digitales financieros (IDF), a pesar de la existencia de hackers y la alta impunidad al llevar a cabo sus actividades ilícitas y en cuarto lugar existe poco apoyo jurídico y normativo ya que existe un exceso de indefinición de las palabras clave de esta investigación, cada país maneja definiciones diferentes. Por lo tanto, la hipótesis de investigación sobre la existencia de factores que influyen en el robo de identidad digital, quedo debidamente contrastada y corroborada mediante los instrumentos estadísticos aplicados.

Referencias

Aguilar, L. J. (2017). *Ciberseguridad: La colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0)*. Recuperado el día 20 de febrero del 2019 de http://www.dialnet.unirioja.es/descarga/articulo/6115620.pdf

Barba Álvarez, R. (2017). El robo de identidad en México. *Revista de Investigación en Derecho, Criminología y Consultoía Jurídica*. Recuperado el día 24 de marzo del 2019 de http://www .apps.buap.mx/ojs3/index.php/dike/article/view/532

Barrio Andrés, M. (2017). *Ciberdelitos: amenazas criminales del ciberespacio*. Madrid: Editorial Reus.

Garatu, G. (2018). *¿Qué es y qué aporta la Industria 4.0?* Recuperado el 12 julio del 2019 de https: //grupogaratu.com/que-es-y-que-aporta-la-industria-4-0/

Gutiérrez, S. (2018). *Así sacudió a México el ciberataque al sistema financiero*. Recuperado el día 14 de mayo del 2019 de https://www2.deloitte.com/mx/es/pages/dnoticias/articles/ciberataque -sistema-financeiro.html

Gutiérrez, S. (2019). *La Ciberseguridad: tema de negocios.* Recuperado el día 20 de julio del 2019 de https://www2.deloitte.com/mx/es/pages/dnoticias/articles/ciberseguridad-y-negocios.html

Hérnandez Aros, L., Cerquera Suaréz , J. A., y Vanegas Rodríguez , J. A. (2016). Riesgos presentes en los Ciberataques: Un análisis a partir de Herramientas de Auditoria Forense. *Revista pensamiento Republicano*. Recuperado el dia 24 de marzo del 2019 de http://ojs.urepublicana. edu.co/index.php/pensamientorepublicano/article/view/300

Joyanes Aguilar, L. (2017). *Industria 4.0 la cuarta revolución industrial*. México: Alfaomega.

Riquelme, R. (2017). 6 datos sobre la Ciberseguridad en México y el mundo. El economista. Recuperado el día 23 de abril del 2019 de https://www.eleconomista.com.mx /tecnologia/6-datos-sobre-la-ciberseguridad-en-Mexico-y-el-mundo-20170909-0003.html

Robles, E. (2018). *Ciberseguridad en México. ¿Cuáles serán los desafíos del nuevo gobierno?* . Recuperado el día 22 de febrero del 2019 de https://www2.deloitte.com/mx/es/pages/ dnoticias/articles/ciberseguridad-en-mexico.html

Sánchez Canet, F. J. (2016). *Cibercriminalidad: Especial referencia al delito de usurpación y suplantación de identidad*. Recuperado el dia 14 de marzo del 2019 de https://reunir.unir.net/ handle/123456789/4845.

Sánchez Domingo, M. B. (2016). Robo de Identidad personal a través de la manipulación o el acceso ilegítimo a sistemas informáticos, ¿ Necesidad de una tipificación específica? *Revista General de Derecho Pena, Iustel.* Recuperado el día 23 de marzo del 2019 dehttps://www. iustel.com/v2/revistas/detalle_revista.asp?id_noticia=418038

Schwab, K. (2017). *La cuarta revolución industrial. Ciudad de México*, México: Penguin Random House Grupo Editorial S. A. de C. V.

Unión Internacional de Telecomunicaciones. (2015). *Índice mundial de ciberseguridad y perfiles de ciberbienestar*. Recuperado el dia 15 de abril del 2019 de https://www.itu.int/dms_ pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf.