Artículo Original Pág.[143 - 172] ISSN 2411-0035

Fides Et Ratio **Volumen 21** Marzo 2021

Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos

Factors that determine computer vulneration and the development of a mobile app to raise awareness about the impacts on assets

Kevin Andrés Peñafiel Lucuy[1]
kevin_penafiel@hotmail.com
Instituto de Investigaciones en Ciencia y Tecnología,
Universidad La Salle - Bolivia

Resumen

La exposición a la vulneración de datos personales, es una realidad que afecta a todas las personas que utilizan dispositivos tecnológicos. Esto hace que se estudie y se obtenga información adecuada para tomar decisiones al respecto. El trabajo de investigación tiene por objetivo general "Determinar el grado de conocimiento sobre seguridad informática y el desarrollo de una aplicación que oriente sobre la prevención de la vulneración de datos y activos". El trabajo se realizó bajo las técnicas de investigación descriptiva cualitativa, realizando análisis descriptivo he inferencial bajo un modelo lineal generalizado mixto. Los resultados de la investigación sobre el grado de conocimiento que los usuarios/as tienen sobre, seguridad informática, en un 8 y 5% en varones y mujeres respectivamente que conocen sobre seguridad informática; en ocupación los que más conocen son Profesional independiente 46%. Esta información es el punto de partida para el desarrollo de una aplicación móvil informativa que contribuya a concientizar a usuarios/as sobre la facilidad con la que sus datos pueden ser extraídos y vulnerados.

Palabras clave:

Seguridad Informática, riesgos informáticos, vulnerabilidad de datos.

1 Ing. en Sistemas en Universidad La Salle con énfasis en diseño de sistemas y seguridad informática. https://orcid.org/0000-0002-4655-7432

Abstract

Exposure to the violation of personal data is a reality that affects all people who use technological devices. This means that adequate information is studied and obtained to make decisions in this regard. The general objective of the research work is "To determine the degree of knowledge about computer security and the development of an application that guides the prevention of data and assets infringement". The work was carried out under qualitative descriptive research techniques, performing descriptive and inferential analysis under a mixed generalized linear model. The results of the research on the degree of knowledge that users have about computer security, in 8 and 5% in men and women respectively who know about computer security; in occupation, those who know the most are Professional 46%. This information is the starting point for the development of an informative mobile application that helps to make users aware of the ease with which their data can be extracted and compromised.

Key words:

Computer Security, computer risks, data vulnerability.

Introducción

Con el avance de la tecnología y los dispositivos electrónicos inteligentes, se manejan diariamente los datos en diferentes lugares; tanto en empresas como en cuentas bancarias o en dispositivos personales. Estos datos ya mencionados pueden ser de diferente magnitud dependiendo del tipo de información que se maneja. Existen diferentes tipos de datos que pueden ser confidenciales y/o personales. La seguridad de dichos datos, dependen mucho de la seguridad del dispositivo que los almacena y la protección que se le proporcione.

Por un lado, las empresas cuentan con una seguridad de alto nivel en sus bases de datos, por otro lado, toda la información personal que se almacena en algún dispositivo o computador, puede ser vulnerado fácilmente si no se tienen las medidas de seguridad necesarias, aun así existen maneras de acceder a dichos datos con facilidad.

La vulnerabilidad de datos se ve afectada por diferentes componentes, entre ellos se resalta el bajo nivel de seguridad que viene predeterminado en los dispositivos. La facilidad de poder "hackear" o en el peor de los casos el "crackear" y entrar en la raíz del sistema. De igual manera se tiene poca información del usuario, sobre la seguridad de datos, esto conlleva a varios descuidos que de una u otra manera dan paso a que se pueda vulnerar de forma rápida y sencilla sin el consentimiento del usuario.

Cuando navegamos o usamos aplicaciones vamos dejando rastros de información. Esa información puede revelar quienes somos y cómo usamos la tecnología. Muchas veces entregamos datos personales (como nuestro nombre, hábitos de consumo y localización) porque páginas y aplicaciones solicitan. En otros casos, los datos personales son deducidos o generados a partir de nuestro uso. Estos datos personales también son analizados por quienes nos brindan servicios en Internet para diversos fines que incluyen desde brindar una mejor experiencia de uso hasta clasificarnos discriminatoriamente. Esta situación se repite todo el tiempo.

El objetivo general de la presente investigación es: Determinar el grado de conocimiento sobre seguridad informática y el desarrollo de una aplicación que oriente sobre la prevención de la vulneración de datos y activos. Y como Objetivos específicos se tiene: Describir los factores que influyen en los tipos de vulnerabilidad y sus efectos, en los activos de tecnología informática. Concientizar a las personas sobre los riesgos a los que se exponen mediante una aplicación informativa basada en una metodología ágil.

Referentes Conceptuales

Seguridad Informática

La seguridad informática según Canelario y Rodríguez (2015) se la define como un conjunto de conocimientos sistemáticos orientados a conseguir niveles altos de seguridad" donde el objetivo principal es proteger y salvaguardar *la información* desde su confidencialidad, integridad y

disponibilidad.

Según Avenia (2017), para precisar los principios que definen la seguridad informática entorno a los datos y servicios, menciona tres componentes principales: la confidencialidad, la integridad y la disponibilidad que actúan interrelacionados; la ausencia de uno de ellos provocaría la vulnerabilidad de los mismos.

La seguridad informática también es conocida como ciberseguridad, es una rama de la Informática. Dentro del ámbito informático la seguridad se puede dividir en dos tipos; la seguridad física y la seguridad lógica, en ambos casos los principales protagonistas son los activos, como ser datos, software y otros.

La seguridad física consta de medidas y protocolos de seguridad con el fin de proteger diferentes dispositivos electrónicos; ordenadores, periféricos, etc. La seguridad lógica según Castillo (2017) consiste en una serie de barreras y procedimientos que resguarden el acceso a los datos. "Todo lo que no está permitido debe estar prohibido". La seguridad lógica requiere de medidas de protección bien definidas, caso contrario estarían expuestos a diferentes vulnerabilidades que a la larga pueden tener un impacto de gran manera.

Activos

Los activos son recursos del sistema de seguridad de información (ISO 27001). Se clasificarán de acuerdo a la siguiente lista: Dato, Software, Hardware, Redes, Soporte, Instalaciones, Personal, Servicios. Los activos más valiosos son los datos. Su protección contempla métodos de seguridad contra el extravío el daño y la difusión o abuso de información confidencial.

Amenazas

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que "de tener

la oportunidad" atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad (López, 2010, p. 13). Entre ellas se puede mencionar, a las Amenazas internas: De tipo interruptora. Deshabilitan el acceso a la información; De tipo interceptivo Factores que interceptan y acceden a los recursos o activos; De tipo modificable. Al igual que los interceptivos, estos alteran o modifican los datos; De tipo fabrica. Agregan información falsa al sistema. Entre las Amenazas Directas: Accidentales. Accidentes meteorológicos, errores humanos. Intencionadas. Acción humana desde un punto externo.

Riesgos

La Organización Internacional por la Normalización (ISO) Según la Gestión de la seguridad de las tecnologías de la información y las comunicaciones (IS/ISO/IEC 13335-1, 2004) define riesgo tecnológico como: la posibilidad de que una amenaza determinada se materialice haciendo que las vulnerabilidades causen daños a uno o varios grupos de activos perjudicando a la organización.

Vulnerabilidades

La vulnerabilidad se refiere a un efecto en el sistema (activo) que podría dejarlo desprotegido ante ataques. Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. (Avenía, 2017, p.12). Estas debilidades pueden presentarse en cualquiera de los activos y su consecuencia son los impactos como efectos nocivos de un evento.

Métodos

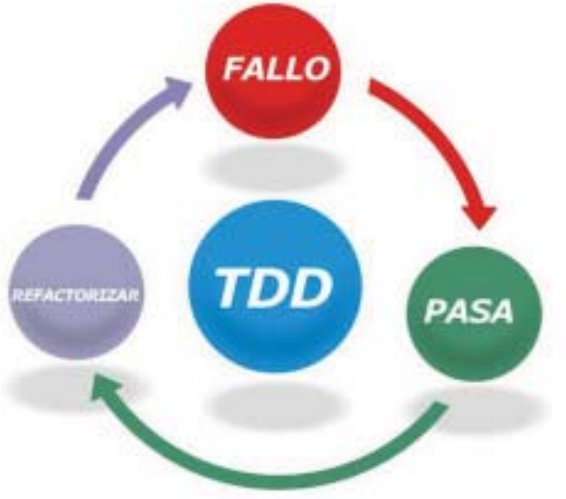
El trabajo se realizó bajo las técnicas de investigación descriptiva cualitativa, realizando análisis descriptivo he inferencial bajo un modelo lineal generalizado mixto; adaptado a las características del presente estudio y situación de la población, contemplando la siguiente secuencia de procesos: Inicialmente se realizó la revisión de información secundaria**,** de las teorías

de vulneración informática consultando bibliografía sobre el tema de estudio.

Se elaboró y aplicó encuestas de acuerdo a las variables obtenidas en la primera parte de este procedimiento, donde se obtuvo la información sobre el tema de investigación, el instrumento se elaboró en el "Formulario" de la aplicación de Google. Para luego sistematizar esta información en una base de datos, y posteriormente estos analizados estadísticamente el software estadístico InfoStat.

Para el desarrollo de la aplicación se optó por una metodología ágil en este caso la metodología TDD. Esta metodología "es una disciplina de diseño y programación, donde cada nueva línea de código que escribe un programador es en respuesta a una prueba que ha fallado" (Araújo, s/f p.1)

Figura 1: Proceso de funcionamiento del TDD



Fuente: Test-Driven Development - Beneficios y Desafíos para el Desarrollo de Software (2014)

Esta metodología se enfoca en 3 puntos importantes, según (Ble, 2010) -Diseño ágil con TDD- menciona que: La implementación de las funciones deben ser justas con lo que el cliente o usuario necesita, la reducción del número de defectos que puede llegar a tener el software y la producción de software modular. Existen 3 pasos para el desarrollo de una aplicación según esta metodología. (Ble, 2010) menciona como primer punto escribir la especificación o requisito del código, como segundo punto hay que implementar el código según el test establecido y finalmente refactorizar el código para evitar la duplicidad y corregir los errores.

Muestra

Se determinó el tamaño de la muestra de acuerdo a las características de la población (carácter infinito) de la ciudad de La Paz, con la siguiente formula:

$$n=(Z^2*p*p)/e^2$$

Fuente: León Velarde y Quiroz (1993)

Donde:

n = tamaño de la muestra
e = error estimado (5%)
Z = nivel de confianza (tabla de distribución normal para el 95% de confiabilidad)=1.96
p = Probabilidad a favor =0.5
q = Probabilidad en contra= 0.5

$$n=(1.96^2*0.5*0.5)/0.05^2 =384$$

Por la situación sanitaria de la pandemia COVID-19 que afecta a nuestro país, se realizó la encuesta virtual a diferentes personas por género y ocupación; en su mayoría, estudiantes universitarios de diferentes carreras.

Análisis Estadístico

El análisis estadístico se dividió en dos partes el primero de forma descriptiva y el segundo un análisis factorial donde se utilizó un modelo lineal con las variables Género y Ocupación si la interacción (debido a que no existe influencia de un factor al otro). El análisis se realizó con el siguiente modelo Lineal:

$$Y_{ijk} = \mu + \theta_i + \alpha_j + \varepsilon\varepsilon_{ij}$$

Donde:

Y_{ijk} = Cualquier observación (variables dependientes)
μ = Media de la población
θ_i = Efecto del i-ésimo Género
α_j = Efecto del j-ésimo Ocupación
$\varepsilon\varepsilon_{ij}$ = Error al modelo.

El Modelo establecido utilizado es para ajustar modelos de efectos fijos entre el género y la Ocupación.

El análisis estadístico se realizó con "El Modelo Lineal Generalizado Mixto" de la familia Binaria en una distribución de Chi cuadrado.

Materiales

Se utilizaron los siguientes materiales: Computadora de escritorio, Teléfono móvil.

Herramientas y software: Google Forms, Android Studio, Pixel Perfecto, Adobe Photoshop, WhatsApp, InfoStat.

Resultados y Discusión sobre 384 participantes

¿Alguna vez ha navegado estando en un cibercafé? (Punto de INTERNET/Juegos en Red).

Entre los encuestados respondieron sobre la pregunta de alguna vez ha navegado estando en un cibercafé, en un 77.1% afirman que navegaron en un cibercafé, y en un 29.9%, que no navegaron en un cibercafé. Al respecto en un estudio que se realizaron Beranuy y Fernández-Montalvo (2016) indican que la principal motivación para acudir a un cibercafé era no tener conexión a Internet en casa. En concreto, el 51.6% de la muestra señalaba esta como su razón principal, los datos encontrados en el presente estudio difieren a los encontrados en trabajo anterior. Esto puede deberse a que la mayor parte de los encuestados no tiene internet en casa.

Utiliza un sistema de seguridad en computadora de escritorio (PC).

En la utilización de un sistema de seguridad en computadora de escritorio (PC), los encuestados respondieron en un 48.6% que, si utilizan, en un 11.8% que no utilizan y en un 39.3%, que no tienen PC. Según Arellano y Peralta (2014), un 42,7% de las empresas que utiliza Internet no cuenta ni utiliza instalaciones o procedimientos internos de seguridad, coincidiendo aproximadamente con los porcentajes encontrados en el trabajo.

Utiliza un sistema de seguridad en Smartphone (Android, IOs).

En la utilización de un sistema de seguridad en smartphone (Android, IOs), respondieron los encuestados en un 54.9% que, si utilizan, en un 27.2% que no utilizan y en un 17.6%, que no tienen Smartphone. En relación a la pregunta no se encontró investigaciones realizadas.

Sabe lo que es el Phishing.

La respuesta de los encuestados sobre si sabe lo que es el Phishing, solo en un 19.1% conocen y en un 80.9% que no conocen. En un 46% de los

encuestados afirmó haber recibido un mensaje fraudulento que afirmaba provenir de servicios de correo electrónico como Yahoo!, Microsoft y Gmail**.** Le siguen las redes sociales con un 45%**,** los bancos 44% y tiendas en línea 37%**,** no se obtuvo información si conocen (www.welivesecurity.com/la-es/2013/01/09/).

Sabe la diferencia entre hacker y cracker.

Los encuestados respondieron sobre la pregunta, si sabe la diferencia entre hacker y cracker, en un 59.4% no conocen y en un 40.6% que conoce.

Con qué frecuencia realiza usted copias de seguridad.

La respuesta de los encuestados sobre con qué frecuencia realiza usted copias de seguridad, en un 33.5% hace copias Anualmente, en un 15.3% hace copias Diariamente, en un 26.3% hace copias Mensualmente, en un 14.2% hace copias Semanalmente y en un 10.4% hace copias Trimestralmente.

Sabe lo que es una Dirección IP.

La respuesta de los encuestados sobre si sabe lo que es una dirección IP, en un 37.7% no conocen y en un 62.3% que si conocen.

Sabe lo que es una dirección MAC.

Los encuestados respondieron sobre la pregunta, si sabe lo que es una dirección MAC, en un 77.4% no sabe y en un 22.6% que si saben lo que es una dirección MAC.

Sabe lo que significa el protocolo https.

La respuesta de los encuestados sobre si Sabe lo que significa el protocolo https, mencionan que en un 52.5% no sabe y en un 47.5% que sabe lo que significa el protocolo https.

¿Sabe lo que es una VPN?

Entre los que saben lo que es una VPN, están en un 39.7% y entre los que no saben están en un 60.3%.

Cómo considera la seguridad para hacer pagos a través de Internet.

Entre los encuestados que respondieron con respecto a cómo considera usted la seguridad para hacer pagos a través de Internet, se observa que, el 3.8% indica que es muy seguro, el 19.9% menciona que es nada seguro, el 47.1% indica que es poco seguro y el 28.9% indica que es seguro.

Seguridad Informática.

En el Tabla 1, se observa la prueba de hipótesis secuenciales para los efectos fijos de Seguridad Informática.

Entre la Fuente de variación Género existe diferencias estadísticas (Pr<0.05), entre la Fuente de variación Ocupación no existe un efecto significativo (Pr>0.05).

Tabla 1. Análisis de efectos fijos del porcentaje de Seguridad Informática

Fuente de variación	GL	Deviance	Resid. GL	Resid. Dev	Pr(>Chi)
NULL			344	453.98	
Género	**1**	**5.49**	343	448.5	0.0192
Ocupación	6	4.53	337	443.97	0.6054

Para establecer los patrones de diferencia se realizó una prueba de comparaciones múltiples, utilizando la prueba de Fisher (5%).

De acuerdo a la Tabla 2, el Género Masculino obtuvo 8.0% de seguridad informática y el Género Femenino obtuvo 5.0% de seguridad informática, ambos con un error estándar de; para Masculino, un 6.60% y 4.2% para Femenino.

Tabla 2. Comparación de medias de porcentaje en seguridad informática en Género.

Género	PredLin	E.E.	Media	E.E.	
Masculino	-2.42	88.01	0.08	6.6	A
Femenino	-2.93	88.01	0.05	4.2	B

Al respecto, los porcentajes ajustados de Género son muy bajos en el conocimiento de la seguridad informática. Esto se puede deber probablemente a la poca información que se tiene sobre la seguridad informática en general.

Al respecto podemos decir que los porcentajes ajustados de Género son muy bajos en el conocimiento de la seguridad informática.

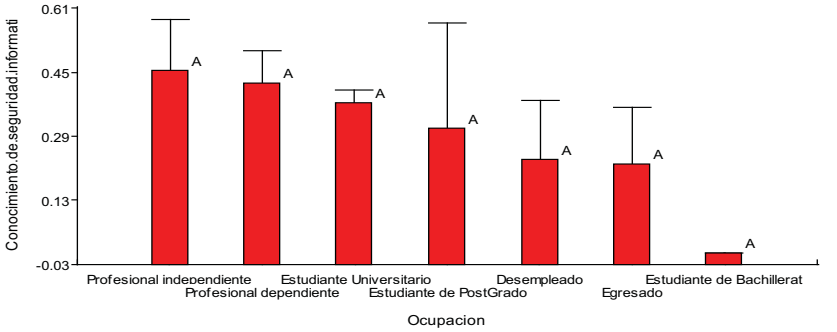
Esto se puede observar y complementar de acuerdo a las siguientes tablas: En el Tabla 3 y gráfica 1, se observa los promedios de Ocupación con referente a la seguridad informática. El conocimiento de seguridad informática en la ocupación es el siguiente: la ocupación Profesional independiente con 46%; la ocupación Profesional dependiente con 43%; la ocupación Estudiante universitario con 38%; la ocupación Estudiante de Postgrado con 31%; la ocupación Desempleado con 24%; la ocupación Egresado con 22%; la ocupación Estudiante Bachillerato con 0.0%, son estadísticamente similares. En todas las ocupaciones no pasan del 50%, por lo tanto, es muy bajo el conocimiento de la seguridad informática de las distintas ocupaciones.

Tabla 3. Comparación de medias del porcentaje de seguridad informática en Ocupación.

Ocupación	PredLin	E.E.	Media	E.E.
Profesional independiente	-0.16	0.51	0.46	0.13 A
Profesional dependiente	-0.3	0.33	0.43	0.08 A
Estudiante Universitario	-0.5	0.13	0.38	0.03 A
Estudiante de Postgrado	-0.79	1.23	0.31	0.26 A
Desempleado	-1.18	0.82	0.24	0.15 A

Egresado	-1.24	0.81	0.22	0.14 A
Estudiante de Bachillerato	-14.57	616.1	4.7E-07	2.90E-04 A
Medias con una letra común no son significativamente diferentes (p > 0.05)				

Gráfica 1. Comparación de medias del porcentaje de seguridad informática en Ocupación



Fuente: Elaboración propia

Robo de identidad.

El Tabla 4, muestra la prueba de hipótesis secuenciales para los efectos fijos de Robo de identidad.

Entre la Fuente de variación Género y Ocupación no existe diferencias estadísticas (Pr<0.05), en el Robo de identidad.

Tabla 4. Análisis de efectos fijos del porcentaje de Robo de identidad

Fuente de variación	GL	Deviance	Resid. GL	Resid. Dev	Pr(>Chi)
NULL			344	431.93	
Género	1	0.14	343	431.79	0.7082
Ocupación	6	11.35	337	420.45	0.0782

Para establecer los patrones de diferencia se realizó una prueba de comparaciones múltiples, con la prueba de Fisher (5%).

De acuerdo al Tabla 5, el Género Masculino alcanzó 9.0% de Robo de identidad y el Género Femenino alcanzó 7.0% de Robo de identidad, ambos con un error estándar de 4.0%.

Tabla 5. Comparación de medias de porcentaje en Robo de identidad en Género.

Género	PredLin	E.E.	Media	E.E.	
Masculino	-2.37	89.01	0.09	6.98	A
Femenino	-2.58	89.01	0.07	5.84	A

Medias con una letra común no son significativamente diferentes (p > 0.05)

Observando los promedios, los porcentajes ajustados de Género son muy bajos en el Robo de identidad, indicando que en su mayoría no sufrieron Robo de Identidad, en género.

En la tabla 6 y Gráfica 2, se observan los promedios de Ocupación con referente al Robo de identidad. En la ocupación Profesional independiente con 64% de seguridad informática; la ocupación Profesional dependiente con 55%; la ocupación Estudiante universitario con 34%; la ocupación Estudiante de Postgrado con 30%; la ocupación Desempleado con 28%; la ocupación Egresado con 25%; la ocupación Estudiante Bachillerato con 0.0%, son estadísticamente similares.

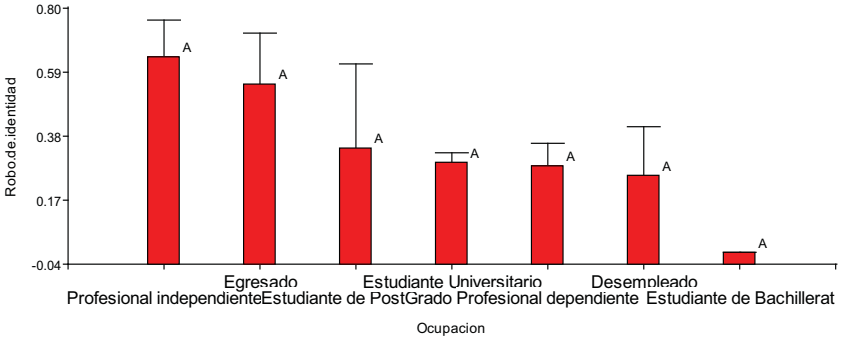
Tabla 6. Comparación de medias del porcentaje de Robo de identidad en Ocupación.

Ocupación	PredLin	E.E.	Media	E.E.
Profesional independiente	0.58	0.52	0.64	0.12 A
Profesional dependiente	0.21	0.67	0.55	0.17 A
Estudiante Universitario	-0.66	1.23	0.34	0.28 A
Estudiante de Postgrado	-0.87	0.14	0.3	0.03 A
Desempleado	-0.92	0.36	0.28	0.07 A

Egresado	-1.07	0.82	0.25	0.16 A
Estudiante de Bachillerato	-14.57	623.04	4.70E-07	2.90E-04 A
Medias con una letra común no son significativamente diferentes (p > 0.05)				

En las ocupaciones los que más sufrieron Robo de identidad son los profesionales independientes y dependientes.

Gráfica 2. Comparación de medias del porcentaje de Robo de identidad en Ocupación.



Fuente: Elaboración propia

Infestación de virus

En el Tabla 7, se observa la prueba de hipótesis secuenciales para los efectos fijos de Infestación de virus.

Entre la Fuente de variación Género y Ocupación existe diferencias altamente significativas (Pr<0.01), en la Infestación de virus.

Tabla 7. Análisis de efectos fijos del porcentaje de Infestación de virus

Fuente de variación	GL	Deviance	Resid. GL	Resid. Dev	Pr(>Chi)
NULL			344	465.18	
Género	1	13.96	343	451.22	0.0002
Ocupación	6	18.66	337	432.56	0.0048

Para establecer los patrones de diferencia se realizó la prueba de comparaciones múltiples, de Fisher (5%).

De acuerdo a la tabla 8, el Género Masculino alcanzó 96% de Infestación de virus siendo estadísticamente diferente al Género Femenino que alcanzó 92% de Infestación de virus, con un error estándar de 4.5% para Masculino y 8.5% para Femenino.

Tabla 8. Comparación de medias de porcentaje en Infestación de virus en Género.

Género	PredLin	E.E.	Media	E.E.	
Masculino	3.18	117.54	0.96	4.5	A
Femenino	2.47	117.54	0.92	8.46	B

Observando los promedios, los porcentajes ajustados de Género son muy altos en Infestación de virus, indicando que en su mayoría sufrieron la infestación de virus, en género.

En el Tabla 9 y Gráfica 3, se observan los promedios y prueba de medias de Ocupación con referente a la Infestación de virus. Las ocupaciones Estudiante de Postgrado con 100%; la ocupación Desempleado con 87%; la ocupación Profesional dependiente con 82%; y la ocupación Profesional independiente con 78%, son estadísticamente superiores a las ocupaciones Estudiante universitario con 58%; la ocupación Estudiante Bachillerato con 5% y la ocupación Egresado con 0.0%; son estadísticamente similares.

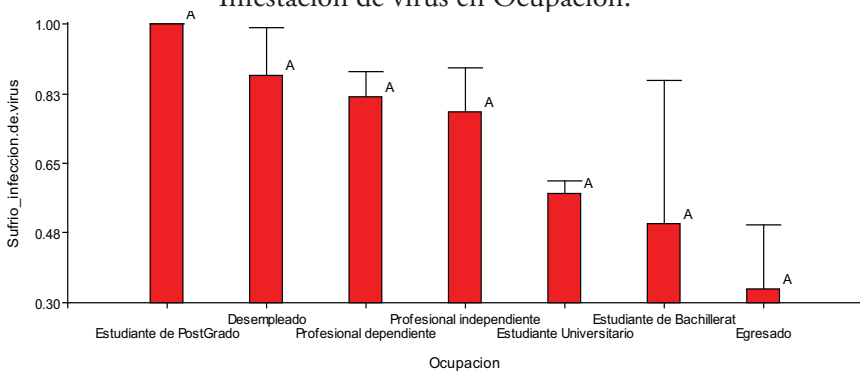
Tabla 9. Comparación de medias del porcentaje de Infestación de virus en Ocupación.

Ocupación	PredLin	E.E.	Media	E.E.
Estudiante de PostGrado	15.47	822.76	1	0.00016 A
Desempleado	1.9	1.08	0.87	0.12 A
Profesional dependiente	1.51	0.42	0.82	0.06 A
Profesional independiente	1.27	0.65	0.78	0.11 A
Estudiante Universitario	0.3	0.13	0.58	0.03 B

Estudiante de Bachillerat	0	1.44	0.5	0.36 B
Egresado	-0.67	0.72	3.40E-01	1.60E-01 B
Medias con una letra común no son significativamente diferentes (p > 0.05)				

En las ocupaciones los que más sufrieron Infestación de virus son los estudiantes de postgrado, los profesionales independientes, dependientes y los estudiantes Universitarios.

Gráfica 3. Comparación de medias del porcentaje de Infestación de virus en Ocupación.



Fuente: Elaboración propia

Utiliza autentificador de seguridad

La prueba de hipótesis secuenciales para los efectos fijos, que utiliza autentificador de seguridad, se observa en la Tabla 10.

Entre la Fuente de variación Género existe diferencias significativas (Pr<0.05), en la fuente de variación de Ocupación no existe diferencias estadísticas (Pr>0.05), en que utiliza autentificador de seguridad.

Tabla 10. Análisis de efectos fijos del porcentaje de Utiliza autentificador de seguridad.

Fuente de variación	GL	Deviance	Resid. GL	Resid. Dev	Pr(>Chi)
NULL			344	402.15	
Género	1	9.31	343	392.84	0.0023
Ocupación	6	9.23	337	383.61	0.1611

Para establecer los patrones de diferencia se realizó una prueba de comparaciones múltiples, con la prueba de Fisher (5%).

La prueba de medias de Fischer (Tabla 11) demuestra, que el Género Masculino alcanzó 1% que utiliza autentificador de seguridad, siendo superior estadísticamente al Género Femenino que alcanzó 0.03% que utiliza autentificador de seguridad.

Tabla 11. Comparación de medias de porcentaje de utiliza autentificador de seguridad en Género.

Género	PredLin	E.E.	Media	E.E.	
Masculino	-4.84	185.17	0.01	1.44	A
Femenino	-5.69	185.17	3.40E-03	0.62	B

Observando los promedios, los porcentajes ajustados de Género son muy bajos que utiliza autentificador de seguridad, indicando que en su generalidad no utiliza autentificador de seguridad prácticamente.

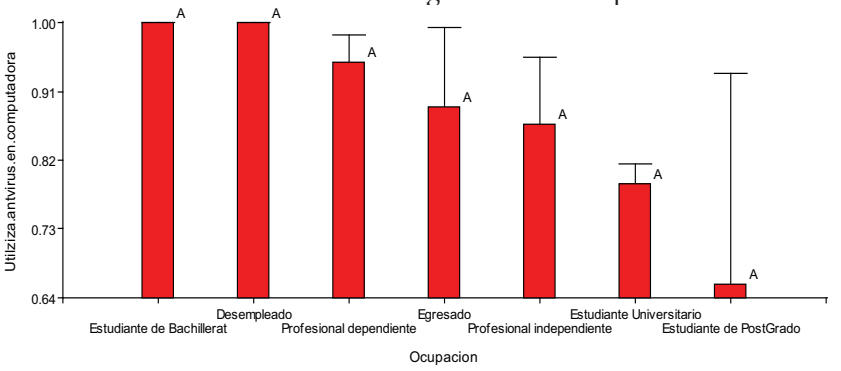
Los promedios de Ocupación del Tabla 12 y Gráfica 4, con referente a que utiliza autentificador de seguridad, se tiene: que en la ocupación Desempleado con 47%; superior a las ocupaciones Estudiante Bachillerato con 0.0%, Estudiante de Postgrado con 0.0%; las ocupaciones Estudiante universitario con 29%, Profesional dependiente con 26%, Egresado con 22% y Profesional independiente con 10%; son estadísticamente similares, en utilizar autentificador de seguridad.

Tabla 12. Comparación de medias del porcentaje de utiliza autentificador de seguridad en Ocupación.

Ocupación	**PredLin**	**E.E.**	**Media**	**E.E.**	
Desempleado	-0.11	0.72	0.47	1.80E-01	A
Estudiante Universitario	-0.88	0.14	0.29	3.00E-02	AB
Profesional dependiente	-1.03	0.36	0.26	0.07	AB
Egresado	-1.26	0.81	0.22	0.14	AB
Profesional independiente	-2.25	0.77	0.1	0.07	AB
Estudiante de Bachillerat	-15.6	1002.49	1.70E-07	1.70E-04	B
Estudiante de PostGrado	-15.73	821.61	1.50E-07	1.20E-04	B
Medias con una letra común no son significativamente diferentes ($p > 0.05$)					

En las ocupaciones los que más utiliza autentificador de seguridad son el Desempleo, Estudiante universitario y profesional dependiente, pero no pasan del 50%.

Gráfica 4. Comparación de medias del porcentaje de utiliza autentificador de seguridad en Ocupación.



Fuente: Elaboración propia

Reconstrucción de inferencias

Tabla 13. Tabla de escala de problemas en la vulneración

Escala de problema	Descripción
Menor	Problemas leves, causan molestias
Moderada	Problemas intermedios, muy molestos y en algunos casos pueden llegar a causas mayores
Mayor	Causan problemas irreversibles o muy difíciles de solucionar

Fuente: Elaboración propia

Tabla 14. Tabla descriptiva de factores, con posibles riesgos, vulnerabilidad y tipos de amenazas.

Variables	Posibles Riesgos	Tipo de vulnerabilidad o exposición	Activo sobre el que trabaja	Tipos de amenaza	Tipo de consecuencia	Posibles consecuencias
¿Alguna vez ha navegado estando en un cibercafé? (Punto de INTERNET/ Juegos en Red)	Infección de virus en dispositivos extraíbles.	Moderada	Dato	Interceptivo, modificable, directa	Negativa	Infección de virus, robo de contraseñas, suplantación de identidad
	Cesiones abiertas sin cerrar		Hardware			
			Software			
PC de escritorio/ Computadora portatil sin uso de un sistema de seguridad	Infección de virus.	Menor-Moderada	Software, Red	Modificable, interruptiva, interceptiva	Negativa	Infección de PC, instalación de programas, Instalación de programas "sospechosos" o desconocidos, Aparición de archivos desconocidos
	Infección de malwares.					
Dispositivo smarth sin uso de un sistema de seguridad	Filtración de apps malwares	Menor	Dato, software, red	Interceptivo, modificable	Negativa	Robo de datos, bancarios, robo de contraseñas, filtración en red (nivel LAN)
¿Usted sabe lo que es el Phishing?	Ciber ataques, robo de información	Moderada	Personal	Interceptivo, intencionada	Negativa	Trata y tráfico de personas
Diferencia entre hacker y cracker	Información fraudulenta	Menor	Personal	De fábrica	Negativa, positiva	Confusión de información/ Reconocimiento de individuos

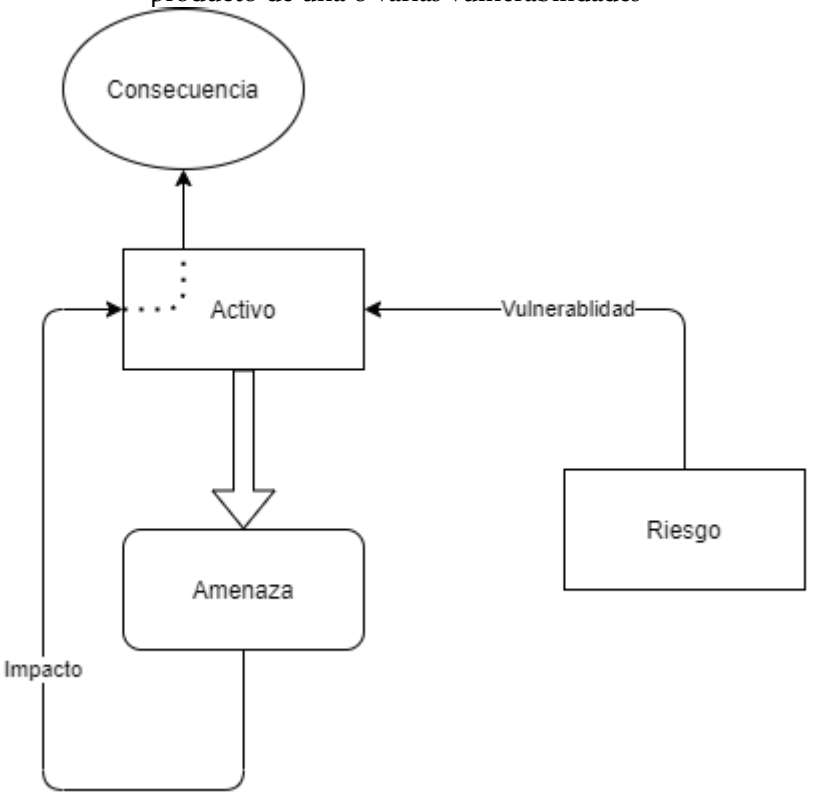
Conocimiento y uso de un autenticador de seguridad	Vulneración de sistemas tecnológicos	Moderada	Dato	Interceptivo	Negativa	Robo de datos bancarios, vulneración a contraseñas
No realizar copias de seguridad	Erradicación de datos	Moderada	Dato	Accidental	Negativa	Pérdida total de información
Conocimiento de Dirección IP	Fácil vulneración de red local	Menor-Moderada-Mayor	Red-Instalaciones	Interruptora, modificable, de fábrica, intencionada	Negativa, Positiva	Interceptación de red local, acceso a datos, alteración de configuración, corte de tráfico de información, monitoreo de red
Conocimiento y manejo de las propiedades de un Firewall	Vulneración total de red	Mayor	Red-Instalaciones	Intencionada, interruptora, interceptivo, modificable, de fábrica intencionada	Negativa	Apertura de puertos de red, exposición total de red local, bloqueo y rastreo de equipos
¿Conocimiento de la dirección MAC?	Ubicación precisa de un dispositivo	Menor-Mediana	Software	Interruptora	Negativa	Rastreo de red, filtración de información
Protocolo https	Infección de virus	Menor	Software	Interceptivo, intencionada	Negativa	Infección de virus, rastreo, vulneración de red
Uso de VPN	Rastreo		Red	Accidental	Positiva	Lugar erróneo de navegación/ Protección de ubicación real y de Ip

Uso del modo Incognito en el navegador	Rastro de navegación		Software	Accidental	Positiva	Monitoreo por parte del proveedor de internet /Mayor seguridad cognitiva de navegación
Pagos a través de Internet	Interceptación de terceros	Media	Servicios	Interceptivo, intencionada	Negativa	Pagos indebidos por parte de terceros sin autorización personal, robo de dinero
¿Realiza usted copias de seguridad?	Perdida de información, alteración de datos	Media-Alta	Periférico, Hardware, Software, Dato	Accidental, intencionada, modificable	Negativa	Extravió de datos, pérdida de información

Fuente: Elaboración propia

Al mismo tiempo existe un riesgo de que diferentes amenazas se materialicen producto de una o varias vulnerabilidades que afectan a nuestros activos dando lugar a las consecuencias, tal como se ve en el siguiente esquema:

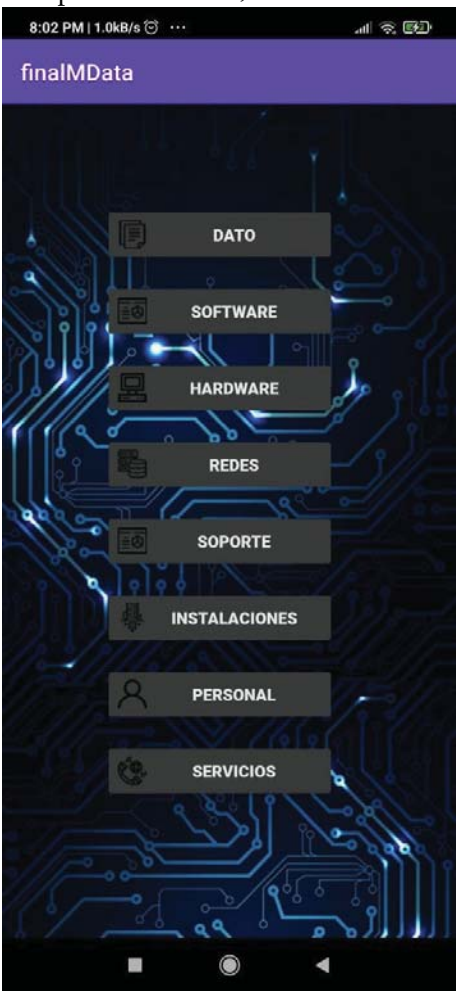
Gráfica 5. Riesgos de que diferentes amenazas se materialicen producto de una o varias vulnerabilidades



Fuente: Elaboración propia

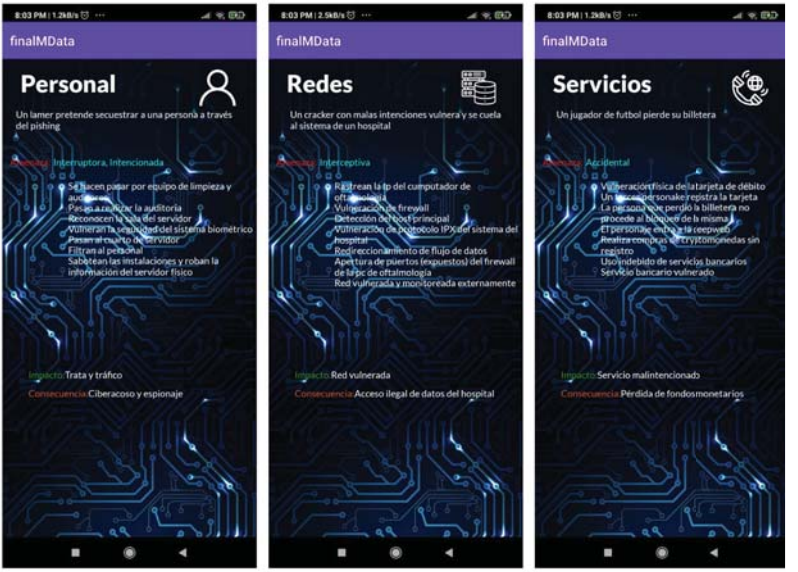
FinalMData

Figura 2. Aplicación móvil, vulneración Informática

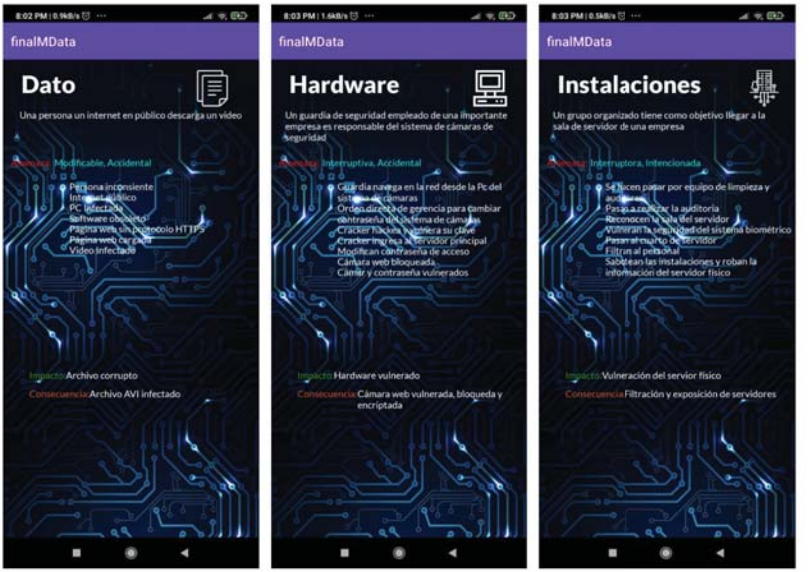


Fuente: Elaboración propia

Figura 3: Opciones de la aplicación Móvil



Fuente: Elaboración propia



Fuente: Elaboración propia

La aplicación, una vez finalizada será publicada con los permisos y aprobación correspondiente, servirá como referencia para personas que estén interesadas en informarse sobre el tema.

Conclusiones

De los resultados del trabajo, se llega a las siguientes conclusiones:

Entre los encuestados respondieron sobre la pregunta de alguna vez ha navegado estando en un cibercafé, en un 77.1% afirman que navegaron en un cibercafé; En la utilización de un sistema de seguridad en computadora de escritorio (PC), los encuestados respondieron en un 48.6% que si utilizan.

En la utilización de un sistema de seguridad en smartphone (Android, IOs), en un 54.9% que si utilizan.

La respuesta de los encuestados sobre si sabe lo que es el Phishing, solo en un 19.1% conocen.

Los encuestados respondieron sobre la pregunta, si sabe la diferencia entre hacker y cracker, en un 40.6% que conoce.

La respuesta de los encuestados sobre con qué frecuencia realiza usted copias de seguridad, en un 33.5% hace copias Anualmente, los demás en menor porcentaje.

La respuesta de los encuestados sobre si sabe lo que es una dirección IP, en un 62.3% que conocen.

La respuesta de los encuestados sobre si Sabe lo que significa el protocolo https, mencionan que en un 47.5% que sabe lo que significa el protocolo https.

Entre los encuestados que respondieron con respecto a cómo considera usted la seguridad para hacer pagos a través de Internet, el 47.1% indica que es poco seguro, entre los de más porcentaje.

El Género Masculino obtuvo 8.0% de conocimiento de seguridad informática.

Los promedios de Ocupación con referente a la seguridad informática. El conocimiento de seguridad informática en la ocupación el que más porcentaje obtuvo es la ocupación Profesional independiente con 46%.

El Género Masculino alcanzó 9.0% de Robo de identidad, siendo muy bajos. Entre los promedios de Ocupación con referente al Robo de identidad. En la ocupación Profesional independiente alcanzo un 64% de seguridad informática.

Entre la infestación del virus el Género Masculino alcanzó 96%. Son muy altos en Infestación de virus. Las ocupaciones de Estudiante de Postgrado alcanzo un 100% y la ocupación Desempleado con 87%.

El Género Masculino alcanzó 1% que utiliza autentificador de seguridad. En la ocupación Desempleado utiliza autentificador de seguridad un 47%. Los que más utiliza autentificador de seguridad son el Desempleo, Estudiante universitario y profesional dependiente, pero no pasan del 50%. Se desarrolló la aplicación con los resultados estadísticos; tomando en cuenta los puntos más importantes y ejemplificados con casos hipotéticos. Dichos casos se respaldan bajo la tabla de factores, riesgos, vulnerabilidades y tipos de amenazas.

Referencias bibliográficas

Araújo, A. (s/f). Test Driven Development Fortalezas y Debilidades. Facultad de ingeniería. Universidad de la República, Montevideo, Uruguay.

André, G. (9 de Junio, 2013) Phishing: webmail, redes sociales y bancos son

los servicios más suplantados. Recuperado de www.welivesecurity.com/la-es/2013/01/09/phishing-webmail-redes-sociales-bancos-servicios-mas-suplantados/

Avenia, C.A. (2017). Fundamentos de la seguridad Informática. Bogotá D.C., Fundación Universitaria del Área Andina.

Arellano, P. y Peralta, S. (2014). Informe de resultados: Tecnologías de la información y comunicación en las empresas. www.economia.gob.cl/wp-content/uploads/2015/10/Informe-de-resultados-TIC-en-las-empresas.pdf

Beranuy y Fernández (2017). Características del uso de Internet en los cibercafés. Recuperado de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-48082016000100001

Ble C. (2010-2013). Diseño ágil con TDD Recuperado de https://uniwebsidad.com/libros/tdd?from=librosweb

Bureau of Indian Standards (BIS) (2004). Information Technology - Security Techniques - Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security Management (IS/ISO/IEC 13335-1)

Candelario, J.J., Rodríguez, M. (2014). Seguridad Informática en el Siglo XXI: Una perspectiva Juridica tecnológica Enfocada hacia las organizaciones nacionales y mundiales. Universidad Nacional.

Castillo, J.A (31 marzo, 2017). Seguridad Lógica. Gestión de la información: Confidencialidad,
integridad, disponibilidad y estanqueidad. Recuperado de https://cronicaseguridad.com/2017/03/31/seguridad-logica-gestion-la-informacion-confidencialidad-integridad-disponibilidad-estanqueidad/

Castro, E., y Rojas, A. (2013). Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. Bogotá. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de sistemas. Trabajo de Investigación. Bogotá.

Iso (1947). Organización Internacional por la Normalización (ISO). Recuperado de https://www.iso.org/home.html.

López, P. (2010). Seguridad Informática, Madrid, España: Editorial Edix

SA.
Quiroz, S. y Macías, D. (2017). Seguridad informática Consideraciones. Ecuador
Romero, M., Figeroa, G., Vera, D., Alava, J., Parrales, G., Alava, C., Murillo, A. y Castillo, M. (2018). Introducción a la Seguridad Informática y el análisis de las vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L.
Sena, L. y Tenzer S. (2004). Introducción al riesgo Informático. Catedra de Introducción a la Computación
Tarazona, C. (2018). Amenazas Informáticas y Seguridad de la Información. 965-texto del artículo-3375-2-10-20180126.
Vaca, P., Maldonado, C., Inchaurrondo, C., Peretti, P., Soledad, M., Bueno, M. y Cagliolo, M. (2014). Test-Driven Development - Beneficios y Desafíos para el Desarrollo de Software. Universidad Tecnológica Nacional – Facultad Regional Córdoba.

Artículo Recibido: 23-10-2020
Artículo Aprobado: 02-02-2021