Data and Metadata. 2024; 3:133
doi: 10.56294/dm2024133

ORIGINAL

Technological disinformation: factors and causes of cybernaut identity theft in the digital world

Desinformación tecnológica: factores y causas del robo de identidad del cibernauta en el mundo digital

Gilberto Murillo González[1], German Martínez Prats[2], Verónica Vázquez Vidal[3]

[1]Universidad Juárez Autónoma de Tabasco. México.

Citar como: González GM, Prats GM, Vidal VV. Desinformación tecnológica: factores y causas del robo de identidad del cibernauta en el mundo digital. Data and Metadata 2024; 3:133. https://doi.org/10.56294/dm2023133.

Enviado: 03-09-2023 **Revisado:** 01-11-2023 **Aceptado:** 09-03-2024 **Publicado:** 10-03-2024

Editor: Prof. Dr. Javier González Argote

ABSTRACT

The contribution of technology in the development of our daily activities has taken a giant step in the dependence of the citizen-technology-society with the integration of the Internet without glimpsing a border. It is therefore necessary to safeguard personal information if you have an active digital life. The identification of the factors and causes that lead to identity theft is a requirement for the technical and operational literacy of citizens, who are easy victims. This article aims to analyze some aspects of causes and factors of identity theft of citizens of the municipality of the center of the State of Tabasco. A quantitative instrument was designed, applied via Internet to a population of 3,158. The results show that citizens are unaware of several aspects of security in the environment of digital services, which, depending on gender, age and level of education, are captive in some scenario of digital insecurity.

Keywords: Cybersecurity; Knowledge Society; Digital Ecosystem; Business Intelligence; E-Commerce.

RESUMEN

La contribución de la tecnología en el desarrollo de nuestras actividades cotidianas ha dado un paso gigantesco en la dependencia del ciudadano-tecnología-sociedad con la integración del internet sin vislumbrar una frontera. Es por ello que salvaguardar la información personal si se cuenta con una vida digital activa. La identificación de los factores y causa que propician el robo de identidad se traducen en una exigencia para la culturización técnica y operativa de los ciudadanos, los cuales son víctimas fáciles. El presente articulo pretende analizar algunos aspectos de causas y factores del robo de identidad de los ciudadanos del municipio del centro del Estado de Tabasco. Se diseñó un instrumento cuantitativo, aplicado vía Internet a una población de 3,158. Los resultados muestran que los ciudadanos desconocen varios de los aspectos de seguridad en el entorno de los servicios digitales, los cuales, dependiendo del género, edad y nivel de estudio, son cautivos en algún escenario de inseguridad digital.

Palabras clave: Ciberseguridad; Sociedad del Conocimiento; Ecosistema Digital; Inteligencia del Negocio; Comercio Electrónico.

INTRODUCCIÓN

El uso del internet cada día es más una exigencia social. Desde este enfoque y su rápida penetración en las actividades cotidianas permiten visualizarlo como un perfecto aliado para la transformación de diversas tareas que día a día se desempeñan.(1)

La historia del internet se remonta a la década de 1960, cuando el Departamento de Defensa de los Estados

Unidos desarrolló una red llamada ARPANET para conectar computadoras en diferentes ubicaciones y permitir la comunicación entre ellas. A medida que la tecnología avanzaba, ARPANET evolucionó en lo que hoy conocemos como internet.

El robo de identidad, por otro lado, es un problema relativamente reciente que se ha intensificado con el aumento del uso de internet y la digitalización de la información personal. El robo de identidad se refiere a la apropiación ilegal de la identidad de otra persona, ya sea para cometer fraudes financieros o para otro tipo de delitos.[2]

En los primeros días de internet, el robo de identidad no era un problema tan grande debido a que la información personal no se compartía en línea con tanta frecuencia. Sin embargo, a medida que el comercio electrónico y las redes sociales se popularizaron, el robo de identidad se convirtió en un problema cada vez más común.[2,3]

Los ladrones de identidad pueden utilizar una variedad de técnicas para obtener información personal, como phishing, virus informáticos, campañas motivadoras por correo electrónicos y ataques de ingeniería social. Con la información personal de una víctima, a través del ciberespacio se pueden abrir cuentas bancarias, solicitar tarjetas de crédito o incluso cometer delitos en nombre de la víctima, lo que transforma el escenario digital en un entorno de alto cuidado.[4]

Estos fenómenos técnicos y poco visibles para la sociedad y en particular para los grupos de población que empiezan a interactuar con los servicios digitales, son altamente vulnerables. El reflejo del uso de las tecnologías digitales durante el periodo de mayor confinamiento en la pandemia del Covid-19, desbordo el uso de estos servicios y también incremento los padecimientos tecnológicos por el uso de la red sin los mínimos cuidado requeridos.

De acuerdo con la empresa Avast, la desinformación tecnológica y el robo de identidad están relacionados, ya que la falta de conocimiento sobre seguridad en línea puede hacer que los usuarios sean más vulnerables al robo de identidad. Esto es uno de los elementos que contribuyen y aceleran el robo de identidad en los diversos grupos en la población mundial. En México de acuerdo con estudios establecidos por el Instituto Nacional de Estadística y Geografía (INEGI), en su Encuesta Nacional de victimización de Empresas 2022 (ENVE), se contempla un incremento del 0,5 %, de este delito que contempla elementos como: ataques a redes, servidores o sistemas informáticos, entre otros factores.[5] En años anteriores y en específico en los años de mayor impacto de la pandemia, estos elementos tenían una tasa de incidencia del 1,8 %.[5,6]

La desinformación tecnológica se refiere a la propagación de información errónea o engañosa sobre tecnología y seguridad en línea. Esto puede incluir consejos falsos sobre cómo proteger su información personal o cómo evitar el robo de identidad. La desinformación también puede incluir noticias falsas o engañosas que se propagan en línea, lo que puede llevar a las personas a tomar decisiones basadas en información incorrecta.[7]

Los factores del robo de identidad pueden incluir una variedad de aspectos, como la falta de medidas de seguridad adecuadas en los sitios web y aplicaciones, la falta de conciencia de los usuarios sobre cómo proteger su información personal, el uso de contraseñas débiles y la exposición accidental de información personal. Cuando los usuarios no tienen suficiente información sobre cómo proteger su información personal en línea, son más propensos a tomar decisiones que los ponen en riesgo de robo de identidad. Uno de los escenarios más comunes donde se violenta este estado de seguridad es a través del uso del correo electrónico el cual muchas veces, invita a abrir o descargar archivos adjuntos que contienen programas informáticos malicioso o mejor conocidos como virus informáticos.[8]

Sin duda alguna, el entorno social y digital actual son de mucha importancia y beneficio, pero contienen varios aspectos que dañan y violentan, los aspectos de integridad de los usuarios.

Revisión documental

¿Qué es un robo de identidad en internet?

El robo de identidad en internet se refiere a la apropiación ilegal de la identidad de otra persona en línea, la cual sirve para cometer fraudes financieros u otro tipo de delitos. A través de diversos instrumentos los delincuentes informáticos pueden obtener información altamente valiosa de las víctimas utilizando aspectos como el phishing, virus informáticos y la ingeniería social.[4]

Esta práctica invasiva trae graves consecuencias para las víctimas y los cibernautas, la cual incluye la pérdida de su perfil, reputación, dinero, crédito y aspectos sociales y financiero para ellos y su círculo más cercano. Sin duda alguna, este tipo de experiencias nublan la gran utilidad que brindan los servicios digitales, lo que se traduciría para el usuario final en un proceso largo y complicado para recuperar su identidad robada y resolver los problemas financieros y legales que surgen de esta mala práctica.

¿Qué es la Ciberseguridad?

La ciberseguridad es el conjunto de medidas, tecnologías y prácticas diseñadas para proteger los sistemas informáticos, dispositivos conectados a internet y redes de ataques malintencionados y amenazas cibernéticas.

[5] El objetivo de la ciberseguridad es proteger la información confidencial y los recursos críticos de una organización o individuo, incluyendo datos personales, financieros, comerciales y gubernamentales.[6]

La ciberseguridad incluye diversas áreas de protección, tales como:

- La seguridad de la información: protección de datos, privacidad, confidencialidad y cumplimiento normativo.
- La seguridad de los sistemas: protección de la infraestructura de TI y los sistemas de información, incluyendo servidores, dispositivos de red, bases de datos y software.
- La seguridad de las redes: protección de la conectividad y comunicación entre los dispositivos y sistemas, incluyendo el control de acceso, la segmentación de redes, la detección y prevención de intrusiones, y el monitoreo de la red.
- La seguridad física: protección de los recursos físicos y la infraestructura de TI, incluyendo los centros de datos, los dispositivos de almacenamiento y los dispositivos móviles.
- La ciberseguridad se ha vuelto cada vez más importante en el mundo actual, ya que las amenazas cibernéticas están en constante evolución y se han vuelto más sofisticadas y peligrosas. Las organizaciones y los individuos deben tomar medidas de seguridad en línea adecuadas para protegerse contra las amenazas y asegurar la privacidad y seguridad de su información.

Leyes que se aplican para el robo de identidad en internet y México

Desde una perspectiva jurídica, muchos de los aspectos normativo para los servicios que se están generando en el Internet son relativamente nuevos, algunas de estas leyes que se aplican al robo de identidad en internet varían según el país y la jurisdicción.[7] En general, los delitos de robo de identidad en línea pueden estar cubiertos por leyes que se enfocan en la privacidad, el fraude, el robo de propiedad intelectual, el ciberacoso y otros delitos informáticos y varios factores más.

En los Estados Unidos, se contempla la Ley de Fraude y Abuso Informático (Computer Fraud and Abuse Act) y la Ley de Identificación Falsa en Línea (Online Identity Theft Act) son leyes federales que se ocupan de los delitos informáticos, incluyendo el robo de identidad en línea.[9,10] Además, muchos estados tienen leyes específicas que abordan el robo de identidad en línea y otras formas de fraude en línea.[11]

En la Unión Europea, el Reglamento General de Protección de Datos (RGPD) establece las normas para la protección de la privacidad y la información personal en línea. Además, la Directiva de la UE sobre delitos informáticos y la Convención del Consejo de Europa sobre Cibercrimen establecen normas y medidas para combatir el cibercrimen en general, incluyendo el robo de identidad en línea.[12]

En otros países, las leyes pueden variar y pueden ser menos específicas en cuanto a delitos informáticos y robo de identidad en línea. En cualquier caso, es importante que las víctimas de robo de identidad en línea informen el delito a las autoridades y busquen asesoramiento legal para proteger sus derechos y recuperarse de los daños causados.[11,12]

En México, el robo de identidad en internet está tipificado como un delito en el Código Penal Federal, específicamente en el artículo 210 Bis. Además del Código Penal Federal, en México existen otras leyes que se aplican al robo de identidad en internet, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que regula la forma en que las empresas y organizaciones deben manejar los datos personales de los ciudadanos. Del mismo modo existe la Ley de Instituciones de Crédito, que establece medidas de seguridad para la protección de la información financiera de los usuarios de los servicios bancarios. [13]

En lo que respecta a que instancia gubernamental es la responsable de la investigación y sanción de los delitos de robo de identidad en internet, en México es la Fiscalía Especializada en Delitos Cibernéticos.[14]

Cabe destacar que este tipo de leyes y regularizaciones, en materia de tecnologías se encuentran en un proceso de actualización constante y sobre todo en los aspectos de robo de identidad, ciberataques, robo de información, extorsión electrónica, ciberacoso y entre otros, los cuales son escenarios altamente cambiantes y la necesidad de contar con marcos normativos y regulatorios actualizados son cada día una exigencia local, estatal y nacional.[12,13,14]

El impacto del robo de identidad en México y Tabasco

Contexto Nacional

El robo de identidad en México es un problema importante. A continuación, se analizan algunos datos estadísticos sobre el robo de identidad en México:

De acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), en México se registraron 62 684 reclamaciones por robo de identidad en el primer semestre de 2020, factores que fueron incrementándose al realizar más tramites y servicios en línea, producto de compras electrónicas, pago de servicios o cargos no reconocidos, entre otras. Por otro lado, bajo los mismos aspecto de la ciberdelincuencia, la Asociación de Bancos de México (ABM) reportó que, durante el primer semestre de 2020, se detectaron más de 6 millones de intentos de fraude cibernético, lo que representa un aumento del

84 % en comparación con el mismo periodo del año anterior, es decir, algunos aspectos de la pandemia y el confinamiento provocaron el mayor uso de las compras y operaciones del dinero electrónico, presentándose mayores incidentes en los robos en línea sin precedente alguno.[15]

Según un informe del estudio Panorama de Amenazas de la empresa de seguridad informática Kaspersky, México, es el segundo país de Latinoamérica con más ataques de phishing (suplantación de identidad) en el primer trimestre de 2021, con el 13,5 % del total de ataques en la región.[16] De acuerdo con el Estudio, la mayoría de los ataques informáticos son dirigidos hacia los dispositivos móviles, los cuales han tenido un crecimiento exponencial gigantesco.[17]

Es importante destacar que estas cifras probablemente no reflejen la totalidad de los casos de robo de identidad en México, ya que muchas personas pueden no reportar los delitos por diversas razones, como la falta de confianza en las autoridades o la falta de conocimiento sobre los procesos de denuncia.[18]

Contexto Estatal

Los delitos cibernéticos van en aumento, para el Estado de Tabasco es un factor de interés, debido a los entornos complejos en donde se encuentran. No solo en el robo de identidad, sino en aquellos otros delitos que en el orden del ecosistema digital pudieran a parecer, como resultado del desconocimiento de las fronteras y normas del entorno digital.[19] De acuerdo con los indicadores proporcionados por la Fiscalía General del Estado de Tabasco, en su informó anual del 2020, se registraron alrededor de 400 denuncias por delitos informáticos, incluyendo el robo de identidad. En el 2019, la Asociación de Bancos de México (ABM) reportó que Tabasco se encontraba entre las 10 entidades con mayor número de casos de fraude cibernético. Lo cual indica que durante el periodo de mayor uso de la tecnología producto del confinamiento en la entidad, los usuarios expusieron más sus datos personales, financieros, para la resolución de diversas actividades cotidianas por medio de los servicios digitales.[17,18,19]

Una de las instancias gubernamentales con funciones de seguimiento relacionado con las actividades del ciberespacio, es la Fiscalía Especializada en Delitos Cibernéticos del Estado de Tabasco, informó que, en el primer semestre del año 2021, se registraron alrededor de 180 denuncias por delitos informáticos, incluyendo el robo de identidad.[19]

Sectores vulnerables

En México, todas las personas que utilizan dispositivos conectados a Internet y realizan transacciones en línea, pueden ser vulnerables al robo de identidad cibernético. [20] Sin embargo, algunos sectores de la población pueden ser considerados más vulnerables debido a diversas razones, como su nivel de conocimiento sobre seguridad en línea, su nivel socioeconómico o su grado de exposición a situaciones de riesgo.[11,13] Algunos de los sectores de la población que pueden considerarse más vulnerables son:

- Personas mayores: Debido a que algunas personas mayores pueden tener menos conocimiento sobre las tecnologías en línea, pueden ser más propensas a caer en trampas o engaños en línea, lo que puede poner su información personal en riesgo.
- Niños y adolescentes: Algunos niños y adolescentes pueden ser vulnerables al robo de identidad cibernético debido a que pueden compartir información personal en línea de manera irresponsable, sin entender completamente los riesgos asociados.
- Personas con bajos ingresos: Algunas personas con bajos ingresos pueden ser más vulnerables al robo de identidad cibernético debido a que pueden ser menos propensas a invertir en tecnologías de seguridad en línea, como software antivirus o servicios de monitoreo de crédito.
- Personas que realizan transacciones financieras en línea: Las personas que realizan transacciones financieras en línea, como compras en línea o transferencias bancarias, pueden ser más vulnerables al robo de identidad cibernético, ya que esta información es altamente valiosa para los delincuentes cibernéticos.
- Empresas pequeñas: Las empresas pequeñas pueden ser vulnerables al robo de identidad cibernético debido a que pueden tener menos recursos para invertir en tecnologías de seguridad en línea y pueden ser un objetivo más fácil para los delincuentes cibernéticos que buscan obtener información personal de varios clientes a la vez.

Actualmente son pocos los estudios o análisis del impacto de la inseguridad cibernética en México, así como la identificación de las regiones, zonas, y grupos de mayores riesgos en ser víctimas del robo de identidad o de algún otro delito informático. Contar con dicho estudio, no solo aportaría homogeneidad para Identificar los factores, causas y efectos, de los robos cibernéticos en el mundo digital, sino que, además, aportaría una clasificación, que contribuiría a aumentar las estrategias de alfabetización digital y cultura informática en la sociedad moderna actual.

El objetivo de la presente investigación es identificar factores y causas de la inseguridad informática, que son un detonante en la sensibilización educativa, tecnológica y social, necesaria para fortalecer las estrategias

para una culturización informática, asociación a una mejor experiencia digital.

MÉTODOS

La presente investigación tiene como fundamento el enfoque descriptivo observacional, lo cual permite tener una interpretación de las variables de estudio sin alterar el contexto de su entorno. El objetivo específico de la investigación se concentra en conocer e identificar algunos factores y causa que propicien el robo de identidad electrónica, su relación con aspectos sociodemográficos y la interpretación de los instrumentos de lucha en contra de este fenómeno digital.

El alcance metodológico de la presente investigación se sustenta en la aplicación de una encuesta sobre el mismo medio electrónico, utilizando una de las herramientas de encuestas en línea, como lo es Onlineencuesta.com. El seguimiento de la recopilación de los datos se hizo a partir de la publicación del instrumento el día 17 de marzo de 2022 y concluyo el 28 de noviembre del mismo año, a través de los diversos canales de comunicación sociales y educativas para la integración de la muestra, la cual quedó conformada por 3158, ciudadanos del estado de Tabasco. El análisis y estudio de los datos de la encuesta se realizó a través de la herramienta Power Bi versión 2.112

Dentro del presente estudio se determinaron dos variables independientes, las cuales, incluyen un determinado número de ítems, con la finalidad de poder interpretar los elementos esenciales para la definición de los objetivos de la investigación. La primera variable independiente se encuentra conformado por los siguientes aspectos. *¿Qué efectos de inseguridad informática perciben los ciudadanos del municipio del Centro del Estado de Tabasco, en el uso de los servicios digitales que se ofertan para sus actividades cotidianas a través del internet?*

El compendio de secciones que integran a esta variable independiente son 6, las cuales, se describen:

a) He sufrido de alguna compra no reconocido en los últimos 6 meses,
b) Me han hecho llamadas fraudulentas para acceder a mis datos bancarios,
c) Me han hecho dudar en mis datos personales en el ciberespacio,
d) Me han robado mi contraseña de acceso a mis redes sociales, correo electrónico y cuentas bancarias en los últimos 6 meses,
e) He creído en los correos, mensajes de texto o campañas de difusión de sorteos y premios que soy ganador durante la pandemia del COVID-19,
f) Me han llamado en atención al banco para proteger mis datos durante la pandemia del covid-19.

En el análisis de la segunda variable independiente se encuentra integrada por los *elementos que permiten reducir el riesgo de incidente de inseguridad informática*. Este apartado se encuentra integrado por 3 secciones, las cuales, se describen a continuación:

a) Me siento seguro en realizar operación en Internet y sentirme respaldado por la ley y normas políticas del banco,
b) Me han hecho darme cuenta por medio de campañas en diferentes medios de la importancia de cuidar mis datos personales en el internet, y
c) Me han hecho sentir seguro en la realización de transacciones en línea y en NO creer en esas noticias falsas.

De igual forma se incluyen 3 variables del contexto sociodemográfico que permitan dimensionar el impacto de los datos. Estas variables son:

a) Genero el cual está dividido en dos categorías,
b) Edad, la cual se encuentra integrada por grupos de edad, tales como de 18 – 29, 30-49. 50-60 y 60+ y
c) Grado escolar, la cual se encuentra integrada por tres grandes grupos, Sin estudios, Estudios básicos y profesionales.

RESULTDOS

En el análisis establecido a partir del modelo metodológico, se interpretaron los datos que fueron obtenidos en el instrumento, los cuales muestran aspectos relevantes de los ciudadanos del municipio del centro del Estado de Tabasco, estos perciben a la desinformación tecnológica como un elemento de mucha importancia y de alto nivel de complejidad para el desarrollo de sus actividades cotidianas. En las primeras secciones del instrumento reflejan que muchos han sido víctimas de algún tipo de suceso o experiencia de inseguridad informática. Esto igual permite visualizar, que para muchos ciudadanos el impacto de la inseguridad tecnológica lo visualizan como malas experiencias o actividades que no se deben de realizar en línea sino a través de los medios tradicionales, provocando con ello el aumento de la brecha digital en el uso del comercio electrónico y de servicios digitales y de pagos a través del internet.

Otro de los aspectos relevante de estas secciones, es que el ciudadano determina que muchos de los factores, eventos o sucesos que en el Internet son altamente creíbles y de confianza, lo que permite tener experiencias de aceptación en campañas vía correo electrónico, mensajería instantánea que son fuente

constante de archivos maliciosos para la obtención de información de los cibernautas. En la tabla 1, se muestra los resultados del análisis de las dos variables independientes y sus respectivas secciones, donde se describen de forma general, los factores con mayor recurrencia en el robo de información y de identidad en el internet.

Tabla 1. Factores de la inseguridad y elementos de reducción de riesgo informático

	Items	Porcentaje de por sección
Análisis de las 6 secciones de la primera variable independiente:		
He sufrido de alguna compra no reconocido en los últimos 6 meses	476	15 %
Me han hecho llamadas fraudulentas para acceder a mis datos bancarios	440	14 %
Me han hecho dudar en mis datos personales en el ciberespacio	475	15 %
Me han robado mi contraseña de acceso a mis redes sociales, correo electrónico y cuentas bancarias en los últimos 6 meses	501	16 %
He creído en los correos, mensajes de texto o campañas de difusión de sorteos y premios que soy ganador durante la pandemia del COVID-19	401	13 %
Me han llamado en atención al banco para proteger mis datos durante la pandemia del covid-19	175	6 %
Análisis de las 3 secciones de la segunda variable independiente:		
Me siento seguro en realizar operación en Internet y sentirme respaldado por la ley y normas políticas del banco	165	5 %
Me han hecho darme cuenta por medio de campañas en diferentes medios de la importancia de cuidar mis datos personales en el internet	250	8 %
Me han hecho sentir seguro en la realización de transacciones en línea y en NO creer en esas noticias falsas	275	9 %
Total	3158	100 %

De igual forma, en esta integración de secciones se pueden definir varios factores que permiten contrarrestar estas malas prácticas en el uso de los servicios electrónicos, como son el conocimiento de los marcos normativos existentes, la difusión y apoyo que ofrecen instancias gubernamentales y privadas para la orientación y manejo de los datos personales, bancarios que se deben de tener al momento de realizar cualquier operación o transacción en línea. Sin duda alguna a pesar de que existen campañas y normas que permiten establecer un marco regulatorio en el uso y no uso del servicio tecnológico, los factores de confianza y de poco interés en establecer nuevas y mejores condiciones de uso de los servicios en línea, son fenómenos que muy poca tasa de reducción se ha tenido en los últimos años.

Algunos de estos fenómenos sociales, pueden estar estrechamente ligados al contexto de la alfabetización digital, que si bien es cierto es parte de las acciones de esta sociedad del conocimiento, también se vuelve parte de esta desigualdad colectiva, la cual es usada para violentar el buen servicio digital que existen en esta modernización social en la cual estamos inmersos.

Tabla 2. Factores de inseguridad informática y su interpretación por Género

Análisis de las 6 secciones de la primera variable independiente y su interpretación con el Género							
He sufrido de alguna compra no reconocido en los últimos 6 meses							
Sección 1	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	476	15 %	243	51 %	233	49 %	476
Me han hecho llamadas fraudulentas para acceder a mis datos bancarios							
Sección 2	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	440	14 %	201	46 %	239	54 %	440
Me han hecho dudar en mis datos personales en el ciberespacio							
Sección 3	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	475	15 %	240	51 %	235	49 %	475
Me han robado mi contraseña de acceso a mis redes sociales, correo electrónico y cuentas bancarias en los últimos 6 meses							
Sección 4	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	501	16 %	334	67 %	167	33 %	501

https://doi.org/10.56294/dm2023133

He creído en los correos, mensajes de texto o campañas de difusión de sorteos y premios que soy ganador durante la pandemia del COVID-19							
Sección 5	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	401	13 %	236	59 %	165	41 %	401
Me han llamado en atención al banco para proteger mis datos durante la pandemia del covid-19							
Sección 6	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	175	6 %	98	56 %	77	44 %	175
Análisis de las 3 secciones de la segunda variable independiente y su interpretación con el Género							
Me siento seguro en realizar operación en Internet y sentirme respaldado por la ley y normas políticas del banco							
Sección 1	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	165	5 %	83	50 %	82	50 %	165
Me han hecho darme cuenta por medio de campañas en diferentes medios de la importancia de cuidar mis datos personales en el internet							
Sección 2	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	250	8 %	130	52 %	120	48 %	250
Me han hecho sentir seguro en la realización de transacciones en línea y en NO creer en esas noticias falsas							
Sección 3	Items	Porcentaje de hombres	Hombre	Porcentaje de mujeres	Mujer	Porcentaje de por sección	Total
Resultados	275	9 %	135	49 %	140	51 %	275
Total	3158	100 %	1700	54 %	1458	46 %	3158

Al introducir al universo de datos la variable de género, se puede percibir que los hombres consideran haber tenido mayor experiencias y casos en los temas de la inseguridad informática, dotando a partir de ello elementos como alteración en compras en línea, extorsiones electrónicas producto de virus informáticos, robo de cuentas en redes sociales, clonación de tarjetas de crédito y débito, así como robo de perfil en mensajería instantánea, utilizadas para solicitar recursos económicos a sus contactos. Otro de los elementos identificados es lo endeble que son las contraseñas electrónicas que los ciudadanos utilizan, mismas que carecen de ciertos criterios y reglas de uso.

En lo que respecta al género femenino, la concientización en el uso de los servicios digitales es mucho más alta y con mejores criterios de uso, atenuando con ello el seguir de mejor manera las recomendaciones y reglas para usar y operar en el ámbito digital y sus servicios. En la Tabla 2, se describe los porcentajes general que permite realizar una mejor interpretación del impacto de los factores de inseguridad a nivel género.

Bajo estos aspectos también se logra describir que en ambos géneros si existen mayores procesos, normas y políticas que coadyuben para la reducción de los factores de riesgos existentes en el ámbito del internet, así como la participación de los diversos sectores públicos y privados en establecer una estrategia constante de difusión en el uso de los servicios digitales.

Tabla 3. Factores de inseguridad informática y su interpretación por rango de edades

	Items	**% de por sección**	**De 18 a 29 años**		**De 30 a 49 años**		**De 50 a 64 años**		**Mas de 65 años**	
He sufrido de alguna compra no reconocido en los últimos 6 meses	476	15 %	121	25 %	56	12 %	111	23 %	188	39 %
Me han hecho llamadas fraudulentas para acceder a mis datos bancarios	440	14 %	100	23 %	94	21 %	68	15 %	178	40 %
Me han hecho dudar en mis datos personales en el ciberespacio	475	15 %	97	20 %	70	15 %	141	30 %	167	35 %
Me han robado mi contraseña de acceso a mis redes sociales, correo electrónico y cuentas bancarias en los últimos 6 meses	501	16 %	42	8 %	145	29 %	113	23 %	201	40 %
He creído en los correos, mensajes de texto o campañas de difusión de sorteos y premios que soy ganador durante la pandemia del COVID-19	401	13 %	35	9 %	33	8 %	167	42 %	166	41 %
Me han llamado en atención al banco para proteger mis datos durante la pandemia del covid-19	175	6 %	38	22 %	40	23 %	47	27 %	45	26 %

https://doi.org/10.56294/dm2023133

Me siento seguro en realizar operación en Internet y sentirme respaldado por la ley y normas políticas del banco	165	5 %	67	41 %	52	32 %	34	21 %	12	7 %
Me han hecho darme cuenta por medio de campañas en diferentes medios de la importancia de cuidar mis datos personales en el internet	250	8 %	59	24 %	78	31 %	70	28 %	43	17 %
Me han hecho sentir seguro en la realización de transacciones en línea y en NO creer en esas noticias falsas	275	9 %	102	37 %	91	33 %	70	25 %	12	4 %
Total	3158	100 %	661	21 %	659	21 %	821	26 %	1012	32 %

Desde un enfoque generacional, al introducir la variable de edad en el universo de estudio, podemos visualizar que los aspectos de inseguridad informática se pueden presentar a cualquier rango de edad, lo que permite también interpretar que a partir de la experiencia vivida en la pandemia del Covid-19, la integración de servicios y recursos digitales tuvieron un amplio crecimiento, así como una alta demanda en ciudadanos mayores de 50 años, los cuales muchos incursionaban en el ámbito de los servicios de internet por primera vez, siendo ellos víctimas fácil para el robo o perdida de información digital.

Con estos elementos de edad, el desempeño tecnológico de las nuevas generaciones no las exenta de vivir experiencias de incidencia en el ámbito del internet, de acuerdo con los datos al mayor uso de los servicio se incrementa el riesgo de sufrir alguna incidencia delictiva, por ello el conocimiento tecnológico y del entorno digital, fomenta en las generaciones de 18+ hasta los 50 años de edad, mayor cultura del uso de la tecnologías así como mejores normas, procedimientos e instrumentos tecnológico que permitan evitar el robo de datos electrónicos. En la tabla 3 se muestran algunos de esto criterios técnicos reflejado en la aportación de acciones en donde se identifican los ciudadanos de la entidad.

Desde la interpretación de las diversas variables sociodemográfico, podemos resaltar la relacionada con la interpretación del nivel de estudio, descrita en los datos recolectado en el instrumento e integrados en la Tabla 4. La cual permite establecer, en apego a los datos revisado que la experiencia de factores de inseguridad en el internet no se encuentra estrechamente ligada a la preparación profesional. Esto permite visualizar que dicha actividad de inseguridad puede ser víctima cualquier persona que interactúe con los servicios digitales que se oferten en el ciberespacio.

Desde este enfoque los ciudadanos del municipio del centro integrado con la falta de estudio y estudios académicos básico, contempla tener mayores experiencias en el robo de identidad y sus diversos factores, sin embargo, los profesionistas igual cumplen con este tipo de experiencias a partir de no contar con reglas y proceso de seguridad claro al momento de efectuar transacciones en el universo del internet.

Tabla 4. Factores de inseguridad informática y su interpretación por nivel de estudios

	Items	**% de por sección**	**Sin estudios académicos**		**Estudios académicos básicos**		**Estudios profesionales**	
He sufrido de alguna compra no reconocido en los últimos 6 meses	476	15 %	189	40 %	176	37 %	111	23 %
Me han hecho llamadas fraudulentas para acceder a mis datos bancarios	440	14 %	176	40 %	196	45 %	68	15 %
Me han hecho dudar en mis datos personales en el ciberespacio	475	15 %	153	32 %	181	38 %	141	30 %
Me han robado mi contraseña de acceso a mis redes sociales, correo electrónico y cuentas bancarias en los últimos 6 meses	501	16 %	230	46 %	160	32 %	111	22 %
He creído en los correos, mensajes de texto o campañas de difusión de sorteos y premios que soy ganador durante la pandemia del COVID-19	401	13 %	144	36 %	117	29 %	140	35 %
Me han llamado en atención al banco para proteger mis datos durante la pandemia del covid-19	175	6 %	78	45 %	50	29 %	47	27 %
Me siento seguro en realizar operación en Internet y sentirme respaldado por la ley y normas políticas del banco	165	5 %	67	41 %	52	32 %	46	28 %
Me han hecho darme cuenta por medio de campañas en diferentes medios de la importancia de cuidar mis datos personales en el internet	250	8 %	59	24 %	70	28 %	121	48 %
Me han hecho sentir seguro en la realización de transacciones en línea y en NO creer en esas noticias falsas	275	9 %	80	29 %	93	34 %	102	37 %
Total	3158	100 %	1176	37 %	1095	35 %	887	28 %

https://doi.org/10.56294/dm2023133

CONCLUSIÓN

Hablar hoy en día de información, comercio electrónico, vida digital y otros aspectos relacionados al uso del entorno digital, debemos de visualizar lo correspondiente a la desinformación tecnológica, la cual podemos describirla como un fenómeno complejo que puede tener múltiples factores y causas. En el desarrollo de la presente investigación se detectaron algunos factores que los ciudadanos del municipio del centro propician para continuar fomentando la desinformación tecnológica:

a) La rapidez y aseverada interpretación de acciones relacionadas con la información producto del gran impacto de la era digital presente en la vida cotidiana, promueve acciones engañosas o false que potencialmente son usadas para el robo de identidad o en algunos casos, promueva el intercambio de información altamente sensible para fines ajenos al dueño de los datos.
b) La falta de verificación de la información, de sitios y portales web, correos electrónicos, mensajes de textos o audios, o llamadas telefónicas, que muchas veces se presenta de forma convincente pueden ser difícil de distinguir su legitimidad. El ciudadano puede tener dificultadas para verificar la veracidad de la información antes de desconfiar de los datos presentado. En algunos aspectos de la investigación se identificaron mucha estrategia de ingeniería social aplicada a los ciudadanos para extraer información relevante y sensible para ser extorsionado a partir de medios electrónicos.
c) Otro de los aspectos de la desinformación tecnológica puede ser generada y difundida intencionalmente para influir en la opinión pública, promover agendas políticas o económicas, o simplemente causar confusión. Los actores malintencionados pueden aprovecharse de elementos culturales y de formación académico para motivar a las personas para difundir información falsa y manipular la percepción pública.
d) Sin duda otro de los factores altamente identificados es la falta de alfabetización mediática y tecnológica la cual contribuye desde la perspectiva del conocimientos y habilidades para evaluar críticamente la información en línea puede contribuir a la propagación de la desinformación tecnológica. La alfabetización mediática y tecnológica es fundamental para ayudar a las personas a discernir entre información verdadera y falsa. Este factor se observó plenamente dentro de la interpretación de los datos, la cual factores de edad y conocimiento son una ecuación ideal para ser víctima de los procesos de robo de identidad.
e) A partir de la comprensión del entorno, podemos determinar que otros de los factores y causas para el robo de identidad es la polarización y fragmentación de la sociedad, la cual puede motivar a un ambiente propicio para la desinformación y en esa búsqueda otorgar información altamente sensible que ponga en riesgo la seguridad, física y electrónica de los ciudadanos a partir de información proporcionada o sustraída.

Por último, la ciberseguridad es altamente importante en nuestros tiempos, en lo vivido en la pasada pandemia y la acelerada dependencia a las tecnologías de la información digital en todas las áreas de nuestra vida y sociedad. Debemos de profundizar en la protección de datos personales, prevenir mediante instrumentos y procedimientos técnicos y operativos ataques cibernéticos, virus informáticos, salvaguardar nuestras proceso de comunicación y actualizar periódicamente nuestras nip, contraseñas e instaurar nuevos mecanismos de seguridad vía modelos de autenticación de dos pasos, así como la inclusión de encriptamiento de la información que procesamos día a día, en nuestros diversos equipos de cómputo o dispositivos móviles.

Estos factores y causas interactúan entre sí y pueden variar en diferentes contextos y situaciones. Abordar la desinformación tecnológica requiere un enfoque multifacético que incluya la educación, la promoción de la alfabetización mediática, la responsabilidad de las plataformas en línea y la participación de los usuarios en la verificación y difusión de información precisa.

REFERENCIAS

1. Araujo BS. Transformación Digital en la Administración Pública: 5 Tecnologías Esenciales [Internet]. Blog SYDLE. SYDLE; 2022 [citado el 15 de enero de 2024]. Disponible en: https://www.sydle.com/es/blog/transformacion-digital-en-la-administracion-publica-62a9e7ad73f2f35ffe1290e2

2. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Mantente alerta ante el Robo de Identidad [Internet]. gob.mx. [citado el 15 de enero de 2024]. Disponible en: https://www.gob.mx/condusef/prensa/mantente-alerta-ante-el-robo-de-identidad-274562?idiom=es.

3. Arévalo-Cordovilla, F. E., Ordoñez-Sigcho, I. B., Peñaherrera-Larenas, M. F., & Suárez-Matamoros, V. J. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. Dominio De Las Ciencias, 6(2), 835–846. https://doi.org/10.23857/dc.v6i2.1197

4. Lucuy P, Andrés K. Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación

móvil para concientizar sobre los Impactos en los Activos. Fides Et Ratio [Internet]. 2021 [citado el 15 de enero de 2024];21(21):143–72. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2021000100009

5. Instituto Nacional de Estadística y Geografía. Encuesta Nacional de Victimización de Empresas (ENVE) 2022.

6. Instituto Nacional de Estadística y Geografía. Encuesta Nacional de Seguridad Pública Urbana (ENSU).

7. Ramirez S, Maria E. ARTÍCULO CIENTÍFICO: "Factores que inciden en la seguridad informática y aplicabilidad en el Cloud Computing de las empresas del sector industrial en la ciudad de Manta, Provincia de Manabí". 2018 [citado el 15 de enero de 2024]; Disponible en: http://biblioteca.uteg.edu.ec:8080/handle/123456789/241?locale-attribute=en

8. Auza-Santivañez JC, Lopez-Quispe AG, Carías A, Huanca BA, Remón AS, Condo-Gutierrez AR, et al. Improvements in functionality and quality of life after aquatic therapy in stroke survivors. AG Salud 2023;1:15-15.

9. Castillo-González W. Kinesthetic treatment on stiffness, quality of life and functional independence in patients with rheumatoid arthritis. AG Salud 2023;1:20-20.

10. Quiroga G, Bolívar C. Guía de análisis de brechas de seguridad para entornos de hipervisores. Quito, Ecuador: Universidad Tecnológica Israel; 2023.

11. La Ley de Fraude y Abuso Informático de 1986 [Internet]. CaseGuard. CaseGuard Video Redaction Software; 2022 [citado el 15 de enero de 2024]. Disponible en: https://caseguard.com/es/articles/la-ley-de-fraude-y-abuso-informatico-de-1986/

12. Pino DRSA. Delitos Informáticos: Generalidades [Internet]. Oas.org. [citado el 15 de enero de 2024]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

13. Mayer Lux L, Oliver Calderón G. El delito de fraude informático: concepto y delimitación. Rev Chil Derecho Tecnol [Internet]. 2020 [citado el 15 de enero de 2024];9(1):151. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

14. La protección de datos en la UE [Internet]. Comisión Europea. [citado el 15 de enero de 2024]. Disponible en: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

15. Hernández-Flórez N. Breaking stereotypes: "a philosophical reflection on women criminals from a gender perspective". AG Salud 2023;1:17-17.

16. Raúl LH, Libien P. Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano [Internet]. Gob.mx. [citado el 15 de enero de 2024]. Disponible en: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

17. Caero L, Libertelli J. Relationship between Vigorexia, steroid use, and recreational bodybuilding practice and the effects of the closure of training centers due to the Covid-19 pandemic in young people in Argentina. AG Salud 2023;1:18-18.

18. Ogolodom MP, Ochong AD, Egop EB, Jeremiah CU, Madume AK, Nyenke CU, et al. Knowledge and perception of healthcare workers towards the adoption of artificial intelligence in healthcare service delivery in Nigeria. AG Salud 2023;1:16-16.

19. Gaceta del Senado [Internet]. Gob.mx. [citado el 15 de enero de 2024]. Disponible en: https://www.senado.gob.mx/65/gaceta_del_senado/documento/35208

20. Robo de identidad al acecho – Revista Proteja su Dinero [Internet]. 2022. Disponible en: https://revista.condusef.gob.mx/2022/07/robo-de-identidad-al-acecho/

21. Ciberamenazas empresariales en 2023: chantaje, falsas fugas de datos y ataques en la nube [Internet]. www.kaspersky.es. 2023 [citado el 15 de enero de 2024]. Disponible en: https://www.kaspersky.es/about/press-releases/2023_ciberamenazas-empresariales-en-2023-chantaje-falsas-fugas-de-datos-y-ataques-en-la-nube

22. Boletín de seguridad de Kaspersky, estadísticas de 2021 [Internet]. [cited 2024 Jan 16]. Available from: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_sp.pdf

23. Boletín de seguridad de Kaspersky, estadísticas de 2022 [Internet]. securelist.lat. 2023 [cited 2024 Jan 16]. Available from: https://securelist.lat/ksb-2023-statistics/98257/

24. Prontuario Estadístico de la Fiscalía General del Estado de Tabasco [Internet]. www.fiscaliatabasco.gob.mx. [cited 2024 Jan 16]. Available from: https://www.fiscaliatabasco.gob.mx/Estadistica/Index

25. Padilla P, Elizabeth M. Descripción del ataque del Ransomware Exx bajo un entorno controlado en máquinas virtuales. Quito, Ecuador: Universidad Tecnológica Israel; 2023.

FINANCIACIÓN

Ninguna.

CONFLICTO DE INTERESES

No existe.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Análisis formal: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Investigación: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Metodología: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Software: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Redacción – borrador original: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.
Redacción – revisión y edición: Gilberto Murillo González, German Martínez Prats, Verónica Vázquez Vidal.