



ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Riesgo y Seguridad en los Dispositivos Móviles en
Estudiantes de la Carrera de Desarrollo de Software en el
SENATI, 2019

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
Maestro en Ingeniería de Sistemas con mención en Tecnología de la
Información

AUTOR:

Br. Jose Armando Tiznado Ubillus

ASESOR:

Dr. César Humberto Del Castillo Talledo

SECCION:

Ingeniería

LINEA DE INVESTIGACION:

Telecomunicaciones

LIMA - PERÚ

2019



DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): TIZNADO UBILLUS, JOSE ARMANDO

Para obtener el Grado Académico de *Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información*, ha sustentado la tesis titulada:

RIESGO Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES EN ESTUDIANTES DE LA CARRERA DE DESARROLLO DE SOFTWARE EN EL SENATI, 2019

Fecha: 29 de enero de 2019

Hora: 3:30 p.m.

JURADOS:

PRESIDENTE: Dr. Luzmila Garro Aburto

Firma: 

SECRETARIO: Dra. Roxana Beatriz, Gonzales Huaytahuilca

Firma: 

VOCAL: Dr. César Humberto, del Castillo Talledo

Firma: 

El Jurado evaluador emitió el dictamen de:

APROBADO POR MAYORIA

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....
.....
.....
.....

Recomendaciones sobre el documento de la tesis:

MEJORAR REDACCION APA

.....

Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Dedicatoria

Dedico esta tesis a Dios por guiar mi camino en los objetivos clave de mi vida ayudándome en elaborar proyecto que me costó esfuerzo, tiempo y dedicación en realizar este proyecto.

Agradecimiento

Agradezco a Dios y a Jesús por darme todo lo que pedí en esta vida, por poder encaminar correctamente en mi camino a la mujer que amo mi esposa y que proteja a mis padre y hermana de todo poderoso. Gracias amado Dios.

Declaratoria de Autoría

Yo, **Jose Armando Tizado Ubillus**, estudiante de la Escuela de Posgrado, Maestría en Ingeniería de Sistema con Mención en Tecnología de la Información, de la Universidad César Vallejo, Sede Lima Norte; declaro el trabajo académico titulado "**Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019**" presentada, en 90 folios para la obtención del grado académico de Maestro en Ingeniería de Sistema con Mención en Tecnología de la Información, es de mi autoría.

Por tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 29 de Enero del 2019



Jose Armando Tizado Ubillus
DNI: 43813470

Los Olivos, 12 de Enero del 2019

Presentación

Señores miembros del jurado calificador

De conformidad con el Reglamento de Grados y Títulos de la Universidad César Vallejo, pongo a vuestra consideración la evaluación de la tesis **Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019**, elaborada con el objetivo general de demostrar que el modelo propuesto mejorara el nivel de seguridad en los dispositivos Móviles para bajar y los riesgos que se pueden encontrar por algún ataque.

En el presente trabajo, estudia los niveles de los Riesgo y la seguridad en los dispositivos móvil Android. El estudio comprende los siguientes capítulos: el capítulo I se refiere a la introducción; el capítulo II se refiere al Marco metodológico; el capítulo IV se refiere a la discusión; el capítulo V a las conclusiones; el capítulo VI a las recomendaciones. Por último, el capítulo VII menciona las referencias bibliográficas y los anexos respectivos.

Los resultados obtenidos en la presente investigación han sido elaborados siguiendo el protocolo de la Escuela de Postgrado al demostrar que existe riesgo con una baja medida de seguridad en la información referente a los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Señores miembros del jurado esperamos que esta investigación sea evaluada y merezca su aprobación.

Índices de Contenido

Página del Jurado	ii
Dedicatoria	iv
Agradecimiento	v
Declaratoria de Autoría	vi
Presentación	vii
Índices de Contenido	viii
Resumen	xii
Abstract	xiii
I. Introducción	14
1.1. Realidad Problemática:	15
1.2. Trabajo Previos:	18
1.2.1. Trabajo Previos Internacionales:	18
1.2.2. Trabajo Previos Nacionales	20
1.3. Teoría relacionada al Tema:	22
1.4. Formulación del Problema:	32
1.4.1. Problema General:	32
1.4.2. Problema Específicos :	32
1.5. Justificación del Estudio:	33
1.5.1. Justificación Teórico:	33
1.5.2. Justificación Práctico:	34
1.5.3. Justificación Metodológica:	34
1.6. Hipótesis:	34
1.7. Hipótesis General:	34
1.8. Hipótesis Especificas	35
1.9. Objetivo:	35
1.9.1. Objetivo General:	35
1.9.2. Objetivo Especifico:	35
II. Método	37
2.1. Variable, Operacionalización:	38
2.1.1. Variables:	38

2.1.2. Operacionalización de variable:	39
2.2. Metodología:	40
2.3. Tipo de estudio:	41
2.4. Diseño de estudio:	43
2.5. Población, muestra y muestreo:	45
2.5.1. Población :	45
2.5.2. Muestra:	45
2.5.3. Muestreo:	46
2.6. Técnica e instrumentos:	47
2.6.1. Técnica:	47
2.6.2. Instrumentos:	47
2.6.3. Validez:	48
2.6.4. Confiabilidad:	49
2.7. Métodos de análisis de datos:	49
III. Resultados	50
3.1. Resultados descriptivos :	51
3.1.1. Resultado descriptivo de la v1 - Riesgos Informáticos:	51
3.1.2. Resultado descriptivo de la v2 - Seguridad en Dispositivo Móvil:	52
3.1.3. Resultado descriptivo de la dimensión 1 de los Riesgos proveniente del equipo:	53
3.1.4. Resultado descriptivo de la dimensión 2 de los Riesgos proveniente de los programas:	54
3.1.5. Resultado descriptivo de la dimensión 3 de los Riesgos relacionado con los trabajos:	55
3.1.6. Resultado descriptivo de la dimensión 4 de los Riesgos respecto a las personas:	56
3.2. Prueba de Hipótesis:	57
3.2.1. Prueba de Hipótesis general:	57
3.2.2. Prueba de Hipótesis específica 1:	58
3.2.3. Prueba de Hipótesis específica 2:	59
3.2.4. Prueba de Hipótesis específica 3:	60
3.2.5. Prueba de Hipótesis específica 4:	62
IV. Discusión	64
4.1. Discusión:	65

V. Conclusiones	67
5.1. Conclusión:	68
VI. Recomendaciones	70
6.1. Recomendaciones:	71
VII. Referencias	72
VIII. Anexos	78
Anexo 1: Operacionalización de Variables	79
Anexo 2: Matriz de Operacionalización de Variable	80
Anexo 3: Tabla de escala de coeficiente de correlación	81
Anexo 4: Certificado de Validez de Riesgo Informático del Instrumento 1	86
Anexo 5: Certificado de Validez de Seguridad dispositivo móvil del Instrumento 1	88
Anexo 6: Certificado de Validez de Riesgo Informático del Instrumento 2	91
Anexo 7: Certificado de Validez de Seguridad en dispositivo móvil del Instrumento 2	93
Anexo 8: Certificado de Validez de Riesgo Informático del Instrumento 3	96
Anexo 12: Certificado de Validez de Seguridad en dispositivo móvil del Instrumento 3	98
Anexo 13: Correlación de dimensiones y variables	101
Anexo 14: Análisis y objetivo del proyecto	102
Anexo 15: Matriz de encuesta 1	103
Anexo 16: Matriz de encuesta 2	105
Anexo N 17: Artículo Científico	121

Índices de Tablas

Tabla 1: Operacionalización de variable Riesgo Informático	39
Tabla 2: Matriz de Operacionalización de variable seguridad en dispositivo móvil	40
Tabla 3: Distribución de estudiantes por Semestre.	45
Tabla 4: Ficha de instrumento – v1 riesgo informático	47
Tabla 5: Ficha de instrumento – v2 Seguridad en dispositivo Móvil	48
Tabla 6: Especialista para el certificarón de validez.	48
Tabla 7: Estadística de Confiabilidad	49
Tabla 8: Descripción de los Riesgos Informático	51
Tabla 9: Descripción de la Seguridad en los dispositivos Móvil	52
Tabla 10: Descripción de los Riesgos proveniente del equipo	53
Tabla 11: Descripción de los Riesgos proveniente de los programas.	54
Tabla 12: Descripción de los Riesgos relacionado con los trabajos.	55
Tabla 13: Descripción de los Riesgos respecto a las personas.	56
Tabla 14: Resultado - prueba de correlación Rho Spearman sobre la hipótesis general	57
Tabla 15: Resultado - prueba de correlación Rho Spearman sobre la hipótesis especifica 1	58
Tabla 16: Resultado - prueba de correlación Rho Spearman sobre la hipótesis especifica 2	60
Tabla 17: Resultado - prueba de correlación Rho Spearman sobre la hipótesis especifica 3	61
Tabla 18: Resultado - prueba de correlación Rho Spearman sobre la hipótesis especifica 4	62
Tabla 19: Tabla de escala de coeficiente de correlación	81
Tabla 20: Descripción de los Riesgos Informático	127
Tabla 21: Descripción de la Seguridad en los dispositivos Móvil	128
Tabla 22: Descripción de los Riesgos proveniente del equipo	128
Tabla 23: Descripción de los Riesgos proveniente de los programas.	129
Tabla 24: Descripción de los Riesgos relacionado con los trabajos.	129
Tabla 25: Descripción de los Riesgos respecto a las personas.	130

Índices de Figuras

Figura 1: Vulnerabilidad en Android	16
Figura 2: Digital in 2018	17
Figura 3: Digital in 2018	34
Figura 4: Metodología para enfoque cuantitativo .	41
Figura 5: Esquema de tipo de diseño.	44
Figura 6: Total del tamaño de la población	46
Figura 7: Descripción en porcentaje de los Riesgos Informáticos.	51
Figura 8: Descripción en porcentaje de los Seguridad en los Dispositivo Móvil.	52
Figura 9: Descripción en porcentaje de los Riesgos proveniente de los equipos.	53
Figura 10: Descripción en porcentaje de los Riesgos proveniente de los programas.	54
Figura 11: Descripción en porcentaje de los Riesgos relacionado con los trabajos.	55
Figura 12: Descripción en porcentaje de los Riesgos respecto a las personas.	56
Figura 13: Correlación de Dimensiones y variable	102
Figura 14: Análisis y objetivo del proyecto.	102
Figura 15: Metodología para enfoque cuantitativo.	127

Resumen

En el mundo actual la sociedad vive con una tecnología que tiene una línea de tiempo de muchas evaluaciones transcurrida y de uso personal, esta tecnología nos permite comunicarnos, realizar operaciones matemáticas, tomarnos fotos, grabar videos, escuchar música, etc., unas de las muchas infinidades de acciones que se puede hacer con este dispositivo móvil de gran beneficios para la sociedad, pero existes ciertos riesgos de aquellos delincuentes llamado (Hacker – Cracker) que quiere utilizar tecnología avanzada para poder sustraer información confidencial de nuestro dispositivo móvil, rompiendo la seguridad de acceso para obtener como nuestras cuentas bancarias, nuestras redes sociales, lista de contactos, documentos, etc.

El objetivo de mi proyecto de investigación es determinar la relación que existe entre el riesgo informático y la seguridad en el dispositivo móvil donde se determinó que los riesgos informático tiene un nivel de frecuencia de 30,4% por ciento en cambio en la seguridad de los dispositivo móvil alcanzo un porcentaje de frecuencia de 46% se determinó que identificando los niveles de correlación que existe y el tipo de investigación descriptiva, básica, transeccional con un enfoque cuantitativo y aplicando las recolección de los resultados estadístico en una correlacional no paramétrica de la variable 1 y la variable 2 aplicando Rho Spearman con la coeficiente de correlacional = 0,782 y una sig. (bilateral) = 0,000 pasando en el SPSS con la probabilidades estadísticas. Que a la vez existe niveles de riesgo y de inseguridad que los estudiantes que está propenso a ser atacado por cybercriminales, Se recomienda que se debe aplicar una charla informática sobre los nuevos métodos de hackeo a los dispositivos móviles fortaleciendo los niveles alto de seguridad y bajando los niveles de riesgos.

Palabra clave: Riesgo. Seguridad. Dispositivo móvil

Abstract

In today's world society lives with a technology that has a timeline of many evaluations passed and personal use, this technology allows us to communicate, perform mathematical operations, take pictures, record videos, listen to music, etc., some of the many infinities of actions that can be done with this mobile device of great benefits for society, but there are certain risks of those criminals called (Hacker - Cracker) who wants to use advanced technology to be able to steal confidential information from our mobile device, breaking security access to obtain as our bank accounts, our social networks, contact list, documents, etc.

The objective of my research project is to determine the relationship between computer risk and security in the mobile device where it was determined that computer risks have a level of frequency of 30.4% percent in the security of the mobile device reached a frequency percentage of 46% was determined by identifying the levels of correlation that exist and the type of descriptive, basic, transectional research with a quantitative approach and applying the statistical results collection in a nonparametric correlation of the variable 1 and variable 2 applying Rho Spearman with the correlation coefficient = 0.782 and a sig. (bilateral) = 0.000 passing in the SPSS with the statistical probabilities. That at the same time there are levels of risk and insecurity that students who are prone to be attacked by cybercriminals, It is recommended that a computer chat about new methods of hacking be applied to mobile devices, strengthening high levels of security and lowering the levels of risks.

Keyword: Risk. Security. Mobile device

I. Introducción

1.1. Realidad Problemática:

Desde la creación del 1ra computadora, y el invento de una computadora que ayudo revolucionar y agilizar el análisis algorítmico quien cifro el Enigma Alemán en el tiempo de la 2 guerra mundial creado por el padre de la informática Alan Turín. Ahora en el siglo XXI vivimos en la actualidad en un mundo rodeados de Hackers que analizan, atacan la seguridad y la información de una entidad pública, privada y no solo eso que también la información de las personas para usar el acto de cualquier fechoría que los hackers cibernéticos puedan utilizar con esa información.

Según (Mosquera, 2016) describió en el diario el Mundo:

La empresa de Panda Security, argumento como título: *“2015 ha sido el año en el que se han producido más ciberataques en todo el mundo”*. En lo general se describe una muestra con un total 304 millones de encuestados, una cifra monstruosa se denomina así por el récord en toda la historia de la informática con un 27,63% de todo el virus creado. “El contenido de las intimidaciones se está elevando exponencialmente debido a los Exploit Kits(trozo de código de comando), principalmente son software diseñados para la identificación debilidades en los celulares y para procesar código dañino para el celular”, explicó al diario Raúl Pérez, especialista en seguridad de Panda Security.

Por otro lado, en el 2016 se proyecta que habrá un incremento de este tipo de amenazas en todos los dispositivos móviles logrando alcanzar la existencia de ataques inevitables hacia la raíz principal que logran rootear el celular (logrando autorizaciones superiores al del usuario) y el único medio potencial es formatear el celular. “con solamente basta que los cybercriminales localicen una abertura en la seguridad para que acceda a posicionarse como el administrador llamado(*superusuarios*)”, explicó el señor Pérez. “Los celulares y Tablet son estrechamente apetitoso para ellos, porque el poseedor de estos equipos almacena datos de casi toda su vida: como por ejemplo

sus cuentas bancarias, imágenes, las zonas que han visitado, los deportes que realizan, lo que comunican frecuentemente en las redes sociales y a sus contactos”. (párr. 1 – 2).

Giusto (2018). El autor argumentó en el portal WeliveSecurity del sistema operativo:

Para Android, las detecciones de malware bajaron 27,48% con relación al primer 6 SEM. de 2017; y para iOS redujeron un 15% con relación al mismo tiempo del pasado año (...). el 23% de los fallos publicados en 2018 existieron críticos y el 13% de ellos consentía la realización de código malicioso. Esta resulta una mejora considerable proporción a años preliminares, donde los porcentajes de fallos críticos era significativamente más alto. De todas maneras, los usuarios tiene que instalar a tiempo los parches de seguridad para prevenir de infección de y de las vulnerabilidades como los parcheadas del pasado abril por Google. (párr., 1 - 4).

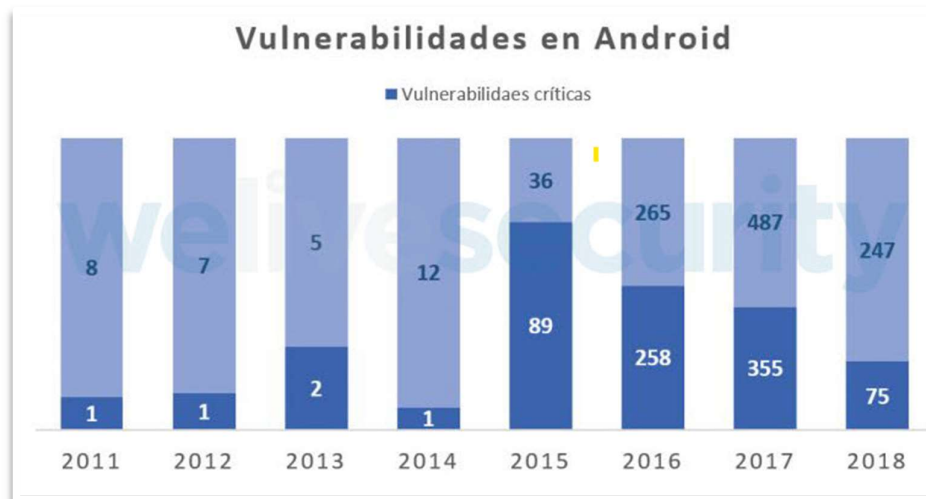


Figura 1: Vulnerabilidad en Android

Fuente: Welivesecurity: “Balance semestral de la seguridad móvil”

(Kemp, 2018). En el portal de Hootsuite publicó datos estadísticos referente a nivel global de la ayuda de otros portales argumentado cierto criterio:

“More than 200 million people achieved their 1st cell phone in 2017, and two thirds of the world's 7.6 million people now have cell phones.” [“Más de 200 millones de personas lograron su 1er dispositivo celular en 2017, y 2 tercios de los 7,6 millones de poblaciones del mundo ahora tienen una telefonía celular.”]. (p. 3)



Figura 2: Digital in 2018

Fuente: <https://hootsuite.com/es/pages/digital-in-2018#>

En Perú se divulgó sobre ataque cibernético que estaban haciendo atacados a los bancos esto lo afirmó El Diario la Republica (2018) en su portal “Tras el ataque cibernético ocurrido hoy, el FBI informo que se espera todavía por un ataque global en los cajeros automáticos (...). Otro punto a tener en **cuenta** es que no se debe realizar ninguna transacción bancaria a través de **internet y vía APP**”. (párrafo 2 - 5). Por otro lado, el diario el Comercio (2018) como tema llamado: En que residió el ciberataque a los bancos financiero-peruanos y como se oponer resistencia. Determinó en su portal: Un ataque cibernético contra agentes del sistema bancario mundial se reportó el pasado viernes a las 3 de la mañana. Las **empresas financieras peruanas lograron repeler el ciberataque**, informo en un comunicado la Asociación de Bancos del Perú (Asbanc). La población estuvo al tanto de estos acontecimientos y fluyó bastante información por canales móviles como WhatsApp y redes sociales. (párr.1 – 3).

Al enterarme sobre estos tipos de incidentes que ocurrieron en los bancos, generalizándose los ataques a nivel nacional de todo el Perú de Virus Malware que atacaron a las entidades Bancarias como a Personas que accedieron por sus aplicaciones Móviles de supuestos Hacker que robaron sus cuentas bancarias y que otros reportaron acceso restringido a sus cuentas Bancaria que los Bancos hicieron por motivo de seguridad, eso me hizo pensar que en mi institución donde trabajo tengo un grupo de estudiantes donde ellos acceden a sus cuentas bancarias y podría ser víctima de un robo cibernético corriendo riesgo de que puedan perder todo su dinero en su cuenta bancario.

En la institución dieron a conocer sobre los peligros que existen entre los virus y malware para las empresas Senati (2018) comentó de, ¿que si un día prendes su ordenador de trabajo y se das la sorpresa de que tu ordenador a sido formateada? ¿O que realizas unas compras online y ves que tu estado de cuenta bancaria se encuentra vacía? Esos podrían ser algunas de las consecuencias que usted le podría ocurrir si es que el lugar donde labora le brindara algunos de los servicios. (párr. 1). En la institución somos líderes en la formación profesional dual en dictar diferentes tipos de carrera ya q SENATI está con lo último en tecnología con convenio en Microsoft, adobe, Cisco y otras también empresa, por eso SENATI se quiere preocupar en el bienestar de sus estudiantes ante cualquier peligro o riesgo físico o cibernético q a ellos les puede ocurrir por eso se aplicó está proyecto de investigación para medir y relacionar los riesgos informático que ocurre en los dispositivos móviles midiendo los niveles de seguridad que hay en sus dispositivos móviles.

1.2. Trabajo Previos:

1.2.1. Trabajo Previos Internacionales:

Según Rojas (2016). En su argumento Magistral *"Evaluación de la seguridad de aplicaciones móviles bancarias"* sustentada en la Universidad de Chile la cual tuvo como objetivo realizar un estudio donde involucro a 10 programas de banca móvil para el entorno de Android en disposición en la tienda de Google Play Store. A cada

programa se le realizó un proceso automatizado de ingeniería reversa, para luego analizar estáticamente la codificación interna extraído como parte de ese proceso, para establecer que debilidades tienen los programas móviles bancarias chilenas que existen en la tienda de Google Play. Se encontró múltiples debilidades que hablan de un desarreglo en cuanto a la inquietud por la seguridad de los usuarios de estos programas, además unos de los primordiales problemas estar a la mira es el acceso a varios privilegios redundantes en los teléfonos de los usuarios (lista de contactos, acceso al sistema de archivos del equipo, etc.)

López (2016). En su tesis *Magistral "Aseguramiento de Dispositivos Móviles Android para el cumplimiento de las Norma (PCI - DSS)"* sustentada en la Universidad Internacional de la Rioja Master universitario en Seguridad Informática. el cual tiene como objetivo en buscar y localizar las principales vulnerabilidades que existes en los vectores a través de ataques, que hacen débiles a los celulares con Android version 5.1 lollipop, para mitigar los riesgos encontrados en el las actividades de prueba. Crear un argumento estructural de pruebas experimental, donde pasaran por una exploración de múltiples series de prueba de test rescatando los conceptos utilizados mediante la metodología de prueba de filtración procediendo a construir una guía para la protección en los sistemas operativo Android. La creación de la prueba experimental permitirá evidenciar que un dispositivo móvil con sistema operativo Android, no se modificará la mínima configuración de seguridad, se convertirá en una víctima fácil, tan fácil que será vulnerable a los ataques informáticos. La instalación de un antivirus da como solución en administrar el celular como una capa de protección de seguridad, garantizando 3 tipo de protección en (1)confidencialidad, (2) disponibilidad e (3) integridad de la información de los usuarios que se almacena y gestiona desde el celular el sistema operativo Android.

Erreyes (2017). En su tesis *Magistral "Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles"* en su tesis expuso como objetivo es crear un procedimiento

para la selección de recursos eficiente y con repertorios adaptados para fortificar la seguridad en los celulares. Se ejecutará la metodología para aplicar cierta selección de recursos de seguridad en los celulares que le permitirán a usuarios en público en general a usarlo para la protección de los datos de información y a la vez disponer de una guía práctica que le permitirá seleccionar los recursos validadas para que puedan mejorar los niveles de protección de su celular de toda la información contenida. Además, se debe fijar que el uso de los recursos adicionales pueda ayudar a evitar el aprovechamiento de la vulnerabilidad que se puedan presentar en los entornos de Sistema Operativo Android. Al utilizar los celulares como uso cotidiano y ser parte de nuestro diario continuo, estamos propensos a ser víctima de robo de nuestro dato de información y que esto ocurra sin darnos cuenta, debido a que nuestro celular se encuentra muchos programas, conectividad de red y datos de información que podrían está abierta incluso cuando nosotros no estemos usándolo el celular.

García (2017). En su tesis Magistral "Seguridad en Smartphone Análisis de riesgos, de vulnerabilidades y auditoría de dispositivos" sustentada en la universidad Oberta de Catalunya en su tesis expuso como objetivo principal desarrollar una metodología de análisis forense, adaptada a dispositivos con sistema operativo Android, que pueda dar soporte a esta necesidad. Para ello se analiza el estado del arte de la seguridad en dispositivo móviles inteligentes partiendo de un análisis de las amenazas de seguridad más comunes que pueden afectar a los dispositivos móviles, se realizara un análisis de la plataforma Android. Cada vez es más habitual la realización de tareas, personales o empresariales desde dispositivo móviles, que manejan información sensible y privada que es necesario proteger. En este escenario, el análisis forense, adaptado a este tipo de dispositivos se convierte en una necesidad que no puede ser obviada.

1.2.2. Trabajo Previos Nacionales

Llontop (2018) en su tesis magistral "*Gestión de riesgos de Tecnología de Información de las empresas de Nephila Networks*", sustentada en la Universidad

Cesar Vallejo que tuvo como en su tesis magistral tuvo como objetivo comparar la información de los resultados de forma numérica mediante mostrándolo en unos cuadros estadísticos a los niveles eficiente de la gestión del riesgo usando tecnología de la información proveniente de las empresas comerciales y de servicios. El proyecto está realizado con un enfoque cuantitativo elemental ya que se basa en una realidad en estudios previos y enfocado en un diseño descriptivo comparativo porque se usa teorías previas y se aplicara en 2 grupos de encuestados. Se aplico el instrumento con su cuestionario con una escala de (Likert - politómico), la encuesta permitirá validar la medición del juicio de expertos demostrando la fiabilidad obtenido por la encuesta obteniendo la coeficiencia de alfa de Cronbach con 0.821 con un numero de encuestado de 20. Se determina la cantidad total de los encuestado con 108. Se identifico que las empresas comerciales tienen como consideración que el plan actual de gestión de riesgos tiene un nivel de eficiencia aceptable con el 83.9% de los encuestados con la comparación de las empresas de servicios con un 63.5% y es considerado eficiente porque se considera el plan de gestión de riesgo como la mayor eficiencia en las empresas comerciales.

Otoya (2017). En su tesis Magistral "*Gestión de riesgos de TI en la seguridad de la información del programa de desarrollo productivo agrario rural 2017*" sustentada en la U. C. V. expuso como objetivo determinar la influencia de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural. El trabajo se desarrolló bajo un enfoque cuantitativo realizando una investigación en un estudio elemental de nivel descriptivo de diseño no experimental transversal comparativo, que permitirá determinar las interacciones causa-efecto entre las variables (investigación cuasi experimental). Se aplico el estudio a un grupo de colaboradores que conforma la muestra del estudio, según oficinas y direcciones con una total de 174 participantes que realizaron la encuesta y se utilizó un tamaño de muestra de 120 colaboradores encuestados aplicando una escala de medición Likert (politómica). Existe una influencia significativa de la gestión de TI en la seguridad de la información de un nivel alto teniendo un valor significancia de 0.035 y una dependencia de la variable

seguridad de información de la variable de gestión de riesgo de TI del 44%, por lo que se indica que es una buena gestión de riesgo que existe la probabilidad de una eficiente seguridad de la información.

Huamán (2017). En su tesis Magistral "*Plan de comunicaciones en seguridad de la información para el personal administrativo de la pontificia universidad católica del Perú*" sustentada en la universidad católica expone en su tesis como objetivo construir una base para culturalizar la seguridad de la información en los empleados administrativo de la PUCP a través de concientizar los problemas para las buenas prácticas en el uso y control de la tecnología (entretenimiento) y por medio de su comportamiento(educación) garantizando en la universidad la protección y auto resguardo de la información. Se presenta a continuación una matriz para la implementación con el modelo de NIST 108 para fomentar cultura de la educación en seguridad de la información. Los empleados administrativos saben y manejan el 50% más de los conceptos básico en la seguridad informático llegando al objetivo del 100% con respecto al objetivo específico 01, lo que logra permitir el principio de la estructura fundamental de conocimiento principal para construir la cultura de la seguridad de la información en la PUCP. El 72% de los empleados reconoce los enlaces de comunicación interna que deberá seguir el administrador y el 37% de los empleados administrativos se conocen y se adaptan un conjunto de las buenas experiencias para los empleados administrativos.

1.3. Teoría relacionada al Tema:

Se procede argumentar 2 variables diferenciando los conceptos y teoría que se relaciona con los Riesgos y seguridad en los dispositivos móviles, identificando y mencionando sus dimensiones que permitirán hacer las mediciones y la metodología correspondientes.

Riesgos Informáticos

Según Téllez (2008) Manifiesta:

Que el significado de riesgo informática es un nuevo concepto en la terminología legal, por lo tanto, es una definición detalla. La palabra *riesgo* se representa a la inseguridad o posibilidad de que suceda o se ejecute una casualidad, la cual podría estar pronosticada; en este sentido, que es permitido decir que la palabra riesgo es la posibilidad de que ocurra un daño. Se puede decir en función a lo anterior, cabe manifestar que los riesgos informáticos se referencia a la inseguridad existente por lo que es posible la ejecución de un acontecimiento referenciado con la amenaza de daño con respecto a los bienes o servicios informáticos todo esto son proveniente de los (1)equipos informáticos, (2)periféricos, (3)instalaciones, (4)proyectos, (5)programas de cómputo, (6)archivos,(7)información, (8)datos confidenciales, (9)responsabilidad civil que estos son ocasionan frente a los terceros por lo que concedió a un servicio informático, etcétera. (p. 158).

(ISO 31000:2009) citado en Serra C. (2013). Determino la palabra riesgo como:

“La determinación que la incertidumbre logra cumplir los procesos de los objetivos”. referenciado por la ISO 31000:2009 donde describe la incertidumbre como la acción de un elemento que nunca logra ocurrir o ejecutarse. A parte también describe el riesgo como un elemento muy importante donde se debe gestionar los efectos actividades positivos o negativo. (p. 14).

Por otro lado (UNE-71504:2008) cita a (Escrivá, Romero, Ramada y Onrubia, 2013). Donde determina que existe diversas definiciones para definir el termino riesgo; entre todas ellas destacamos las siguientes:

La UNE-71504:2008 define El riesgo es el nivel de grado de exposición ante una amenaza no prevista por las materias expuesta

sobre uno mismo o sobre otros mayores activos exponiéndose a daños o perjudicando a la organización.

El centro de la entidad pública Criptológico definió el riesgo como los elementos de una posible amenaza materializándose en los sucesos de vulnerabilidades y causándose daño impactante en las actividades o software.

Los riesgos se denomina como medidas de posibles probabilidades de que se presente una amenaza. ejemplo: Si nos topamos con las instalaciones eléctricas de un edificio antiguo, se pretende que existe riesgo a un nivel elevado acto previsto que sufrirá alguna interrupción de los servicios en caso de producir algún nivel mayor de tensión. (p. 12).

Aguilera (2010). Afirmó que:

Se le denomina riesgos a la supuesta presente que se puede materializar o no en una amenaza donde se aprovecha de una debilidad. No se puede decir riesgo ante una amenaza si no existe vulnerabilidades, ni tampoco si le puede decir vulnerabilidad si no existe la presencia de una amenaza.

Ante la presencia del determinado riesgo, una empresa puede designar por la seleccionar de 3 alternativa diferentes: (A) Asumir sin realizar nada. Esto resulta solamente la lógica cuando el perjuicio no tiene valor esperado alguno o cuando la tarifa de la aplicación de la medida es mayor al de la reparación del daño. (B) Se tiene que aplicar medidas para lograr la disminución o inutilización. (C) El proceso de transferirlo (ejemplo, contrato de un seguro). (p. 14).

Análisis de Riesgos

Aguilera (2010) argumentó sobre los procesos del análisis de riesgo:

Al momento de limitar la seguridad a un sistema informático se tiene que tener presente a todos los componentes previsto que lo conforman, se procede analizar y sistematizar los niveles de vulnerabilidades por cada uno de ellos que se puede presentar algunas amenazas y resaltando el valor del impacto de los ataques que un pueda causar en todo el sistema. (p. 12).

A continuación, se detalla algunos elementos que el autor Aguilera (2010) nos permitirá identificar y clasificar algunas actividades elementales sobre el análisis de riesgos:

Elemento de estudio:

Para iniciar el comienzo del análisis a un sistema de la información nos permitirá pretender llegar a unas medidas sobre la seguridad que se tiene que tener en cuentas los siguientes esquemas: (p. 12).

(1) Activos: “Recursos que son perteneciente al propio sistema de la información o que tiene relación con él. La autenticación de los activos favorece el funcionamiento de la entidad u organización y el logro de su objetivo.” (p. 12).

A continuación, se procede a mencionar las siguientes clasificaciones de los activos que tiene:

Datos: Se establece en el centro principal de la raíz de toda la organización, hasta el punto límite de pensar que los activos están al favor de proteger los datos.

Software: Se establece en la concentración de los sistema operativo y los grupos de aplicaciones que esta instala en los dispositivos proveniente de 1 sistema de la información que recepciona, gestiona o se transforma los dato para finalizar los elementos establecido.

Hardware: Se demuestra que los equipos con características tecnológica llamado servidores y terminales, se confirma que tiene aplicaciones instaladas y funciones que son permitida para almacenar los datos de la información en los sistemas.

Redes: Desde los inicios de las redes locales que conforma una organización hasta los fines elementales metropolitana o internet. Se le puede considera la representación de los medios de conductos de comunicación y transmisión de datos de información a distancia.

Soportes: Fuente principal donde se almacena los registros en un tiempo de periodo largo o si no de una forma de que los datos almacenado sea permanente en un (a) CD, (b) DVD, (c) Tarjeta de memoria, (d) microfilms e incluso papel, (e) disco duro externos dedicado al almacenamiento.

Instalaciones: Lugar donde los sistemas de la información y de las comunicaciones se hospeda. Habitualmente se trata de despacho, oficina, edificio o locales, pero también pueden ser carros y otros medios de deslizamiento.

Personal: Grupo de personas que permitirá la interacción con los sistemas de información como programadores, administradores, usuarios tanto como internos y como externos y resto de personal de la empresa.

Servicios: Es la forma de un servicio que se le ofrece tanto a los usuarios o cliente como los sitios web, productos, servicios, correo electrónico, foros y otros servicios de vía de comunicación, seguridad, información, etc. (p.12 - 13).

(2) Amenazas: La amenaza es la frecuencia de 1 o más factores de diversa personalidad como en (a) personas, (b) maquinas o (c) sucesos, si tuvieran la oportunidad en acceder al sistema, propagarían mucho daño al sistema en el aprovechamiento de su debilidad. Se describe la existencia de otras amenazas que se tiene que cuidar el sistema tanto como físicos, fallas en el hardware, cisuras eléctricas o riesgos climático incluyendo en los errores

intencional o no de aquellos usuarios en el acceso a software de perverso definido como (1) virus, (2) troyanos, (3) gusanos con el hurto, catástrofe o alteración de la información. (p. 13).

Dimensión 1: Riesgos provenientes del Equipo

Según Téllez (2008). describió riesgos en equipo los siguiente:

(A) Proceso de transmisión durante la línea en la pérdida o cambio de mensajes. (B) Se describe la prolongación de un desastre e interrupción siendo de tiempo corto o largo dejando de funcionar el equipo o su línea de comunicación. [...] (C) No realizan respaldo al equipo a la falta de incapacidad en su línea de comunicación y junto con el personal referente a la empresa. (D) Falla de origen del equipo determinando la provocación y suceso de que los datos estén alterado por la falla del equipo con errores, perdida de datos, omiso y otros tipos de problemas. (p. 160).

Dimensión 2: Riesgos provenientes de los programas

Por otro lado, según Téllez (2008). Mencionó los riesgos de los programas lo siguiente:

(A) Fraude o desfalco mediante la afectación de los activos de la empresa (incluida información), por persona no autorizada y en su proyecto, que puede ser un empleado en la compañía o una persona ajena a esta. (B) Robo de programas que ocurrir mediante el apoderamiento físico o por medio del copiado ilícito de estos. (C) Falta de posibilidad de recuperación y reinicio del proceso o comunicación de datos. (D) Modificaciones no autorizadas, ya sean de carácter temporal o permanente o aun las realizadas por personar normalmente autorizado, ya sea por dolo o por imprudencia. (E) Alteración de secuencias. Al no contar con medios para rastrear la información en el proceso de datos, este se puede alterar o perder de manera indebida, la cual provoca, entre otras cosas, complejidad y pérdida de tiempo al tratar de rehacer los movimientos en proceso. (F) Deficiente validación de datos-

programa. Estos es, la edición de datos, la comprobación de cálculos y las acciones específicas que el sistema puede generar y cualquier otra función relacionada con la entrada o salida controlada por programa puede no estar debidamente planteada, lo cual puede hacer que continúe el proceso con base de datos erróneos. (G) Falta de comprobación intermedia. Es decir, la falta de un control debido a los diferentes pasos del proceso puede provocar no estar en condiciones de saber si se procesan bien o no los datos o si no se ha perdido la integridad de la información durante el proceso. (p. 161).

Dimensión 3: Riesgos relacionados con los trabajos

Según Téllez (2008). Clasifico los riesgos relacionados con los trabajos en los siguientes:

Los elementos principales se clasifican según su relación en (A) Los riesgos en los proyectos informáticos. Se procede a realizar un examen con los elementos estadísticos en general donde se expone en reputación la repetición de perjuicio y los problemas que se presenta tanto para las compañías como a sus clientes, dando en la falta de ejecución o deficiencia en el proceso de estos tipos de proyectos. (B) Los riesgos contra los datos. Esta acción son provocados por la devastación voluntaria o inconsciente de los de soportes que dominan la información como los elemento de guardado de discos, cintas, etc. En los cual se ejecuta la desvanecimiento o alteración de los datos de la información. En lo cual también coexiste la publicación deliberado o imprudencial de los datos de la información confidencial existiendo otros tipos de exposiciones representadas por su alto nivel de repercusiones económico relacionada con los datos de una persona o una asunto de la compañía. Este evento se relaciona con la intervención de flujo de acciones y documentos de la información. (C) incitación a los accidentes o intencional de errores y descuidos durante la actividad informático que genere construir información truncada o errónea con el mal trabajo del equipo o cualquier otra irregularidad que sobresalte los archivos de la compañía o falta de vigilancia de los documentos disponibles; esto es la

forma imperceptible de los documentos disponibles como letra de cambio, cheques en el banco, etc. Puede generar su provocada extra vicio o mala manipulación. (D) Acceso Ilícito no autorizado a los sistemas. Los sistemas de acceso no acreditadas a los sistema en progreso y en operaciones exhibe a la compañía y a otra cadena de riesgos como robo, chantaje, fraude, sabotaje, etc.

Acceso no autorizado a las instalaciones. Según lo anterior sobre el acceso no intervenido a los equipos o de lo contrario a sus terminales que representa una posible de nivel muy alta en su modificación o conocimiento de la información íntima.

Se menciona que la protección frente a los riesgos íntegro a agente físicos que exigen durante su proceso de la construcción de los locales sobre el procesamiento a impedir a las exposiciones sobre las radiaciones magnéticas o según electromagnéticas. En esta protección se concierne también con las referentes a los riesgos íntegro a los agentes químicos para que se ejecute de manera completa a las órdenes de protección del usuario y las maquinas. (p. 162).

Para Bustelo (s.f.) Se determino otro argumento sobre el riesgo relacionado con los trabajos que explica a continuación:

“En este nivel estamos tratando los riesgos que pueden sufrir la organización si los documentos dejan de ser auténticos, fiable y si los documentos no se mantienen íntegros y usables todo el tiempo que se necesiten.” (p. 16).

Dimensión 4: Riesgos respecto de las personas

Según Téllez (2008).

Se describe que los riesgos esta entrelazado con la protección para combatir con la existencia de otros riesgos, también en la protección

se incorpora de una forma simultánea la operación de concientizar en la formación y en el control de la seguridad.

La función de concientizado en la informativa y sea acto de presencia sobre los diferentes tipos de peligros a las cuales pueden estar expuesto y que tiene que combatir con las herramientas que pueden estar a su alcance; por eso todos los empleados cualquiera que sea su rango debe de tener conocimiento sobre los reglamento de las clave de la seguridad a la perfección.

Cada personal tiene ser advertido sobre la responsabilidad que tiene uno mismo en herramienta de seguridad con relación a su colaboradores, actividades laboral y los equipos. n). (p. 164).

Seguridad en dispositivo móviles

Para Domingo (2011).

Cuando mencionamos la palabra seguridad es determina una lista de elementos necesario para la identificación de los niveles de protección que se está utilizando. Se tomará como modelo los distintos pasos que se tienen que ejecutar durante el proceso de una llamada telefónica conectado inalámbricamente a una red, donde se podrá identificar los 4 conceptos principal de la seguridad de la información: Confidencialidad, Integridad, Autenticación y el no repudio. (p. 7).

Aguilera (2010). Afirmó:

Un sistema se le puede decir seguro cuando cumpla con las medidas de caracterizadas en la integridad, en la confidencialidad y en la disponibilidad referente a la información. Cada uno de las característica sobrelleva a la integración que se le describe a los servicios y herramienta de seguridad que más adelante se estudiaran. (p. 10).

Dimensión 1: La confidencialidad

Según Domingo (2011). definió que: "Propiedad que asegura aquellas personas que están autorizadas para el acceso a su información, a esto se le denomina como privacidad." (p. 7).

Aguilera (2010). definió la confidencialidad como: "Asegura la protección de los datos contra aparición premeditada o quizás accidental en exponer tu información por medio de una comunicación." (p. 16).

Escrivá, Romero, Ramada y Onrubia (2013). definió: "Aseguramiento en el control de acceso autorizado únicamente aquellos usuarios que puedan acceder y modificar su información." (p. 7).

Dimensión 2: La Integridad

Domingo (2011). "Propiedad que te protege de no alterar tu información guardada. Se describe la palabra alteración que es la acción de ingresar, eliminar o sustituir los datos de tu información." (p. 7)

Aguilera (2010). Determinó la Integridad en "testificar de que los datos estén asegurados en el sistema verificando de que no estén modificados ni tampoco cancelado por personas no autorizadas u otras entidades comprobando que la información de los mensajes haya sido recibida en su totalidad." (p. 16).

Escrivá, Romero, Ramada y Onrubia (2013). Afirmó que: "testificando que tanto la información como los diferentes tipos de técnicas, son procesados en su exactitud y completa totalidad." (p. 7).

Dimensión 3: La Autenticación

Domingo (2011). Definió la autenticación como: "Son las característica que hace una referencia a la relación de su identificación. Es el enlace de la agrupación entre la información y su radiante." (p. 7).

Aguilera (2010). La autenticación

Los programas deberán cumplir en la identificación de los usuarios que accedan a los sistemas o el que quiere una determinada datos de información y es identificado quien decide ser. Solo aquellas entidades o usuario han logrado tener la autenticación al sistema logrando tener acceso autorizado al sistema. Se le aplica la exigencia de autenticar a las entidades de fuente de origen sobre la información en su destino o ambos lados. (p. 16).

Dimensión 4: No repudio

Domingo (2011). Definió el no repudio como: "las cualidades que testificar que ninguna de los eventos no se pueda rechazar ningún compromiso en los eventos ejecutado anteriormente." (p. 7).

Aguilera (2010). Determinó el no repudio como "Proveer al sistema una cadena de eventos incuestionable en las acciones de un evento." (p. 16)

Se puede determinar la palabra no repudio a que hacker que quieren interferir en las conexiones de información que quieren intervenir y el sistema lo detecta y lo excluye fuera de su conexión.

1.4. Formulación del Problema:

1.4.1. Problema General:

¿De qué manera los riesgos informáticos se relacionan con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?

1.4.2. Problema Específicos :

Problema Especifico 1:

¿De qué manera los riesgos informáticos proveniente de los equipos se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?

Problema Especifico 2

¿De qué manera los riesgos informáticos proveniente de los programas se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?

Problema Especifico 3

¿De qué manera los riesgos informáticos relacionados con los trabajos se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?

Problema Especifico 4

¿De qué manera los riesgos informáticos respecto de las personas se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?

1.5. Justificación del Estudio:

1.5.1. Justificación Teórico:

El motivo de mi investigación es porque la inmunidad de la información hackeado es más propensa en dispositivo Android y muy poco en dispositivo iOS haciendo que me enfoque más en Sistemas Operativo Android para la investigación de mi Tesis.

Una de las pruebas es que a nivel mundial el 73.5% por ciento de la población utiliza más el S.O. Android que en vez de iOS, haciendo que el nivel de riesgo este más enfocado en este sistema operativo.

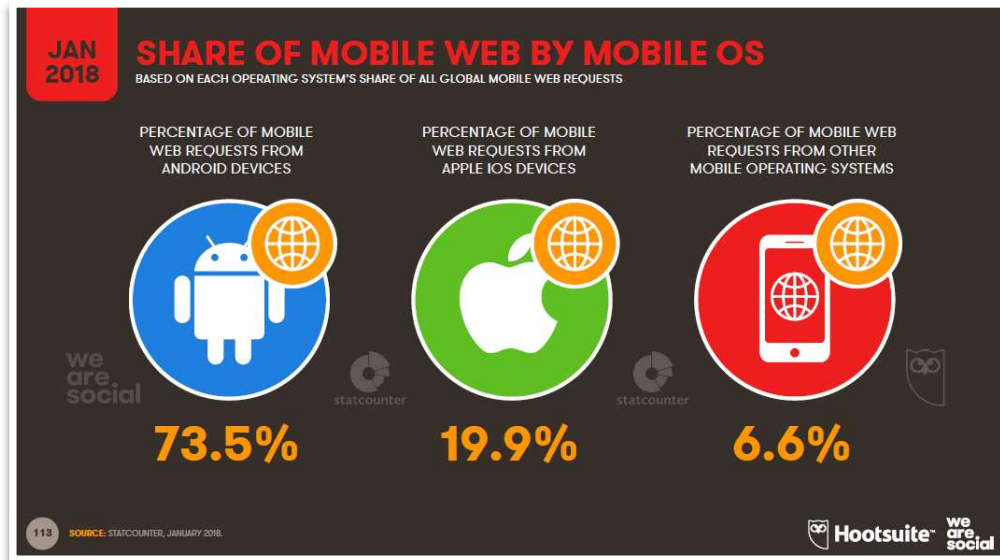


Figura 3: Digital in 2018

Fuente: Digital in 2018, recuperado de: <https://hootsuite.com/es/pages/digital-in-2018#>

1.5.2. Justificación Práctico:

El proyecto lo que quiere es medir la dificultad que existe sobre el robo de información y poder prevenir y salvaguardar la información sobre los dispositivos móviles al momento de usarlo de forma adecuada.

1.5.3. Justificación Metodológica:

Se aplicará una matriz de impacto para medir el nivel de riesgo y dar las prevenciones del dispositivo del usuario para que no poder ser víctima del robo de información.

1.6. Hipótesis:

1.7. Hipótesis General:

Los riesgos informáticos se relacionan se relacionan significativamente en la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019

1.8. Hipótesis Específicas

Hipótesis Especifico 1

Los riesgos informáticos proveniente de los equipos se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019

Hipótesis Especifico 2

Los riesgos informáticos proveniente de los programas se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019

Hipótesis Especifico 3

Los riesgos informáticos relacionados con los trabajos se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019

Hipótesis Especifico 4

Los riesgos informáticos respecto de las personas se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019

1.9. Objetivo:

1.9.1. Objetivo General:

Determinar la relación entre el riesgo informático y la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

1.9.2. Objetivo Especifico:

Objetivo Especifico 1:

Determinar la relación entre los riesgos informático proveniente de los equipos con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Objetivo Especifico 2:

Determinar la relación entre los riesgos informático proveniente de los programas con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Objetivo Especifico 3:

Determinar la relación entre los riesgos informático-relacionados con los trabajos con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Objetivo Especifico 4:

Determinar la relación entre los riesgos informático-respecto de las personas con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

II. Método

2.1. Variable, Operacionalización:

Se ejecutó el proyecto con el fin en determinar la validación y la teoría al describir las variables estudiada junto con sus dimensiones e indicadores.

2.1.1. Variables:

Se presenta y se define las variables del estudio recopilado por mis autores principales del proyecto a continuación se mostrará las variables:

Variable 1: Riesgos Informáticos

Definición conceptual:

Según Téllez (2008) definió los riesgos informáticos como:

Se representa a la incertidumbre o posibilidad de que suceda o se ejecute una casualidad, la cual podría estar pronosticada; en este sentido, que es permitido decir que la palabra riesgo es la posibilidad de que ocurra un daño. (p. 158).

Variable 2: Seguridad en dispositivo móvil

Definición conceptual:

Para Domingo (2011).

Cuando mencionamos la palabra seguridad es determina una lista de elementos necesario para la identificación de los niveles de protección que se está utilizando. Se tomará como modelo los distintos pasos que se tienen que ejecutar durante el proceso de una llamada telefónica conectado inalámbricamente a una red. (p. 7).

2.1.2. Operacionalización de variable:

Variable 1: Riesgos informáticos

Definición Operacional:

A continuación, definirá la operación de la variable riesgo informático y sus dimensiones: Riesgo proveniente del equipo, riesgo proveniente de los programas, riesgo relacionado con los trabajos y riesgo respecto de las personas. Será medidas utilizando los datos recolectados de los estudiantes de la carrera de desarrollo de software.

Tabla 1: Operacionalización de variable Riesgo Informático

Dimensiones	Indicadores	Ítems	Escala de mediciones y valores	Niveles y rangos	
Riesgos Provenientes del Equipos	Nivel de riesgo en resguardo de información	1	1 = Nunca 2 = A veces 3 = Algunas veces 4 = Casi siempre 5 = Siempre	(Alto)	
		2		21	
	Nivel de riesgo sin protección de seguridad	3		-	
		4		49	
Riesgos Provenientes de los programas	Nivel de riesgo en aplicaciones de fuentes desconocida	5	3 = Algunas veces 4 = Casi siempre 5 = Siempre	(Medio)	
		6		50	
		7		-	
	Nivel de riesgo sin protección de Antivirus	8		-	
		9		78	
Riesgos relacionados con los trabajos	Nivel de riesgo en aplicaciones de tiendas no oficiales	10	5 = Siempre	(Bajo)	
		11		79	
	Nivel de riesgo en almacenamiento de Información	12		-	
		13		-	
		14		105	
	Nivel de riesgo en almacenamiento de Memoria	15		5 = Siempre	-
		16			-
		17			-
18		-			
Riesgo respecto de las personas	Nivel de riesgo en las Política de seguridad	19	5 = Siempre	-	
		20		-	
	Nivel de riesgo en protecciones de recomendaciones de seguridad	21		-	

Fuente: Elaboración propia

Variable 2: Seguridad en dispositivo móvil

Definición Operacional

La variable seguridad en dispositivo móvil y sus dimensiones: Confidencialidad, integridad, autenticación, no repudio que será medidas utilizando los datos recolectado por los estudiantes de la carrera de desarrollo de software.

Tabla 2: Matriz de Operacionalización de variable seguridad en dispositivo móvil

Dimensiones	Indicadores	Ítems	Escala de mediciones y valores	Niveles y rangos
Confidencialidad	Nivel de seguridad en la protección de tu Información	1	1 = Nunca	(Bajo)
		2		17
		3		-
	Nivel de seguridad en los accesos de comunicaciones Seguras Nivel de seguridad en la confiabilidad a la nube	4	2 = A veces	39
		5	3 = Algunas veces	(Medio)
		6		40
Integridad	Nivel de seguridad en sistema operativo Nivel de seguridad en los certificados digitales	7	4 = Casi siempre	-
		8		62
	Nivel de permiso de seguridad	9	5 = Siempre	(Alto)
		10		63
Autenticación	Nivel de acceso en las claves de seguridad	11		-
		12		85
		13		
		14		
No repudio	Nivel de seguridad en firma digital Nivel de seguridad en enviar y compartir documentos	15		
		16		
		17		

Fuente: Elaboración propia

2.2. Metodología:

Según Bernal (2010), describió que la hipótesis deductivo: “reside en un proceso que inicia de unas aseveración en calidad de hipótesis y busca contradecir o mentir tales hipótesis, derivando de ellas terminaciones que deben comprobar con hechos reales”. (p. 60).

La metodología es un instrumento que nos permitirá guiar los objetivos claros del estudio del proyecto de investigación deduciéndolo las hipótesis a la necesidad

que se tiene que cumplir en comparar, afirmar o falsear los elementos de la problemática resolviendo estos problemas en los resultados de los datos recolectado en nuestro estudio de investigación.

Por otro lado, Hernández, Fernández y Baptista (2014), clasificó en varios bloques las fases de que conforma la metodología:

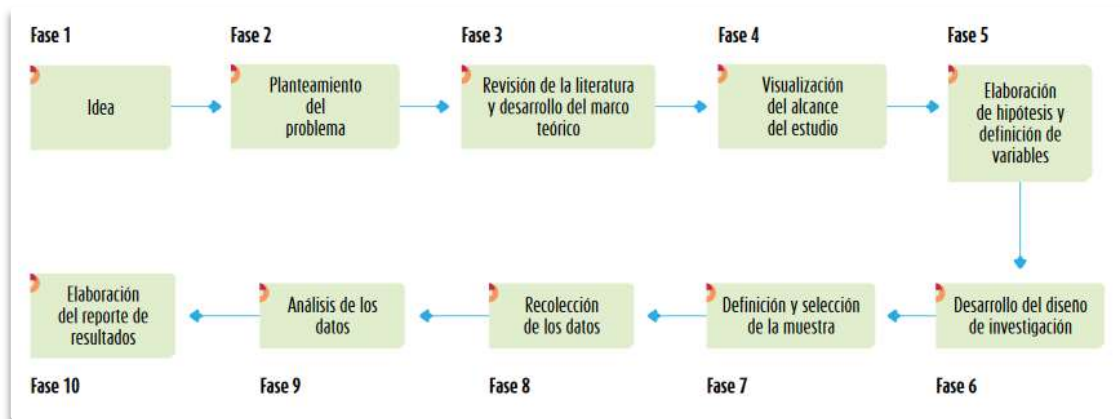


Figura 4: Metodología para enfoque cuantitativo .

Fuente: (Hernández, Fernández y Baptista, 2014, p.5)

Con esta metodología nos permitirá realizar con claridad los objetivo y determinación del estudio de la investigación sobrellevando los elementos de las variables y de las conclusiones de las hipótesis, resolviendo los problemas encontrado en un proyecto dando como resultados recolección de los datos en el análisis y reporte estadístico mostrando como resultado el objetivo de tu proyecto de investigación.

2.3. Tipo de estudio:

Investigación básica

La tesis se basará en una investigación de tipo básica quien el autor Valderrama (2013), definió:

Es conocida también como investigación teórica, pura o fundamental. Está destinada a aportar un cuerpo organizado de conocimientos científicos y no

produce necesariamente resultados de utilidad práctica inmediata. Se preocupa por recoger información de la realidad para enriquecer el conocimiento teórico, científico, orientado al descubrimiento de principios y leyes. (p. 164).

Podemos decir, los métodos científicos de nuestra investigación se pueden clasificar en 3 elementos (a) teórico, (b) pura o (c) fundamental que planteado nos permitirá generar argumentos explícito para entender los objetivos o problemática de la investigación para un resultado positivo o negativos.

Por otro lado, Muños (2014), nos habla sobre el tipo de estudio de investigación básica que sostiene:

La tesis de investigación básica, a través de la aplicación de los métodos formales de investigación, pretenden generar conocimiento científico sobre distintos hechos que interesan a las ciencias particulares o a la filosofía sin buscar lucro o utilidad alguna, salvo la difusión del conocimiento por el propio conocimiento. (p.26).

Tanto Valderrama y Muños coincide en su publicación de su libro sobre el tipo de investigación básica que nos permite generar conocimiento científico para el estudio de una investigación para ambos autores argumentado en sus libros.

Nivel descriptivo:

Según Danhker, (1989), citado en Hernández, Fernández y Baptista, (2006) determinó que la investigación descriptivos “buscan definir las propiedades, características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis”. (p. 81).

Por otro lado, Sabino (2006), señaló que las investigaciones de nivel descriptivas, “se plantean conocer grupos semejantes de fenómenos manejando

criterios sistemáticos que accederán poner de manifiesto su estructura o conducta. Manejando criterios sistemáticos que accederán poner manifiesto en su estructura o comportamiento.” (p. 40).

En conclusión, según los 2 autores describe que la investigación descriptiva nos permitirá realizar el estudio de mi tesis en la población de los estudiantes de la carrera de software para caracterizar los manifiestos del grupo de personas en el comportamiento y recolección de los datos del análisis y fenómeno de aplicar el instrumento a este grupo de población en su manifiesto estructurado según la descripción del homogéneo.

Correlacionales:

Según Hernández, Fernández y Baptista, (2010) definió los estudios de investigación una correlacional planteando “como propósito de conocer la relación o grado de agrupación que exista entre 2 o más conceptos, categorías o variables en un argumento en particular” (p. 81).

Cuantitativo:

Por otro lado, el enfoque de investigación es cuantitativo porque según Hernández, Fernández y Baptista (2011) afirmó “utilizar la recopilación de datos para probar hipótesis fundadas en mediciones numéricas y análisis estáticos, con la finalidad de implantar pautas de comportamiento y comprobar hipótesis” (p.4).

2.4. Diseño de estudio:

El presente proyecto se desarrolló bajo la investigación un enfoque cuantitativo, no experimental, transeccionales, correlacional. Se basa en las observaciones de los hechos en estado natural sin la intervención o manipulación de los investigadores.

Hernández, Fernández y Baptista (2014), se refiere al diseño no experimental: “se trata de estudios en los que no hacemos variar intencionalmente las variables independientes para ver su efecto sobre otras variables” (p. 152).

En lo que se refiere a los diseños transeccionales, Hernández, Fernández y Baptista (2014), afirma que “recolectan datos en un solo momento (en un tiempo único). Tiene como propósito describir variables y analizar su incidencia e interrelación en un momento dado” (p. 154).

Dei (2006) “La investigación es no experimental, los procedimientos más frecuente empleados son la observación y las diversas técnicas de análisis” (p. 66).

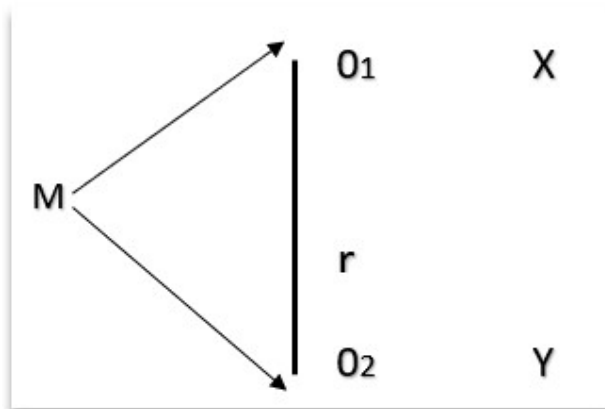


Figura 5: Esquema de tipo de diseño.

Donde:

M : Muestra de estudio

O1 : Riesgos Informáticos

O2 : Seguridad en los dispositivo móvil

O1 y O2 : Puntuaciones de las variables

r : Correlación

Asimismo, en lo referente a los diseños correlacionales, Hernández, Fernández y Baptista (2014), afirma que “describen relaciones entre dos o más categorías, conceptos o variables en un momento dado. A veces, únicamente en términos correlacionales, otras veces en función de la relación causa efecto (causales)” (p. 157).

2.5. Población, muestra y muestreo:

Se procederá argumentar los elementos de la población, muestra y muestreo en la investigación de la tesis.

2.5.1. Población :

Arias (2012), se refiere a la población como “Conjunto limitado o no ilimitado de varios elementos que se define con características frecuentes en las cuales se podrán ser extensiva en sus conclusiones. Esta conforma por un finito por el de los problemas y sus objetivos de la investigación” (p. 81).

En el presente, la población total sobre el objetivo del estudio en la presente investigación que estará conformada por varios grupos de 2, 5, 6 semestre que conforma un grupo total de estudiantes de la institución SENATI.

Tabla 3: Distribución de estudiantes por Semestre.

Semestre	Cantidad de estudiantes.
2 Sem.	30
5 Sem.	19
6 Sem.	17
Total	66

2.5.2. Muestra:

Podemos decir que para Behar (2008), definió los términos de la muestra en los siguientes: “Se afirma que la muestra está conformada por un subgrupo de la población. Se le llamada subconjunto a los elementos que lo relaciona con el conjunto, conceptualizado a las necesidades denominado población” (p. 51). Asimismo, por otro lado Arias (2012), argumento sobre la muestra lo siguientes: “Se dice que la muestra es la representación del subconjunto en un esta concreto que se utiliza de la población en un estado accesible” (p.83).

2.5.3. Muestreo:

A continuación, procederemos a identificar la población total y tamaño de la nueva muestra y Tamayo (1990), citado en Valderrama (2013) aclara las siguientes afirmaciones:

El tamaño de la muestra podrá ser seleccionada por la subpoblación de los cuales se obtendrán los resultados de los datos para luego pueda comprobarse sobre lo verdadero o lo falso todo orientado a la hipótesis en un proceso de extraer e interpretar la deducción sobre el estudio de la población. (p. 188)

Se aplicará el instrumento en la población de 66 estudiantes de la carrera de desarrollo de software el muestreo, pero se aplicará un nuevo cálculo de tamaño de la población pasándolo por un software estadístico “Decision Analyst STATS™ 2.0”; para proceder a ingresar los datos del universo de la población para el calculo proyectado con un margen de 5% de error.

Tamaño de la muestra	Precisión Error máximo aceptable	Porcentaje de estimación	Nivel de confianza
66 estudiantes	5%	50%	95%

The screenshot shows the 'Sample Size Determination' window of the Decision Analyst STATS™ 2.0 software. The 'Inputs' section contains the following values: Universe Size (66), Maximum Acceptable Percentage Points of Error (5%), Estimated Percentage Level (50%), and Desired Confidence Level (95%). The 'Results' section shows 'The Sample Size Should Be...' with the value 56. The software logo and contact information are visible at the bottom.

Figura 6: Total del tamaño de la población

Fuente: Analista de decisiones STATS™ 2.0

Ahora la nueva muestra de toda la población será de **56 estudiantes** de la carrera de desarrollo de software para la institución SENATI.

2.6. Técnica e instrumentos:

2.6.1. Técnica:

Se utilizará una técnica instrumental para el actual estudio de investigación, donde la muestra seleccionada se procederá a realizar una encuesta a cada estudiantes, por lo que mi muestra estará conformada por la cantidad total de mi población, esto lo conforma los estudiantes de la carrera de desarrollo de software de la institución SENATI.

2.6.2. Instrumentos:

El instrumento será aplicado para mi recolección de los datos y beneficio propio de la investigación que se aplicara un cuestionario de preguntas individual a los estudiantes, la cual la muestra se ejecutará a un grupo de estudiantes donde beneficiara a la investigación del estudio a procesar los datos recolectados para los fines de datos estadísticos.

En la ficha se aplicará el instrumento a los estudiantes donde se considera a cada pregunta politómica con una cantidad de cinco alternativas y para cada pregunta utilizaremos un valor utilizando la escala de Likert que nos ayudará a guardar la data de la información que obtenemos como resultado de la muestra recolectada.

Tabla 4: Ficha de instrumento – v1 riesgo informático

Nombre original	Cuestionario Riesgo Informático
Autor	Br. Jose Armando Tiznado Ubillus
Año	2019
Procedencia	Lima – Perú
Tipo de Instrumento	Cuestionario
Objetivo	Recolectar información para determinar la relación entre los Riesgo Informático en el SENATI 2019
Estudiantes	Individual
Aplicación	Directa
Estructura	El instrumento consta de 21 ítems distribuidos con alternativas: 1: Nunca 2: Casi nunca 3: Intermedio 4: Casi siempre 5: Siempre

Fuente: Elaboración propia

Tabla 5: Ficha de instrumento – v2 Seguridad en dispositivo Móvil

Nombre original	Cuestionario Seguridad en dispositivo Movil
Autor	Br. José Armando Tiznado Ubillus
Año	2019
Procedencia	Lima – Perú
Tipo de Instrumento	Cuestionario
Objetivo	Recolectar información para determinar la relación entre los Riesgo Informático en el SENATI 2019
Estudiantes	Individual
Aplicación	Directa
Estructura	El instrumento consta de 17 ítems distribuidos con alternativas: 1: Nunca 2: Casi nunca 3: Intermedio 4: Casi siempre 5: Siempre

Fuente: Elaboración propia

2.6.3. Validez:

Se determinará conformidad de validez de los instrumentos para así usar la recolección de los datos del instrumento para luego ser validado por un juicio de expertos, lo cual se tuvo el apoyo de expertos para su validación del instrumento. A continuación se menciona a los especialistas:

Tabla 6: Especialista para el certificación de validez.

DNI	Grado Académico Apellido y Nombre	Institución donde labora	Calificación
04656793	Doctor en Ingeniería de Sistema Lezama Gonzales, Pedro Martin	UCV	Aplicable
08404620	Magister en Estadístico Torres Cabanillas, Luis Alberto	UCV	Aplicable
10530519	Magister en Gestión Pública y G. Arle Trujillo, Miguel Ángel	UCV	Aplicable

Fuente: Elaboración propia.

Grupo de especialistas validaron el instrumento con los aspectos 3 elemento fundamental (1) claridad, (2) pertinencia y (3) relevancia de los ítems junto con las

dimensiones de que tiene cada variable. Por ambos lados los especialistas coincidieron en que el instrumento se debe optar por aplicar.

2.6.4. Confiabilidad:

Se aplicó el instrumento a los estudiantes un cuestionario para la prueba piloto para lograr determinar la confiabilidad del instrumento si es aceptable, se recolectó la información de 19 encuestados llevándolo a Excel. Se determinó que al pasar por el SPSS aplicando la confiabilidad de Alfa de Cronbach para ambas dimensiones se logró obtener el valor de 0,819 y 0,820

Tabla 7: Estadística de Confiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,819	,820	2

Fuente: Software SPSS 22.

2.7. Métodos de análisis de datos:

En el presente estudio del proyecto de investigación se recolectó los datos de los encuestados realizada a los estudiantes de la institución SENATI, gestionando los datos en el proceso y análisis estadístico del programa SPSS versión 25. Gestionando una serie de pasos como un análisis descriptivo mostrando gráficos de barra juntos con los datos estadístico recolectado con su porcentaje donde se interpretará los que se describirá los objetivos y las afirmaciones de las hipótesis si es aceptable o rechazada.

Se aplicará como objetivo la interpretación del Rho de Spearman sobre los análisis de las hipótesis tanto la general como las específicas teniendo en cuenta uno la aceptación o rechazo según los porcentajes de coeficiente correlacional que muestre.

III. Resultados

3.1. Resultados descriptivos :

3.1.1. Resultado descriptivo de la v1 - Riesgos Informáticos:

Tabla 8: Descripción de los Riesgos Informático

Variable 1: Riesgos Informático				
		Frecuencia	Porcentaje	Porcentaje válido
Valido	Alto	17	(30.4%)	(30.4%)
	Medio	26	(46.4%)	(46.4%)
	Bajo	13	(23.2%)	(23.2%)
Total		56	(100.0%)	(100.0%)

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 7 el resultado de la investigación de tipo descriptivo identificando los niveles de riesgos informáticos con un porcentaje de nivel alto a un 30%, en nivel medio un 46% y nivel bajo 23%.

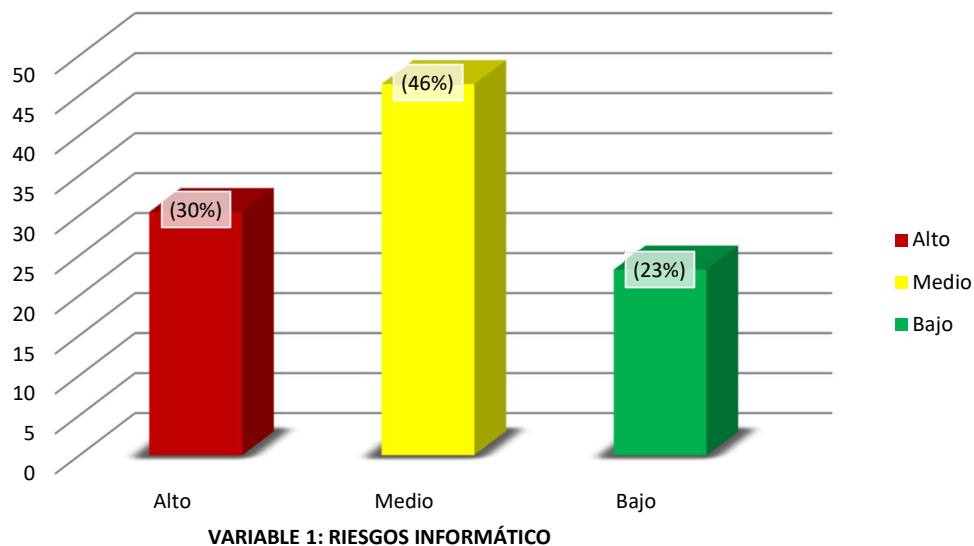


Figura 7: Descripción en porcentaje de los Riesgos Informáticos.

Fuente: Elaboración propia

Se determina que en la figura 8, se identifica que existe riesgo de información a un nivel medio con porcentaje de 30% preocupante para los estudiantes de la carrera de software ante los riesgos que se presenta en su dispositivo móvil.

3.1.2. Resultado descriptivo de la v2 - Seguridad en Dispositivo Móvil:

Tabla 9: Descripción de la Seguridad en los dispositivos Móvil

Variable 2: Seguridad en Dispositivo Móvil					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Valido	Bajo	26	(46.4%)	(46.4%)	(46.4%)
	Medio	21	(37.5%)	(37.5%)	(83.9%)
	Alto	9	(16.1%)	(16.1%)	(100.0%)
Total		56	(100.0%)	(100.0%)	

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 8 el resultado de la investigación de tipo descriptivo identificando los niveles de Seguridad en el dispositivo móvil con los porcentajes de nivel alto a un 46%, en nivel medio un 38% y nivel bajo 16%.

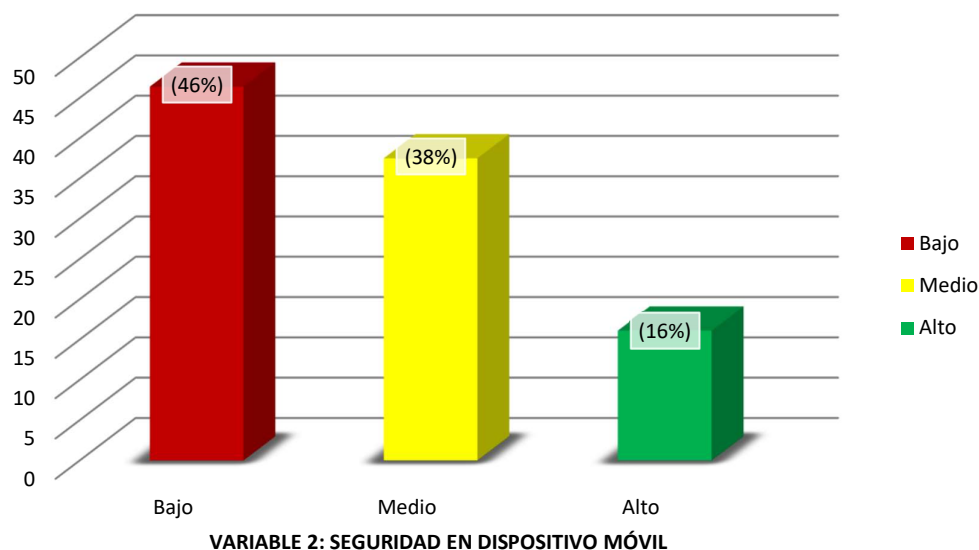


Figura 8: Descripción en porcentaje de los Seguridad en los Dispositivo Móvil.

Fuente: Elaboración propia

Se determina que en la figura 9, se identifica que la seguridad en el dispositivo móvil está a un nivel bajo con porcentaje de 46% preocupante para los estudiantes de la carrera de software ante la inseguridad que se presenta en su dispositivo móvil.

3.1.3. Resultado descriptivo de la dimensión 1 de los Riesgos proveniente del equipo:

Tabla 10: Descripción de los Riesgos proveniente del equipo

Dimensión 1: Riesgos proveniente del equipo					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Valido	Alto	20	(35.7%)	(35.7%)	(35.7%)
	Medio	18	(32.1%)	(32.1%)	(67.9%)
	Bajo	18	(32.1%)	(32.1%)	(100.0%)
Total		56	(100%)	(100%)	

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 9 el resultado de la investigación de tipo descriptivo identificando los niveles de riesgos proveniente del equipo con un porcentaje de nivel alto a un 36%, en nivel medio un 32% y nivel bajo 32%.

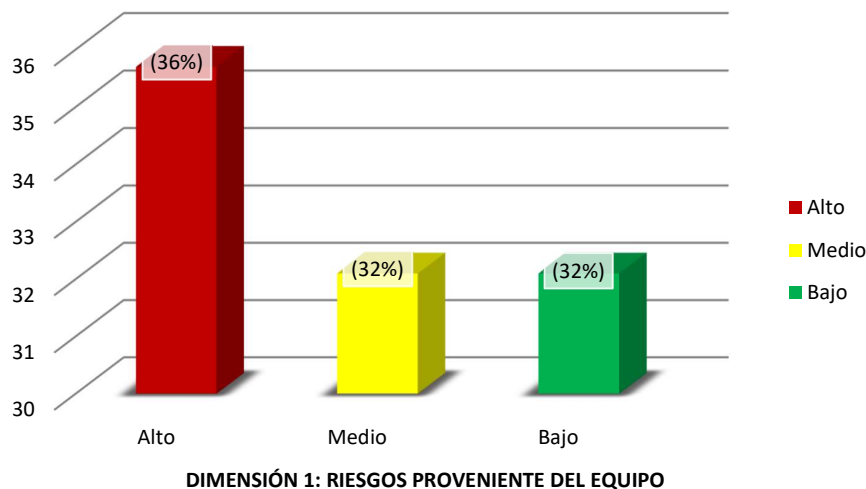


Figura 9: Descripción en porcentaje de los Riesgos proveniente de los equipos.

Fuente: Elaboración propia

Se determina que en la figura 10, se identifica que existe riesgo proveniente del equipo a un nivel alto con porcentaje de 36% preocupante para los estudiantes de la carrera de software ante los riesgos que se presenta en su dispositivo móvil.

3.1.4. Resultado descriptivo de la dimensión 2 de los Riesgos proveniente de los programas:

Tabla 11: Descripción de los Riesgos proveniente de los programas.

Dimensión 2: Riesgos proveniente de los programas					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Valido	Alto	8	(14.3%)	(14.3%)	(14.3%)
	Medio	33	(58.9%)	(58.9%)	(73.2%)
	Bajo	15	(26.8%)	(26.8%)	(100.0%)
Total		56	(100%)	(100%)	

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 10 el resultado de la investigación de tipo descriptivo identificando los niveles de riesgos proveniente de los programas con un porcentaje de nivel alto a un 14%, en nivel medio un 59% y nivel bajo 27%.

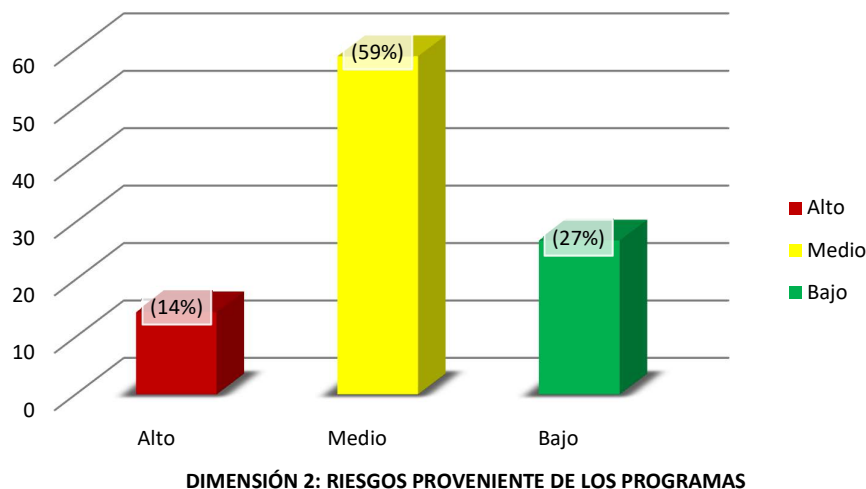


Figura 10: Descripción en porcentaje de los Riesgos proveniente de los programas.

Fuente: Elaboración propia

Se determina que en la figura 11, se identifica que existe riesgo proveniente de los programas a un nivel medio con porcentaje de 59% preocupante para los estudiantes de la carrera de software ante los riesgos que se presenta en su dispositivo móvil.

3.1.5. Resultado descriptivo de la dimensión 3 de los Riesgos relacionado con los trabajos:

Tabla 12: Descripción de los Riesgos relacionado con los trabajos.

Dimensión 3: Riesgos relacionado con los trabajos.					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Valido	Alto	21	(37.5%)	(37.5%)	(37.5%)
	Medio	22	(39.3%)	(39.3%)	(76.8%)
	Bajo	13	(23.2%)	(23.2%)	(100.0%)
Total		56	(100%)	(100%)	

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 9 el resultado de la investigación de tipo descriptivo identificando los niveles de riesgo relacionado con los trabajos con un porcentaje de nivel alto a un 38%, en nivel medio un 39% y nivel bajo 23%.

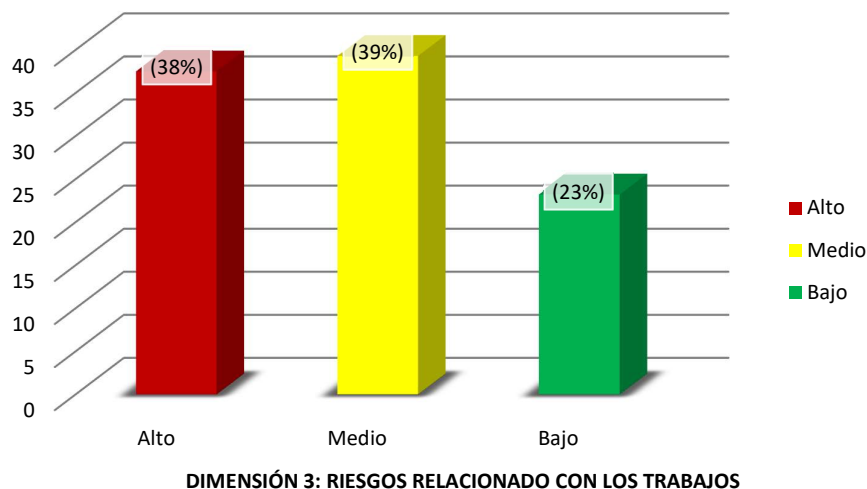


Figura 11: Descripción en porcentaje de los Riesgos relacionado con los trabajos.

Fuente: Elaboración propia

Se determina que en la figura 12, se identifica que existe riesgo de relacionado con los trabajos a un nivel medio con porcentaje de 39% preocupante para los estudiantes de la carrera de software ante los riesgos que se presenta en su dispositivo móvil.

3.1.6. Resultado descriptivo de la dimensión 4 de los Riesgos respecto a las personas:

Tabla 13: Descripción de los Riesgos respecto a las personas.

Dimensión 1: Riesgos respecto a las personas					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Valido	Alto	12	(21.4%)	(21.4%)	(21.4%)
	Medio	17	(30.4%)	(30.4%)	(51.8%)
	Bajo	27	(48.2%)	(48.2%)	(100.0%)
Total		56	(100%)	(100%)	

Fuente: Elaboración propia ejecutado por el SPSS Versión 25

Se determina en la tabla 12 el resultado de la investigación de tipo descriptivo identificando los niveles de riesgos respecto a las personas con un porcentaje de nivel alto a un 21%, en nivel medio un 30% y nivel bajo 48%.

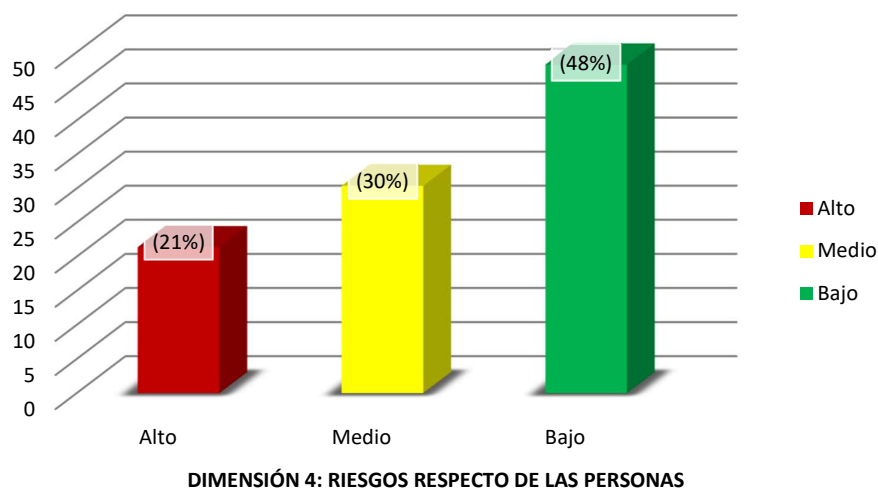


Figura 12: Descripción en porcentaje de los Riesgos respecto a las personas.

Fuente: Elaboración propia

Se determina que en la figura 13, se identifica que existe riesgo respecto a las personas a un nivel bajo con porcentaje de 48%, se puede apreciar una parte de la población que están precavido de los riesgos que los estudiantes de la carrera de software están atento a estos riesgos que se presenta en su dispositivo móvil.

3.2. Prueba de Hipótesis:

3.2.1. Prueba de Hipótesis general:

H1: Los riesgos informáticos tiene relación con la seguridad en el dispositivo móvil en los estudiantes de la carrera de desarrollo de software en SENATI

H0: Los riesgos informáticos no tiene relación con la seguridad en los dispositivos móvil en los estudiantes de la carrera de desarrollo de software en SENATI

Niveles de significancia $\alpha = 0,05$

Normas de decisión:

Si $p < \alpha$; Hipótesis rechazada nula

Si $p > \alpha$; Hipótesis aceptada nula

Tabla 14: Resultado - prueba de correlación Rho Spearman sobre la hipótesis general

		Riesgo Informático	Seguridad D. móvil
Rho de Spearman	Riesgo	1,000	,782**
	informático	.	,000
	N	56	56
Seguridad	D. móvil	,782**	1,000
		,000	.
	N	56	56

** La correlación es significativa en el nivel 0,01 (bilateral).

En el contenido de la tabla 13 se observa los resultados de los datos pasándolo por SPSS generándolo una relación correlacional no paramétrica aplicando Rho Spearman, donde se muestra $r = 0,782$, mostrando que existe relación entre las variables Riesgos informáticos y Seguridad en los dispositivos Móvil de tal forma la investigación del estudio en esta un nivel correlacional positivo alta. Por otro lado, se estima que los valores p (sig. Bilateral) son de 0,00, estando menor al valor α , por lo tanto, entonces hipótesis nula se rechaza.

Entonces la prueba de hipótesis general determinará: Los riesgos informáticos se relacionan significativamente con la seguridad en los dispositivos

móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019, según la información estadístico de la tabla 14.

3.2.2. Prueba de Hipótesis específica 1:

H1: La seguridad en los dispositivos móviles se relacionan significativamente con los riesgos proveniente del equipo en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

H0: La seguridad en los dispositivos móviles no se relacionan significativamente con los riesgos proveniente del equipo en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Niveles de significancia $\alpha = 0,05$

Normas de decisión:

Si $p < \alpha$; Hipótesis rechazada nula

Si $p > \alpha$; Hipótesis aceptada nula

Tabla 15: Resultado - prueba de correlación Rho Spearman sobre la hipótesis específica 1

		Seguridad D. móvil	Riesgo p. de equipo
Rho de Spearman	Seguridad	1,000	,178
	D. móvil	.	,191
	N	56	56
Riesgo p. de equipo	Coeficiente de correlación	,178	1,000
	Sig. (bilateral)	,191	.
	N	56	56

** . La correlación es significativa en el nivel 0,01 (bilateral).

En el contenido de la tabla 14 se observa los resultados de los datos pasándolo por SPSS generándolo una relación correlacional no paramétrica aplicando Rho Spearman, donde se muestra $r = 0,178$, mostrando que no existe relación entre las dimensiones y la variable de los riesgos informático proveniente de los equipos no se relacionan significativamente con la seguridad en los dispositivos móviles de tal forma la investigación del estudio está a un nivel de

correlacional positiva muy baja. Por otro lado, se aprecia que el valor p (sig. Bilateral) es de 0,191, siendo mayor al valor α , por lo que se acepta la hipótesis nula.

Entonces la forma la prueba de hipótesis de la prueba 1 determinará: los riesgos informático proveniente de los equipos no se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019. Los resultados estadísticos muestran que es mayor los valores que alcanza la seguridad en los dispositivos móvil que son mayores que los riesgos provenientes del equipo, según la información estadístico de la tabla 15.

3.2.3. Prueba de Hipótesis específica 2:

H1: La seguridad en los dispositivos móviles se relacionan significativamente con los riesgos proveniente de los programas en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

H0: La seguridad en los dispositivos móviles no se relacionan significativamente con los riesgos proveniente de los programas en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019.

Niveles de significancia $\alpha = 0,05$

Normas de decisión:

Si $p < \alpha$; Hipótesis rechazada nula

Si $p > \alpha$; Hipótesis aceptada nula

Tabla 16: Resultado - prueba de correlación Rho Spearman sobre la hipótesis específica 2

			Seguridad D. móvil	Riesgo p. de los programas
Rho de Spearman	Seguridad	Coefficiente de correlación	1,000	,679**
	D. móvil	Sig. (bilateral)	.	,000
		N	56	56
	Riesgo p. de los programas	Coefficiente de correlación	,679**	1,000
		Sig. (bilateral)	,000	.
		N	56	56

** La correlación es significativa en el nivel 0,01 (bilateral).

En el contenido de la tabla 16 se observa los resultados de los datos pasándolo por SPSS generándolo una relación correlacional no paramétrica aplicando Rho Spearman, donde se muestra $r = 0,679$, mostrando que si existe relación entre las dimensiones y la variable de los riesgos informático proveniente de los programas si se relacionan significativamente con la seguridad en los dispositivos móviles de tal forma la investigación del estudio está a un nivel correlacional moderado. Por otro lado, se aprecia que el valor p (sig. Bilateral) es de 0,000, siendo menor al valor α , por lo tanto, hipótesis nula se rechaza.

Entonces la forma la prueba de hipótesis de la prueba 2 determinará: riesgos informático proveniente de los programas si tiene relación significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019. Los resultados estadísticos muestran que es mayor los valores que alcanza la seguridad en los dispositivo móvil que son mayores que los riesgos proveniente de los programas, según la información estadístico de la tabla 16.

3.2.4. Prueba de Hipótesis específica 3:

H1: La seguridad en los dispositivos móviles se relacionan significativamente con los riesgos relacionados con los trabajos en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019

H0: La seguridad en los dispositivos móviles no se relacionan significativamente con los riesgos relacionados con los trabajos en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019

Niveles de significancia $\alpha = 0,05$

Normas de decisión:

Si $p < \alpha$; Hipótesis rechazada nula

Si $p > \alpha$; Hipótesis aceptada nula

Tabla 17: Resultado - prueba de correlación Rho Spearman sobre la hipótesis específica 3

			Seguridad D. móvil	Riesgo r. con los trabajos
Rho de Spearman	Seguridad	Coefficiente de correlación	1,000	,577**
	D. móvil	Sig. (bilateral)	.	,000
		N	56	56
	Riesgo	Coefficiente de correlación	,577**	1,000
	relacionado	Sig. (bilateral)	,000	.
	con los	N	56	56
	trabajos			

** . La correlación es significativa en el nivel 0,01 (bilateral).

El contenido de la tabla 17 se observa los resultados de los datos pasándolo por SPSS generándolo una relación correlacional no paramétrica aplicando Rho Spearman, donde se muestra $r = 0,577$, mostrando que si existe relación entre las dimensiones y la variable de los Riesgo relacionado con los trabajos si se relacionan significativamente con la seguridad en los dispositivos móviles de tal forma la investigación del estudio está a un nivel correlacional moderado. Por otro lado, se estima que el valor p (sig. Bilateral) es de 0,000, estando menor al valor α , por lo tanto, la hipótesis nula se rechaza.

Entonces la forma la prueba de hipótesis de la prueba 3 determinará: riesgos informáticos relacionado con los trabajos si tiene relación significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019. Los resultados estadísticos muestran que es mayor

los valores que alcanza la seguridad en los dispositivos móviles que son mayores que los riesgos informáticos relacionados con los trabajos, según la información estadística de la tabla 17.

3.2.5. Prueba de Hipótesis específica 4:

H1: La seguridad en los dispositivos móviles se relacionan significativamente con los riesgos respecto de las personas en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019

H0: La seguridad en los dispositivos móviles no se relacionan significativamente con los riesgos respecto de las personas en los estudiantes de la carrera de desarrollo de software en el SENATI, 2019

Nivel de significancia $\alpha = 0,05$

Normas de decisión:

Si $p < \alpha$; Hipótesis rechazada nula

Si $p > \alpha$; Hipótesis aceptada nula

Tabla 18: Resultado - prueba de correlación Rho Spearman sobre la hipótesis específica 4

		Seguridad D. móvil	Riesgo R. a las personas
Rho de Spearman	Seguridad D. móvil	Coeficiente de correlación	1,000
		Sig. (bilateral)	,637**
		N	56
Riesgo respecto a las personas	Coeficiente de correlación	,637**	1,000
	Sig. (bilateral)	,000	.
	N	56	56

** . La correlación es significativa en el nivel 0,01 (bilateral).

El contenido de la tabla 17 se observa los resultados de los datos pasándolo por SPSS generándolo una relación correlacional no paramétrica aplicando Rho Spearman, donde se muestra $r = 0,637$, mostrando que si existe relación entre las dimensiones y la variable de los Riesgo respecto de las personas si se relacionan significativamente con la seguridad en los dispositivos móviles de tal forma la

investigación del estudio está a un nivel correlacional moderado. Por otro lado, se estima que el valor p (sig. Bilateral) es de 0,000, estando menor al valor α , por lo tanto, hipótesis nula es rechazada.

Entonces la forma la prueba de hipótesis de la prueba 4 determinará: riesgos informáticos respecto de las personas si tiene relación significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019. Los resultados estadísticos muestran que es mayor los valores que alcanza la seguridad en los dispositivo móvil que son mayores que los riesgos respecto de las personas, según la información estadístico de la tabla 18.

IV. Discusión

4.1. Discusión:

Se sustenta el objetivo del proyecto de la investigación, fue determinar la relación entre el riesgo informático y la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019. La recolección de los datos fue beneficioso para el resultado del estudio de la investigación, mostro como resultado el coeficiente de correlación de los datos de Rho de Spearman = 0,782, significa que existe una moderada relación positiva entre la relación de las variables 1 y la variable 2 Riesgos informáticos y Seguridad en el dispositivo móvil, frente al (grado de significación estadística) $p < 0,005$, indicando que es rechazada la hipótesis nula.

Se clasifica en 3 niveles la variable 1 en los Riesgo informático que identifico y visualizo los porcentajes en los diferentes niveles, nivel (1) 30% en un nivel alto, nivel (2) 46% en un nivel medio y nivel (3) 23% en un nivel bajo. Resulta que en el proceso de la investigación de mi variable riesgos informáticos se encontró una coincidencia en la investigación de su tesis magistral Otoya (2017) donde los resultados generales de los niveles de la Gestión del riesgo llego a un 63.33% identificando que el nivel es malo, 26.67% identificando que es regular y 10.00% es buena, todo referente con la gestión de riesgo, Por otro lado, Llontop (2018) argumento también que existe una deficiencia pequeña sobre la gestión del riesgo con una cantidad de 9.3% a un nivel deficiente del total. entonces se manifiesta que la afirmación de Téllez (2008) que la palabra riesgo es la posibilidad de que ocurra un daño. [...] cabe manifestar que los riesgos informáticos se referencian a la inseguridad existente por lo que es posible la ejecución de un acontecimiento referenciado con la amenaza de daño con respecto a los bienes o servicios informáticos (p. 158).

A continuación, también se clasifica en 3 niveles sobre la variable 2 en la Seguridad en el dispositivo móvil que se identificó y visualizo los porcentajes en los diferentes niveles, nivel (1) alto a un 46%, en nivel medio un 38% y nivel bajo 16%. Donde se encontró una similitud con el autor Otoya (2017) mostrando como resultados generales de los niveles de Seguridad de la información, donde se muestra estadísticamente los resultados que son: 50.00% donde se perciben que el nivel es Deficiente, 34.17% donde se percibe que es regular y 15.83% es

eficiente. Se argumenta que existe una similitud sobre la seguridad en dispositivo móvil Erreyes (2017) tuvo como objetivo en su metodología seleccionar y aplicar recursos de seguridad en los celulares que le permitirán a usuarios en publico en general a usarlo para la protección de sus datos. Esto lo confirma mi autor Domingo (2011) “Cuando menciona la palabra seguridad en determinar una lista de elementos necesario para la identificación de los niveles de protección que se esta utilizando.” (p. 7).

Por ultimo da entender la comparación de la variable 1 y la variable 2 que identifica que la seguridad es existente con la vulnerabilidad ya que si existe riesgo y si existe riesgo los niveles de la seguridad es propenso a ser victima de una ciberataque y esto lo argumenta López (2016) quien tuvo como el objetivo en su tesis es buscar y localizar las principales vulnerabilidades que existes en los vectores a través de ataques, que hacen débiles a los celulares con Android versión 5.1 lollipop, para mitigar los riesgos encontrados en las actividades de prueba.

Por otro lado, las recomendaciones que menciona mis antecedentes sobre el riesgo y la seguridad envolviéndolo en un análisis que se plantío e identifico que existe una similitud sobre las capacitaciones que se quiere proponer para reforzar y bajar los niveles de riesgos que existe, esto lo confirma Huamán (2017) Se recomienda el presente proyecto de comunicación que permitió tener las bases para construir la cultura de seguridad de la información en el personal administrativo de la PUCP.

V. Conclusiones

5.1. Conclusión:

Primera: Se determino los resultados general de la investigación obtenida en las variables de riesgo informático y seguridad en dispositivo móvil y junto con el objetivo que se logró con la meta de las investigaciones de la tesis concluye en que si existe relación entre la variable 1 y la variable 2 sacando el coeficiente Rho de Spearman = 0,782 y $p = 0,000$ y se detectó que existe riesgo en la información con un 30% a nivel medio y la seguridad está en 46% en un nivel de inseguridad bajo que los estudiantes que está propenso a ser atacado por cybercriminales corriendo el riesgo que pueden ser hackeado la filtración, pérdida o robo de la información confidencial de tu dispositivo móvil.

Segunda: Se determino los resultados del primera dimensión de la investigación obtenida en la dimensión y junto con el objetivo que se logró alcanzar con la meta de las investigaciones en concluir en que no existe correlación entre la dimensión 1 y la variable 2 sacando el coeficiente Rho de Spearman = 0,178 y $p = 0,191$ y se detectó que existe riesgos informático proveniente de los equipos un 36% a nivel alto corriendo riesgo en sus dispositivo móvil en los estudiantes que está propenso a ser atacado por cybercriminales corriendo el riesgo de la pérdida del equipo o robo de la información.

Tercera: Se determino los resultados del segunda dimensión de la investigación obtenida en la dimensión y junto con el objetivo que se logró alcanzar con la meta de las investigaciones en concluir en que si existe correlación entre la dimensión 2 y la variable 2 sacando el coeficiente Rho de Spearman = 0,679 y $p = 0,00$ y se detectó que existe riesgos informático proveniente de los programas un 59% a nivel medio corriendo riesgo en sus dispositivo móvil en los estudiantes que está propenso a ser atacado por cybercriminales corriendo el riesgo una infección de Malware de tu dispositivo móvil.

Cuarto: Se determino los resultados del tercera dimensión de la investigación obtenida en la dimensión y junto con el objetivo que se logró alcanzar con la meta de las investigaciones en concluir en que si existe correlación entre la dimensión 3 y la variable 2 sacando el coeficiente Rho de Spearman = 0, 679 y $p = 0,00$ y se detectó que existe riesgos informático relacionado con los trabajos un 36% a nivel medio corriendo riesgo en sus dispositivo móvil en los estudiantes que está propenso a ser atacado por cybercriminales corriendo el riesgo de la pérdida de los documentos de trabado.

Quinto: Se determino los resultados del cuarta dimensión de la investigación obtenida en la dimensión y junto con el objetivo que se logró alcanzar con la meta de las investigaciones en concluir en que si existe correlación entre la dimensión 4 y la variable 2 sacando el coeficiente Rho de Spearman = 0, 637 y $p = 0,00$ y se detectó que existe riesgos informático respecto a las personas en un 48% a nivel bajo tratan doce de no descuidarse sobre un supuesto riesgo en sus dispositivo móvil en los estudiantes que pueden ser propenso a ser atacado por cybercriminales corriendo el riesgo de la captura de cuenta bancaria por no respetar las políticas de seguridad.

VI. Recomendaciones

6.1. Recomendaciones:

Primera: Se recomienda que se debe aplicar una charla informática tal como se muestra en la *Figura 15* explicándole sobre los nuevos métodos de hackeo a los dispositivos móviles fortaleciendo los niveles alto de seguridad y bajando los niveles de riesgos que ahora actualmente está ocurriendo a nivel mundial sobre la captura de información y cuentas bancarias.

Segunda: Otras de las recomendaciones es hay que tratar de no activar los elementos inalámbricos que tiene nuestro dispositivo móvil al momento de colgarse o acceder a internet por que podemos ser víctima de que nuestro dispositivo móvil pueda ser hackeado.

Tercera: También se recomienda en no descargar o instalar cualquier aplicación no segura a nuestro dispositivo móvil ya que poder ser víctima de malware y deje de responder o perder toda la información confidencial de la integridad de los datos guardados en tu móvil.

Cuarto: Descartar y verificar los permisos de seguridad al momento de la instalación donde los niveles de seguridad podrían ser filtrado por aplicaciones que desean obtener tus datos de tu información capturando tu contraseña o credenciales en tu móvil.

VII. Referencias

- Aguilera P., (2010). *Seguridad Informática*, Madrid. España, Editora Editex, S.A.,
Recuperado de:
<https://books.google.com.pe/books?id=Mgvm3AYIT64C&pg=PA2&dq=riesgo+informatico&hl=es-419&sa=X&ved=0ahUKEwiWrOuMlfrdAhXMt1MKHf1vC1sQ6AEIUzAJ#v=onepage&q=riesgo%20informatico&f=false>
- Arias, F. (2012). "*El proyecto de investigación*, Introducción a la metodología científica." Sexta Edición. Venezuela: Editorial Episteme. ISBN: 980-07-8529-9
- Behar, D. (2008). *Metodología de la investigación*. Editorial Shaloom., ISBN 978-959-212-783-7
- Bernal, C. (2010). *Metodología de la investigación*. Bogotá, Tercera Edición. Bogotá. Colombia., D.C.: Pearson Education Prentice Hall.
- Bustelo C. (s.f.). *Identificación de riesgos en la producción, gestión y mantenimiento de documentos electrónicos.*, Catalunya, España,
Recuperado de: <https://docplayer.es/3714521-Identificacion-de-riesgos-en-la-produccion-gestion-y-mantenimiento-de-documentos-electronicos.html>
- Carcausto W., y Guillen O., (2013). *Guía de SPSS 21.*, Universidad Cesar Vallejo
- Dei D. (2008). *La tesis: Cómo orientarse en su elaboración.*, Tercera Edición. Prometeo Editorial. Buenos Aires.
- Domingo M. (2011). *Seguridad en Dispositivo Móviles.*, España, Create Commons, Recuperado de:
<https://www.lawebdelprogramador.com/pdf/8436-Seguridad-en-Dispositivos-Moviles.html>

- El Comercio (19 de 08 del 2018). *En que consistió el Ciberataque a los bancos peruanos y cómo se repelió.*, Perú., Recuperado de:
<https://elcomercio.pe/tecnologia/actualidad/consistio-ciberataque-bancos-peruanos-repelio-noticia-548181>
- Erreyes D. (2017). *Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles*. Cuenca, Ecuador., (Tesis de Maestría). Universidad de Cuenca., Recuperado de:
<http://dspace.ucuenca.edu.ec/bitstream/123456789/27971/1/3.%20Trabajo%20de%20Titulaci%c3%b3n.pdf>
- Escrivá G., Romero R., Ramada D., y Onrubia R. (2013). *Seguridad Informática.*, Madrid. España, Compañía Macmillan Iberia, S.A., Recuperado de:
<https://ebookcentral.proquest.com/lib/bibliotecasisesp/reader.action?docID=3217398&query=Seguridad+en+dispositivos+m%C3%B3viles>
- Giusto D. (6 Agos, 2018). *Balance Semestral de Seguridad Móvil.*, Recuperado de: <https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/>
- González A. (2018). *Seguridad en Smartphone: Análisis de riesgos, de vulnerabilidades y auditoria de dispositivos* España, (Tesis de Maestría). Universidad de Catalunya., Recuperado de:
<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72966/6/agonzalezfernandez3TFM0118Memoria.pdf>
- Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación*. Sexta Edición. México., McGraw-Hill / Interamericana Editores, S.A de C.V.
- Hernández, R., Fernández, C. y Baptista, P. (2006). *Metodología de la investigación.*, 4ta ed., México., McGraw-Hill /ISBN: 970-10-5753-8

- Hernández, R., Fernández, C. y Baptista, P. (2010). *Metodología de la investigación.*, 5ta ed., México., McGraw-Hill /ISBN: 970-10-5753-8
- Huamán F. (2017). *Plan de comunicaciones en seguridad de la información para el personal administrativo de la pontificia universidad católica del Perú.*, Perú., (Tesis de Maestría). Universidad Católica del Perú., Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/8358/HUAMAN_MONZON_FERNANDO_PLAN.pdf?sequence=1&isAllowed=y
- Kemp S. (2018). *Digital in 2018.*, Recuperado de: <https://hootsuite.com/es/pages/digital-in-2018#>
- La República. (20 de 08 del 2018). *Ataque Cibernético: Conoce cómo sabrás si eres víctima de un hacker.*, Perú., Recuperado de: Recuperado de: <https://larepublica.pe/tecnologia/1300225-ataque-cibernetico-forma-sabras-victima-hacker-ransomware-malware-ataque-udp>
- La República. (18 de 08 del 2018). *Asbanc confirma que ataque financiero mundial afectó al Perú.*, Perú., Recuperado de: <https://larepublica.pe/economia/1300366-asbanc-bancos-peru-sufrieron-ataques-ciberneticos>
- Llontop G. (2018). *Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks.*, Perú., (Tesis de Maestría). Universidad Cesar Vallejo., Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/17596/Llontop_DGC.pdf?sequence=1&isAllowed=y
- López A., (2016). *Aseguramiento de dispositivos Móviles Android para el Cumplimiento de la Norma (PCI - DSS).*, Bogotá. Colombia., (Tesis de Maestría). Universidad Internacional de la Rioja., Recuperado de: <https://reunir.unir.net/bitstream/handle/123456789/4740/LOPEZ%20MARTINEZ%2C%20ANGEL%20DANIEL.pdf?sequence=1&isAllowed=y>

Mosquera E. (26 de 01 del 2016). *Protege tu móvil, es el año del Malware.*, Madrid. España., El Mundo., Recuperado de:
<https://www.elmundo.es/tecnologia/2016/01/26/56a67666ca47418a398b459f.html>

Muñoz, C. (2011). *Cómo elaborar y asesorar una investigación de tesis* "Segunda edición.", México., Pearson educación.

Otoya M. (2017). *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017*, Perú., (Tesis de Maestría). Universidad de UCV., Recuperado de:
<http://repositorio.ucv.edu.pe/handle/UCV/16120?show=full>

Rojas C., (2016). *Evaluación de la seguridad de aplicaciones Móviles Bancarias.*, Santiago de Chile., (Tesis de Maestría). Universidad de Chile., Recuperado de:
<http://repositorio.uchile.cl/bitstream/handle/2250/144529/Evaluaci%C3%B3n-de-la-seguridad-de-aplicaciones-m%C3%B3viles-bancarias.pdf?sequence=1>

Sabino, C. (2006). *Como hacer una tesis*. Caracas. Colombia., Editorial PANAPO de Venezuela.

Senati (2018). *Cisco Advierte sobre nocivos virus y Malware en Empresas.*, Perú., Recuperado de: <http://www.senati.edu.pe/noticias/cisco-advierte-sobre-nocivos-virus-y-malware-en-empresas>

Serra C. (2013). *Herramienta para Evaluar la Gestión de Riesgos.*, CISA CGEIT - ISO 31000:2009, Uruguay, DataSec, Recuperado de:
<https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf>

Téllez J. (2008). *Derecho Informático., 4ta ed.*, México., Instituto de investigación Jurídica, Universidad Nacional Autónoma de México., Recuperado de:
<https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf>

Valderrama, S. (2013). *Pasos para elaborar proyectos de investigación científica.* Lima: Editorial San Marcos.

VIII. Anexos

Anexo 1: Operacionalización de Variables

Operacionalización de variables

Definición Operacional de las Variables	Tipo de Variable	Nombre de la Variable
	Variable 1	Seguridad en dispositivo móviles
	Variable 2	Riesgo Informático

Operacionalización de variables

Definición operacional de las variables	Tipo de Variable	Nombre de la Variable	Dimensiones
	Variable 1	Riesgo Informático	X1. Riesgos provenientes del Equipos
			X2. Riesgos provenientes de los programas
			X3. Riesgos relacionados con los trabajos
			X4. Riesgos respecto de las personas
	Variable 2	Seguridad en dispositivo Móviles	Y1. Confidencialidad
			Y2. Integridad
			Y3. Autenticación
Y4. No Repudio			

Anexo 2: Matriz de Operacionalización de Variable

Operacionalización de Variables

	Tipo de Variable	Nombre de la Variable	Dimensiones	Indicadores
Definición operacional de las variables	Variable 1	Riesgo Informático	X1. Riesgos provenientes del Equipos	1.1 Nivel de riesgo en resguardo de información 1.2 Nivel de riesgo sin protección de seguridad
			X2. Riesgos provenientes de los programas	2.1 Nivel de riesgo en aplicaciones de fuentes desconocida 2.2 Nivel de riesgo sin protección de Antivirus 2.3 Nivel de riesgo en aplicaciones de tiendas no oficiales
			X3. Riesgos relacionados con los trabajos	3.1 Nivel de riesgo en almacenamiento de Información 3.2 Nivel de riesgo en almacenamiento de Memoria 3.3 Nivel de riesgo en activación firewall 3.4 Nivel de riesgo en conexiones a redes externa e internas
			X4. Riesgos respecto de las personas	4.1 Nivel de riesgo en las Política de seguridad 4.2 Nivel de riesgo en protecciones de recomendaciones de seguridad
	Variable 2	Seguridad en dispositivo Móviles	Y1. Confidencialidad	1.1 Nivel de seguridad en la protección de tu Información 1.2 Nivel de seguridad en los accesos de comunicaciones Seguras

				1.3 Nivel de seguridad en la confiabilidad a la nube
			Y2. Integridad	2.1 Nivel de seguridad en sistema operativo 2.2 Nivel de seguridad en los certificados digitales 2.3 Nivel de permiso de seguridad
			Y3. Autenticación	3.1 Nivel de acceso en las claves de seguridad
			Y4. No Repudio	4.1 Nivel de riesgo en las Política de seguridad 4.2 Nivel de riesgo en protecciones de recomendaciones de seguridad

Anexo 3: Tabla de escala de coeficiente de correlación

Tabla 19: Tabla de escala de coeficiente de correlación

Valor	Significado
-1	Correlación negativa grande y perfecta
-0,9 a -0,99	Correlación negativa muy alta
-0,7 a -0,89	Correlación negativa alta
-0,4 a -0,69	Correlación negativa moderada
-0,2 a -0,39	Correlación negativa baja
-0,01 a -0,19	Correlación negativa muy baja
0	Correlación nula
0,01 a 0,19	Correlación positiva muy baja
0,2 a 0,39	Correlación positiva baja
0,4 a 0,69	Correlación positiva moderada
0,7 a 0,89	Correlación positiva alta
0,9 a 0,99	Correlación positiva muy alta
1	Correlación positiva grande y perfecta

Fuente: Guía de SPSS 21 (2013)

MATRIZ DE CONSISTENCIA							
Título: Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019.							
Autor: Jose Armando Tiznado Ubillus							
PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLE E INDICADORES				
Problema General ¿De qué manera los riesgos informáticos se relacionan con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?	Objetivo General Determinar la relación entre el riesgo informáticos y la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.	Hipótesis General: Los riesgos informáticos se relacionan se relacionan significativamente en la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019	Variable 1:	Riesgos Informáticos (Téllez J., 2008)			
			Dimensiones	Indicadores	Ítems	Escala de Medición	Niveles o Rangos
Problema Especifico ¿De qué manera los riesgos informáticos proveniente de los equipos se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?	Objetivo Especifico Determinar la relación entre los riesgos informáticos proveniente de los equipos con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.	Hipótesis Especificas Los riesgos informáticos proveniente de los equipos se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019	Riesgos provenientes del Equipos	1.1 Nivel de riesgo en resguardo de información 1.2 Nivel de riesgo sin protección de seguridad	Ítem 1 Ítem 2 Ítem 3 Ítem 4	1 = Nunca	(Baja)
			Riesgos provenientes de los programas	2.1 Nivel de riesgo en aplicaciones de fuentes desconocida 2.2 Nivel de riesgo sin protección de Antivirus 2.3 Nivel de riesgo en aplicaciones de tiendas no oficiales	Ítem 5 Ítem 6 Ítem 7 Ítem 8 Ítem 9 Ítem 10 Ítem 11		
¿De qué manera los riesgos informáticos proveniente de los programas se relacionan con la seguridad en el dispositivo móvil en	Determinar la relación entre los riesgos informáticos proveniente de los programas con la seguridad en los dispositivos móviles	Los riesgos informáticos proveniente de los programas se relacionan significativamente con la seguridad en los dispositivos	Riesgos relacionados con los trabajos	3.1 Nivel de riesgo en almacenamiento de Información 3.2 Nivel de riesgo en almacenamiento de Memoria 3.3 Nivel de riesgo en activación firewall 3.4 Nivel de riesgo en conexiones a redes externa e internas	Ítem 12 Ítem 13 Ítem 14 Ítem 15 Ítem 16 Ítem 17 Ítem 18	3 = Casi siempre	50 - 78
						4 = Casi siempre	(Alto) 79

estudiantes de la carrera de desarrollo de software en el SENATI, 2019?	en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.	móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019	Riesgos respecto de las personas	4.1 Nivel de riesgo en las Política de seguridad 4.2 Nivel de riesgo en protecciones de recomendaciones de seguridad	Ítem 19 Ítem 20 Ítem 21	5 = Siempre	- 105
			Variable 2:	Seguridad en dispositivo Móvil (Domingo M., 2011)			
¿De qué manera los riesgos informáticos relacionados con los trabajos se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?	Determinar la relación entre los riesgos informáticos relacionados con los trabajos con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.	Los riesgos informáticos relacionados con los trabajos se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019	Dimensiones	Indicadores	Ítems	Escala de Medición	Niveles o Rangos
¿De qué manera los riesgos informáticos respecto de las personas se relacionan con la seguridad en el dispositivo móvil en estudiantes de la carrera de desarrollo de software en el SENATI, 2019?	Determinar la relación entre los riesgos informáticos respecto de las personas con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019.	Los riesgos informáticos respecto de las personas se relacionan significativamente con la seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019	Confidencialidad	1.1 Nivel de seguridad en la protección de tu Información 1.2 Nivel de seguridad en los accesos de comunicaciones Seguras 1.3 Nivel de seguridad en la confiabilidad a la nube	Ítem 1 Ítem 2 Ítem 3 Ítem 4 Ítem 5 Ítem 6	1 = Nunca 2 = A veces	(Baja) 17 - 39 (Moderado)
			Integridad	2.1 Nivel de seguridad en sistema operativo 2.2 Nivel de seguridad en los certificados digitales 2.3 Nivel de permiso de seguridad	Ítem 7 Ítem 8 Ítem 9 Ítem 10	3 = Casi siempre	40 - 62 (Alto)
			Autenticación	3.1 Nivel de acceso en las claves de seguridad	Ítem 11 Ítem 12 Ítem 13 Ítem 14	4 = Casi siempre	63 - 85
			No Repudio	4.1 Nivel de seguridad en firma digital	Ítem 15 Ítem 16	5 = Siempre	

				4.2 Nivel de seguridad en enviar y compartir documentos	Ítem 17		
TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICA E INSTRUMENTO	ESTADÍSTICA PARA UTILIZAR				
<p>Método:</p> <p>Cuestionario con escala de liker, prueba estadística de regresión logística ordinal</p> <p>Enfoque:</p> <p>Cuantitativo</p> <p>Tipo:</p> <p>Tipo básica de nivel descriptivo con enfoque cuantitativo y de</p> <p>Correlacional</p> <p>Diseño:</p> <p>No experimental, transeccional, correlacional</p>	<p>Población:</p> <p>La población o universo de interés en esta investigación, está conformado por 66 estudiantes de la carrera de desarrollo de software de la institución CFP. Luis Cáceres Graziani SENATI, 2019</p> <p>Tipo de muestreo:</p> <p>El tipo de muestreo que se utilizo fue el muestreo aleatorio simple debido a que se conoce el tamaño de la población.</p> <p>Tamaño de muestra:</p> <p>Se aplico la encuesta a un tamaño de 56 estudiantes</p>	<p>Variable 1: Riesgo Informático</p> <p>Variable 2: Seguridad en los dispositivos móviles</p> <p>Instrumento:</p> <ul style="list-style-type: none"> - Cuestionario de riesgo informático. - Cuestionario Seguridad en los dispositivos móviles. <p>Técnica: Ficha de Observación</p> <p>Autor: Jose Tiznado</p>	<p>Programa Informático:</p> <p>SPSS 25</p> <p>Análisis descriptivo:</p> <p>Tabla y gráficos</p> <p>Análisis Inferencial</p> <p>Prueba de confiabilidad</p> <p>Alfa de Cronbach</p> $\alpha = \frac{K}{K-1} \cdot \left[1 - \frac{\sum Vi}{vt} \right] \Rightarrow \text{SPSS 25}$ <p>Prueba de Hipótesis:</p>				

	Autor: Jose Armando Tiznado Ubillus	Año: 2019 Monitoreo: Jose Tiznado Ámbito de Aplicación: SENATI	Rho Spearman
--	--	--	--------------

Anexo 4: Certificado de Validez de Riesgo Informático del Instrumento 1



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL RIESGO INFORMÁTICO

Nº	DIMENSIONES / ítems	Pertinenci a ¹		Relevanci a ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
RIESGOS PROVENIENTES DEL EQUIPOS								
1	¿Con cuanta frecuencia realizas copia de seguridad de toda tu información personal que contiene tu dispositivo móvil?	✓		✓		✓		
2	¿Con que frecuencia realizas copia de seguridad de tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
3	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad para prevenir robos, sustracción de información y otros actos maliciosos?	✓		✓		✓		
4	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad a tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
RIESGOS PROVENIENTES DE LOS PROGRAMAS								
5	¿Habitualmente comprueba la instalación de programas de fuentes no confiable tomando el riesgo de ser infectado de virus a tu dispositivo móvil?	✓		✓		✓		
6	¿Compruebas habitualmente los privilegio administrativo que tiene tu dispositivo móvil en su proceso de instalación?	✓		✓		✓		
7	¿Mides las consecuencias cuando una página web te pide instalar un aplicación de fuente desconocida poniendo en riesgo de una infección de malware a tu dispositivo móvil?	✓		✓		✓		
8	¿Utilizas habitualmente un antivirus en tu dispositivo móvil?	✓		✓		✓		
9	¿Con cuanta frecuencia utiliza tu antivirus para examinar tus aplicaciones y archivo que contiene tu dispositivo móvil?	✓		✓		✓		
10	¿Frecuentemente compruebas que las aplicaciones descargadas e instalas de sitios web no oficiales son seguras para tu dispositivo móvil?	✓		✓		✓		
11	¿Frecuentemente compruebas que las aplicaciones de	✓		✓		✓		

	tiendas no oficiales ya instalada te permite la petición de instalar otras aplicaciones adicionales de fuentes no confiable a tu dispositivo móvil?	✓		✓		✓	
	RIESGOS RELACIONADOS CON LOS TRABAJOS	Si	No	Si	No	Si	No
12	¿Frecuentemente tus archivos almacenados en la memoria interna de tu dispositivo móvil le asignas una contraseña de acceso?	✓		✓		✓	
13	¿Frecuentemente tus archivos almacenados en la memoria externa (SSD) de tu dispositivo móvil le asignas una contraseña de acceso?	✓		✓		✓	
14	¿Frecuentemente has tenido algunos archivos en tu memoria interna o externas modificado o dañado en tu dispositivo móvil sin tu consentimiento?	✓		✓		✓	
15	¿Identifica tu sistema operativo deo de responder, bloqueando todas las funciones del sistema operativo?	✓		✓			
16	¿Con cuanta frecuencia activas tu Firewall de tu dispositivo móvil al momento de navegar por internet?	✓		✓		✓	
17	¿Mides el riesgo al acceder a wifi publicas libre sin contraseña utilizando tu dispositivo móvil para obtener acceso a internet?	✓		✓		✓	
18	¿Mides el riesgo al acceder a wifi privadas en lugares como supermercado, cafetería, trabajo laboral u otros locales utilizando tu dispositivo móvil para obtener acceso a internet?	✓		✓		✓	
	RIESGO RESPECTO DE LAS PERSONAS	Si	No	Si	No	Si	No
19	¿Habitualmente aplicas medidas de seguridad al momento de realizar transacciones bancarias con tu dispositivo móvil?	✓		✓		✓	
20	¿Habitualmente usas los reglamentos de seguridad cuando realizas transacciones bancarias con tu dispositivo móvil?	✓		✓		✓	
21	¿Habitualmente sigues las recomendaciones de seguridad para proteger tus cuentas bancarias, correo, SMS y otros elementos accediendo estos elementos con tu único dispositivo móvil?	✓		✓		✓	

Anexo 5: Certificado de Validez de Seguridad dispositivo móvil del Instrumento 1



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL SEGURIDAD EN DISPOSITIVO MÓVIL

N°	DIMENSIONES / ítems	Pertinenci a ¹		Relevanci a ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
CONFIDENCIALIDAD								
1	¿Habitualmente protege tu información de tu memoria interno y externo ante la confidencialidad de tu dispositivo móvil restringiendo con algún medio de seguridad?	✓		✓		✓		
2	¿Habitualmente encripta tu información confidencial de tu dispositivo móvil como medida de seguridad?	✓		✓		✓		
3	¿Frecuentemente la información guardada en tu memoria externa (SSD) fue protegida ante una extracción y lo pierdes en cualquier parte, sabiendo que tienes información confidencial guardada?	✓		✓		✓		
4	¿Con que frecuencia configura el acceso de comunicaciones por internet con el cifrado de tus datos y comunicación personales desde tu dispositivo móvil?	✓		✓		✓		
5	¿Utiliza frecuente algunas aplicaciones de tiendas oficiales para acceder y transferir a tus datos, archivos, contacto y videos con la confiabilidad de tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
6	¿Utiliza frecuentes conexiones seguras para acceder y transferir tus datos confiable, archivos, contacto y videos a tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
INTEGRIDAD								
7	¿Actualmente actualizas tu sistema operativo de para reforzar la integridad de la seguridad de tu dispositivo móvil?	✓		✓		✓		
8	¿Con cuanta frecuencia identificas los sitios web con certificados digitales en conexiones seguras que tiene cada negador web al momento de realizas una transacción bancaria con tu dispositivo móvil?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Suficiencia

Opinión de aplicabilidad: Aplicable Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Luis Ferrer Caballero

DNI: 08404670

Especialidad del validador: ING. ESTADISTICO CIP 49863

06 de Enero del 2019

PROFE DICE Q PREGUNTAN QUE MIDE LA VALIDEZ DE JUICIO DE EXPERTOS 06-1-19

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión


Firma del Experto Informante

Anexo 6: Certificado de Validez de Riesgo Informático del Instrumento 2



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL RIESGO INFORMÁTICO

Nº	DIMENSIONES / ítems	Pertinencia ^{a1}		Relevancia ^{a2}		Claridad ^{a3}		Sugerencias
		Si	No	Si	No	Si	No	
RIESGOS PROVENIENTES DEL EQUIPOS								
1	¿Con cuanta frecuencia realizas copia de seguridad de toda tu información personal que contiene tu dispositivo móvil?	✓		✓		✓		
2	¿Con que frecuencia realizas copia de seguridad de tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
3	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad para prevenir robos, sustracción de información y otros actos maliciosos?	✓		✓		✓		
4	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad a tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
RIESGOS PROVENIENTES DE LOS PROGRAMAS								
5	¿Habitualmente comprueba la instalación de programas de fuentes no confiable tomando el riesgo de ser infectado de virus a tu dispositivo móvil?	✓		✓		✓		
6	¿Compruebas habitualmente los privilegio administrativo que tiene tu dispositivo móvil en su proceso de instalación?	✓		✓		✓		
7	¿Mides las consecuencias cuando una página web te pide instalar un aplicación de fuente desconocida poniendo en riesgo de una infección de malware a tu dispositivo móvil?	✓		✓		✓		
8	¿Utilizas habitualmente un antivirus en tu dispositivo móvil?	✓		✓		✓		
9	¿Con cuanta frecuencia utiliza tu antivirus para examinar tus aplicaciones y archivo que contiene tu dispositivo móvil?	✓		✓		✓		
10	¿Frecuentemente compruebas que las aplicaciones descargadas e instalas de sitios web no oficiales son seguras para tu dispositivo móvil?	✓		✓		✓		
11	¿Frecuentemente compruebas que las aplicaciones de	✓		✓		✓		

	tiendas no oficiales ya instalada te permite la petición de instalar otras aplicaciones adicionales de fuentes no confiable a tu dispositivo móvil?	✓		✓		✓	
	RIESGOS RELACIONADOS CON LOS TRABAJOS	Si	No	Si	No	Si	No
12	¿Frecuentemente tus archivos almacenados en la memoria interna de tu dispositivo móvil le asignas una contraseña de acceso?	✓		✓		✓	
13	¿Frecuentemente tus archivos almacenados en la memoria externa (SSD) de tu dispositivo móvil le asignas una contraseña de acceso?	✓		✓		✓	
14	¿Frecuentemente has tenido algunos archivos en tu memoria interna o externas modificado o dañado en tu dispositivo móvil sin tu consentimiento?	✓		✓		✓	
15	¿Identifica tu sistema operativo deo de responder, bloqueando todas las funciones del sistema operativo?	✓		✓			
16	¿Con cuanta frecuencia activas tu Firewall de tu dispositivo móvil al momento de navegar por internet?	✓		✓		✓	
17	¿Mides el riesgo al acceder a wifi publicas libre sin contraseña utilizando tu dispositivo móvil para obtener acceso a internet?	✓		✓		✓	
18	¿Mides el riesgo al acceder a wifi privadas en lugares como supermercado, cafetería, trabajo laboral u otros locales utilizando tu dispositivo móvil para obtener acceso a internet?	✓		✓		✓	
	RIESGO RESPECTO DE LAS PERSONAS	Si	No	Si	No	Si	No
19	¿Habitualmente aplicas medidas de seguridad al momento de realizar transacciones bancarias con tu dispositivo móvil?	✓		✓		✓	
20	¿Habitualmente usas los reglamentos de seguridad cuando realizas transacciones bancarias con tu dispositivo móvil?	✓		✓		✓	
21	¿Habitualmente sigues las recomendaciones de seguridad para proteger tus cuentas bancarias, correo, SMS y otros elementos accediendo estos elementos con tu único dispositivo móvil?	✓		✓		✓	

Anexo 7: Certificado de Validez de Seguridad en dispositivo móvil del Instrumento 2



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL SEGURIDAD EN DISPOSITIVO MÓVIL

N°	DIMENSIONES / ítems	Pertinencia ^{a1}		Relevancia ^{a2}		Claridad ^{a3}		Sugerencias
		Si	No	Si	No	Si	No	
CONFIDENCIALIDAD								
1	¿Habitualmente protege tu información de tu memoria interno y externo ante la confidencialidad de tu dispositivo móvil restringiendo con algún medio de seguridad?	✓		✓		✓		
2	¿Habitualmente encripta tu información confidencial de tu dispositivo móvil como medida de seguridad?	✓		✓		✓		
3	¿Frecuentemente la información guardada en tu memoria externa (SSD) fue protegida ante una extracción y lo pierdes en cualquier parte, sabiendo que tienes información confidencial guardada?	✓		✓		✓		
4	¿Con que frecuencia configura el acceso de comunicaciones por internet con el cifrado de tus datos y comunicación personales desde tu dispositivo móvil?	✓		✓		✓		
5	¿Utiliza frecuente algunas aplicaciones de tiendas oficiales para acceder y transferir a tus datos, archivos, contacto y videos con la confiabilidad de tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
6	¿Utiliza frecuentes conexiones seguras para acceder y transferir tus datos confiable, archivos, contacto y videos a tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
INTEGRIDAD								
7	¿Actualmente actualizas tu sistema operativo de para reforzar la integridad de la seguridad de tu dispositivo móvil?	✓		✓		✓		
8	¿Con cuanta frecuencia identificas los sitios web con certificados digitales en conexiones seguras que tiene cada negador web al momento de realizas una transacción bancaria con tu dispositivo móvil?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. Dr/ Mg: Dr. Lezama Gonzales Pedro Martin

DNI: 09656793.....

Especialidad del validador: Ing. de Sistemas.....

PROFE DICE Q PREGUNTAN QUE MIDE LA VALIDEZ DE JUICIO DE EXPERTOS 06-1-19

06 de Enero del 20

- ¹**Pertinencia:** El ítem corresponde al concepto teórico formulado.
- ²**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
- ³**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Firma del Experto Informante

Anexo 8: Certificado de Validez de Riesgo Informático del Instrumento 3



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL RIESGO INFORMÁTICO

Nº	DIMENSIONES / ítems	Pertinenci a ¹		Relevanci a ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
RIESGOS PROVENIENTES DEL EQUIPOS								
1	¿Con cuanta frecuencia realizas copia de seguridad de toda tu información personal que contiene tu dispositivo móvil?	✓		✓		✓		
2	¿Con que frecuencia realizas copia de seguridad de tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
3	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad para prevenir robos, sustracción de información y otros actos maliciosos?	✓		✓		✓		
4	¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad a tus aplicaciones instaladas en tu dispositivo móvil?	✓		✓		✓		
RIESGOS PROVENIENTES DE LOS PROGRAMAS								
5	¿Habitualmente comprueba la instalación de programas de fuentes no confiable tomando el riesgo de ser infectado de virus a tu dispositivo móvil?	✓		✓		✓		
6	¿Compruebas habitualmente los privilegio administrativo que tiene tu dispositivo móvil en su proceso de instalación?	✓		✓		✓		
7	¿Mides las consecuencias cuando una página web te pide instalar un aplicación de fuente desconocida poniendo en riesgo de una infección de malware a tu dispositivo móvil?	✓		✓		✓		
8	¿Utilizas habitualmente un antivirus en tu dispositivo móvil?	✓		✓		✓		
9	¿Con cuanta frecuencia utiliza tu antivirus para examinar tus aplicaciones y archivo que contiene tu dispositivo móvil?	✓		✓		✓		
10	¿Frecuentemente compruebas que las aplicaciones descargadas e instalas de sitios web no oficiales son seguras para tu dispositivo móvil?	✓		✓		✓		
11	¿Frecuentemente compruebas que las aplicaciones de	✓		✓		✓		

Anexo 12: Certificado de Validez de Seguridad en dispositivo móvil del Instrumento 3



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE EL SEGURIDAD EN DISPOSITIVO MÓVIL

N°	DIMENSIONES / ítems	Pertinenci a ¹		Relevanci a ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
CONFIDENCIALIDAD								
1	¿Habitualmente protege tu información de tu memoria interno y externo ante la confidencialidad de tu dispositivo móvil restringiendo con algún medio de seguridad?	✓		✓		✓		
2	¿Habitualmente encripta tu información confidencial de tu dispositivo móvil como medida de seguridad?	✓		✓		✓		
3	¿Frecuentemente la información guardada en tu memoria externa (SSD) fue protegida ante una extracción y lo pierdes en cualquier parte, sabiendo que tienes información confidencial guardada?	✓		✓		✓		
4	¿Con que frecuencia configura el acceso de comunicaciones por internet con el cifrado de tus datos y comunicación personales desde tu dispositivo móvil?	✓		✓		✓		
5	¿Utiliza frecuente algunas aplicaciones de tiendas oficiales para acceder y transferir a tus datos, archivos, contacto y videos con la confiabilidad de tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
6	¿Utiliza frecuentes conexiones seguras para acceder y transferir tus datos confiable, archivos, contacto y videos a tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?	✓		✓		✓		
INTEGRIDAD								
7	¿Actualmente actualizas tu sistema operativo de para reforzar la integridad de la seguridad de tu dispositivo móvil?	✓		✓		✓		
8	¿Con cuanta frecuencia identificas los sitios web con certificados digitales en conexiones seguras que tiene cada negador web al momento de realizas una transacción bancaria con tu dispositivo móvil?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable Aplicable después de corregir No aplicable

Apellidos y nombres del juez validador. Dr/ Mg: MIGUEL ANGEL ARLE TRUSILLO

DNI: 10530519

Especialidad del validador: GESTIÓN PÚBLICA Y GOBERNABILIDAD

PROFE DICE Q PREGUNTAN QUE MIDE LA VALIDEZ DE JUICIO DE EXPERTOS 06-1-19

04 de Enero del 20

- ¹Pertinencia: El ítem corresponde al concepto teórico formulado.
- ²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
- ³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



 Firma del Experto Informante
10530519

Anexo 13: Correlación de dimensiones y variables

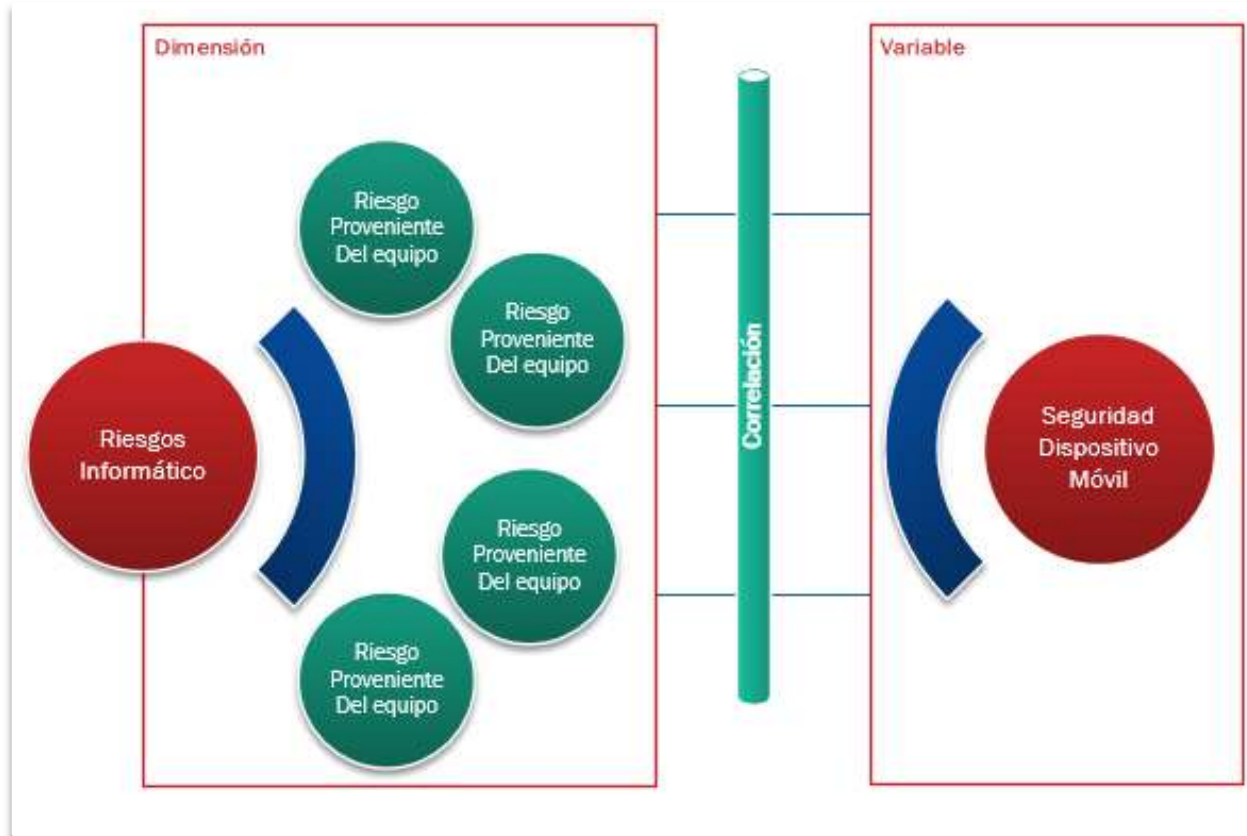


Figura 13: Correlación de Dimensiones y variable
Fuente: Elaboración propia.

Anexo 14: Análisis y objetivo del proyecto

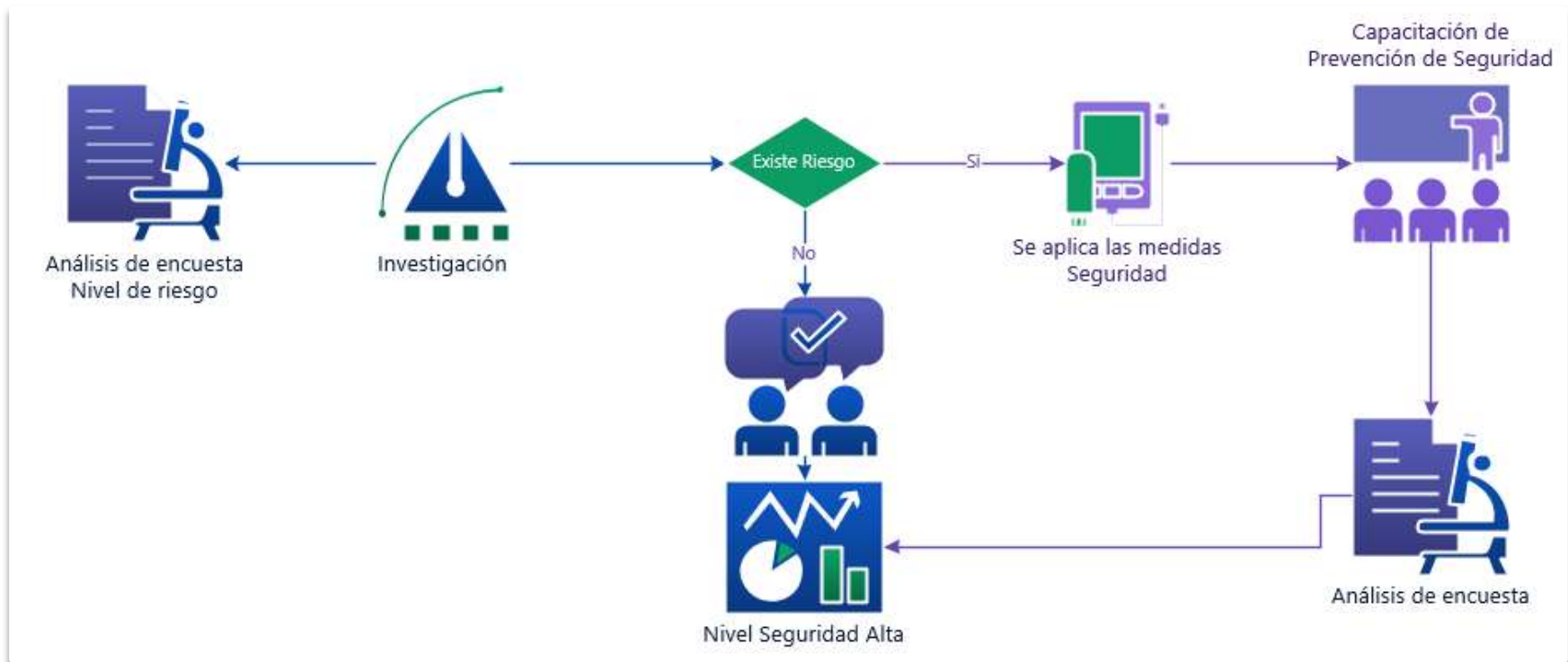


Figura 14: Análisis y objetivo del proyecto.
Fuente: Elaboración propia

2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	2	2	1	2	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	2	1	1	29	3 7
1	2	1	2	1	2	1	2	2	2	2	2	1	1	2	1	1	1	1	3	2	2	1	2	1	2	1	2	1	2	1	2	1	1	1	2	3	2	2	27	3 3				
3	3	2	4	1	1	1	2	2	2	2	2	2	1	2	2	2	1	4	3	2	3	3	5	3	5	4	1	1	1	2	2	2	2	2	1	4	3	2	44	4 4				
2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	1	2	2	5	2	2	2	2	2	2	2	2	2	2	36	3 8	
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	5	2	5	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	41	4 3	
2	3	2	3	2	3	1	2	2	2	2	2	3	2	4	4	4	3	3	2	2	2	3	2	3	2	3	2	3	1	2	2	2	2	5	3	2	2	41	5 3					
2	2	2	2	1	3	2	2	2	2	2	1	4	3	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	3	2	5	1	1	1	1	1	1	2	2	32	4 3			

4 4 5 3 4 4 5 2 2 2 4 3 3 4 5 4 3 3 4 3 4 4 3 3 2 5 4 4 3 4 5 5 5 5 5 4 4 4	6 7								
3 3 5 4 4 3 5 5 4 4 4 5 5 5 5 3 4 4 5 5 5 5 4 2 4 5 5 5 5 5 5 5 5 5 5 5	9 5	16	23	25	11	21	16	20	12
3 2 5 1 3 4 5 1 1 2 4 1 1 4 2 1 5 3 5 5 5 3 1 1 2 4 5 5 5 5 5 5 2 1 1 1 1	8 9								
2 4 5 3 2 2 3 2 2 4 3 1 1 2 2 2 1 1 5 5 3 2 2 2 3 3 2 2 4 5 3 4 5 2 2 3 3 2	0 0	15	29	31	15	25	20	20	15
3 2 3 2 4 3 2 2 2 2 2 3 2 4	4 6								
1 1 5 2 3 2 4 1 1 2 2 1 1 2 3 1 1 1 3 3 2 2 1 2 1 1 4 1 4 5 5 5 5 1 1 3 2 1	8 3	11	20	17	15	16	20	9	3
3 3 5 4 4 3 5 5 4 4 4 5 5 5 5 3 4 4 5 5 5 5 4 2 4 5 5 5 5 5 5 5 5 5 5 5	4 5								
3 2 5 1 3 4 5 1 1 2 4 1 1 4 2 1 5 3 5 5 5 3 1 1 2 4 5 5 5 5 5 5 2 1 1 1 1	9 5	14	18	10	13	14	14	13	8
2 4 5 3 2 2 3 2 2 4 3 1 1 2 2 2 1 1 5 5 3 2 2 2 3 3 2 2 4 5 3 4 5 2 2 3 3 2	5 5								
3 2 3 2 4 3 2 2 2 2 2 3 2 4	1 7	10	17	21	9	18	12	12	9
4 2 5 3 5 4 5 1 1 3 4 2 2 1 1 1 5 4 3 2 4 1 3 5 1 5 4 5 3 1 5 5 5 1 5 1 3 1	4 4								
2 1 5 3 4 3 4 2 3 3 3 2 2 3 3 2 2 2 4 5 3 3 2 3 3 3 3 4 4 4 4 4 4 3 5 1 3 2	4 2	9	15	10	8	11	15	12	6
5 5 4 1 4 2 5 5 5 4 3 1 1 1 1 2 2 2 2 5 5 5 5 5 1 5 5 5 1 1 5 5 5 1 1 1 2	8 9								
4 4 5 5 5 5 5 3 3 5 5 5 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3	0 0	15	29	31	15	25	20	20	15
2 3 4 2 3 2 3 4 3 3 3 2 2 2 3 2 3 2 2 2 2 2 2 1 2 2 2 2 5 2 2 2 4 4 2 3 2 2 2	4 6								
3 4 4 5 3 5 5 2 3 4 5 5 5 4 4 2 2 2 3 5 5 5 4 2 3 4 4 3 3 4 5 5 5 3 2 4 2 3	8 3	11	20	17	15	16	20	9	3
5 5 5 2 4 4 3	4 5								
	9 5	14	18	10	13	14	14	13	8
	5 5								
	1 7	10	17	21	9	18	12	12	9
	5 6								
	4 2	14	23	16	9	19	14	16	5
	5 6								
	5 1	11	22	16	12	17	16	16	6
	5 6								
	4 5	15	28	10	12	26	12	12	4
	4 7								
	5 3	18	31	18	6	12	11	13	9
	4 5								
	1 4	11	21	16	6	11	11	13	6
	6 8								
	1 0	16	27	24	13	22	15	15	9
	4 7								
	2 0	17	23	21	9	8	13	12	9

4 4 5 4 4 4 3 1 1 4 4 1 1 3 4 2 4 4 1 1 1 1 4 3 2 2 2 2 2 2 2 4 5 1 1 1 1 1	3 6								
	6 0	17	21	19	3	14	8	11	3
2 2 5 2 2 2 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 5 3 1 1 1 1 1 1 1 4 4 3 4 1 2 4 5 1 1 1 1 1	3 4								
	6 0	11	13	13	3	12	10	11	3
4 2 5 3 5 4 5 1 1 3 4 2 2 1 1 1 1 5 4 3 2 4 1 3 5 1 5 4 5 3 1 5 5 5 1 5 1 3 1	5 6								
	4 2	14	23	16	9	19	14	16	5
2 1 5 3 4 3 4 2 3 3 3 2 2 3 3 2 2 2 4 5 3 3 2 3 3 3 3 4 4 4 4 4 4 3 5 1 3 2	5 6								
	5 1	11	22	16	12	17	16	16	6
5 5 4 1 4 2 5 5 5 4 3 1 1 1 1 1 2 2 2 2 5 5 5 5 5 1 5 5 5 1 1 5 5 5 1 1 1 1 2	5 6								
	4 5	15	28	10	12	26	12	12	4
3 3 5 5 3 2 5 1 1 1 3 1 1 1 1 1 4 1 1 1 1 4 1 1 1 1 5 1 5 1 5 5 5 1 1 1 1 1	4 4								
	0 5	16	16	10	3	13	12	12	3
4 4 5 5 5 5 5 3 3 5 5 5 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 4 3 3 3 3	4 7								
	5 3	18	31	18	6	12	11	13	9
2 3 4 2 3 2 3 4 3 3 3 2 2 2 3 2 3 2 2 2 2 2 2 1 2 2 2 2 5 2 2 2 4 4 2 3 2 2 2	4 5								
	1 4	11	21	16	6	11	11	13	6
3 4 4 5 3 5 5 2 3 4 5 5 5 4 4 2 2 2 3 5 5 5 4 2 3 4 4 3 3 4 5 5 5 3 2 4 2 3	6 8								
	1 0	16	27	24	13	22	15	15	9
4 4 5 4 4 4 3 1 1 4 4 1 1 3 4 2 4 4 1 1 1 1 4 3 2 2 2 2 2 2 2 4 5 1 1 1 1 1	3 6								
	6 0	17	21	19	3	14	8	11	3
3 1 5 4 2 4 5 1 1 5 5 1 1 1 1 1 1 1 1 1 5 5 5 1 1 1 4 5 5 5 1 5 5 5 5 1 1 5 5 5	6 5								
	0 8	13	23	7	15	17	16	12	15
5 5 5 2 4 4 3 1 1 1 1 1 4 3 3 3 3 3 3 3 3 3	4 7								
	2 0	17	23	21	9	8	13	12	9



ESCUELA DE POSGRADO

UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CESAR VALLEJO
ESCUELA DE POSTGRADO
CUESTIONARIO SOBRE LOS RIESGOS INFORMÁTICO

OBJETIVO:

El cuestionario tiene como objetivo determinar los niveles de riesgo informático que existe en el dispositivo móvil que utilizan los estudiantes de la carrera de desarrollo de software de la institución SENATI

DATOS GENERALES:

Apellido y Nombre: _____

Semestre: 2 Semestre – 5 Semestre – 6 Semestre

INSTRUCCIONES:

Estimados estudiantes, el presente cuestionario, tiene el propósito de recopilar información para medir los niveles de riesgo informático que tiene su dispositivo móvil.

Leer detenidamente cada una de las preguntas y seleccionar los elementos adecuado. Al terminar el cuestionario con las respuestas que seleccionaste nos permitirán a detectar y ayudar en recopilar la informar a que nivel de riesgo correr tu dispositivo móvil tanto en tu información como tu equipo.

Escalas: 1: Nunca

2: Casi nunca

3: Intermedio

4: Casi siempre

5: Siempre

RIESGO INFORMÁTICO

Pregunta	Nunca	Casi nunca	Intermedio	Casi Siempre	Siempre
1.- ¿Con cuanta frecuencia realizas copia de seguridad de toda tu información personal que contiene tu dispositivo móvil?					
2.- ¿Con que frecuencia realizas copia de seguridad de tus aplicaciones instaladas en tu dispositivo móvil?					
3.- ¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad para prevenir robos, sustracción de información y otros actos maliciosos?					
4.- ¿Frecuentemente le asignas a tu dispositivo móvil una contraseña o patrón de seguridad a tus aplicaciones instaladas como (Whatsapp, Facebook y otros) en tu dispositivo móvil?					
5.- ¿Habitualmente comprueba la instalación de programas de fuentes no confiable tomando el riesgo de ser infectado de virus a tu dispositivo móvil?					
6.- ¿Compruebas habitualmente el privilegio administrativo que tiene tu dispositivo móvil en su proceso de instalación?					
7.- ¿Mides las consecuencias cuando una página web te pide instalar una aplicación de fuente desconocida poniendo en riesgo de una infección de malware a tu dispositivo móvil?					
8.- ¿Utilizas habitualmente un antivirus en tu dispositivo móvil?					
9.- ¿Con cuanta frecuencia utiliza tu antivirus para examinar tus aplicaciones y archivo que contiene tu dispositivo móvil?					
10.- ¿Frecuentemente compruebas que las aplicaciones descargadas e instalas de sitios web no oficiales son riesgoso para tu dispositivo móvil?					
11.- ¿Frecuentemente compruebas que las aplicaciones de tiendas no oficiales ya instalada te permite la petición de instalar otras aplicaciones adicionales de fuentes no confiable a tu dispositivo móvil?					
12.- ¿Frecuentemente tus archivos almacenados en la memoria interna de tu dispositivo móvil le asignas una contraseña de acceso restringido?					
13.- ¿Frecuentemente tus archivos almacenados en la memoria externa (SSD) de tu dispositivo móvil le asignas una contraseña de acceso restringido?					
14.- ¿Compruebas frecuentemente los contenidos de tus archivo en tu memoria interna o externas,					

verificando que todos tus contenido no esté alterado o dañado en tu dispositivo móvil sin tu consentimiento?					
15.- ¿Realizas mantenimiento de limpieza a tu memoria RAM para prevenir de posible filtraciones de malware o de las sobrecarga del sistema operativo dejando de responder todas las funcionalidades de tu dispositivo móvil?					
16.- ¿Con cuanta frecuencia activas tu Firewall de tu dispositivo móvil al momento de navegar por Internet?					
17.- ¿Mides el riesgo al acceder a wifi publicas libre sin contraseña utilizando tu dispositivo móvil para obtener acceso a Internet?					
18.- ¿Mides el riesgo al acceder a wifi privadas en lugares como supermercado, cafetería, trabajo laboral u otros locales utilizando tu dispositivo móvil para obtener acceso a Internet?					
19.- ¿Habitualmente aplicas medidas de seguridad al momento de realizar transacciones bancarias con tu dispositivo móvil?					
20.- ¿Habitualmente usas los reglamento de seguridad que los bancos brindan a sus cliente, cuando realizas transacciones bancarias con tu dispositivo móvil?					
21.- ¿Habitualmente sigues las recomendaciones de seguridad que un banco brinda a sus cliente para proteger tus cuentas bancarias, correo, SMS y otros elementos, accediendo a estos elemento con tu dispositivo móvil?					



ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

UNIVERSIDAD CESAR VALLEJO

ESCUELA DE POSTGRADO

CUESTIONARIO SOBRE LA SEGURIDAD EN EL DISPOSITIVO MÓVIL

OBJETIVO:

El cuestionario tiene como objetivo determinar los niveles de seguridad en el dispositivo móvil en los estudiantes de la carrera de desarrollo de software de la institución SENATI

DATOS GENERALES:

Apellido y Nombre: _____

Semestre: 2 Semestre – 5 Semestre – 6 Semestre

INSTRUCCIONES:

Estimados estudiantes, el presente cuestionario, tiene el propósito de recopilar información para medir los niveles de riesgo informático que tiene su dispositivo móvil.

Leer detenidamente cada una de las preguntas y seleccionar los elementos adecuado. Al terminar el cuestionario con las respuestas que seleccionaste nos permitirán a detectar y ayudar en recopilar la información para determinar los niveles de seguridad que tiene tu dispositivo móvil tanto en tu información como tu equipo.

Escalas: 1: Nunca

2: Casi nunca

3: Intermedio

4: Casi siempre

5: Siempre

SEGURIDAD EN DISPOSITIVO MÓVIL

Pregunta	Nunca	Casi Nunca	Intermedio	Casi Siempre	Siempre
1.- ¿Habitualmente protege tu información confidencial que se encuentra en tu memoria interna y externa (SSD) de tu dispositivo móvil restringiéndolo con algún medio de seguridad?					
2.- ¿Habitualmente encrypta tu información confidencial de tu memoria almacenamiento interna de tu dispositivo móvil como medida de seguridad?					
3.- ¿Frecuentemente encryptar la información guardada en tu memoria externa(SSD), separandolo de tu móvil y dejandolo en cualquier parte, sabiendo que tienes información confidencial guardada?					
4.- ¿Con que frecuencia configura el acceso de comunicaciones por Internet con el cifrado de tus datos y comunicación personales segura desde tu dispositivo móvil?					
5.- ¿Utiliza frecuente algunas aplicaciones de tiendas oficiales para acceder y transferir a tus datos, archivos, contacto y vídeos con la confiabilidad de tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?					
6.- ¿Utiliza frecuente conexiones seguras para acceder y transferir tus datos confiable, archivos, contacto y vídeos a tu cuenta oficial de la nube (Gmail, Hotmail, etc), desde tu dispositivo móvil?					
7.- ¿Actualmente actualizas tu sistema operativo de para reforzar la integridad de la seguridad de tu dispositivo móvil?					

8.- ¿Con cuanta frecuencia identificas los sitios web con certificados digitales en conexiones seguras que tiene cada navegador web al momento de realizas una transacción bancaria con tu dispositivo móvil?					
9.- ¿Al momento de realizar una transacción bancaria verificaste si los permiso de seguridad han sido alterado poniendo el peligro la seguridad de tu integridad de tus datos de información de tu dispositivo móvil?					
10.- ¿Al momento de acceder a tus cuentas bancaria, correo y redes sociales, verificaste que no este instalado alguna aplicación que permita alterar los permiso de seguridad en el funcionamiento de tu dispositivo móvil?					
11.- ¿Habitualmente le asignas contraseña o PIN de seguridad a tu dispositivo móvil?					
12.- ¿Habitualmente le asignas patrón de seguridad a tu dispositivo móvil?					
13.- ¿Habitualmente le asignas reconocimiento facial a tu dispositivo móvil por motivo de seguridad?					
14.- ¿Habitualmente le agregas huella dactilar a tu dispositivo móvil por motivo de seguridad?					
15.- ¿Frecuentemente adjuntas documentos confidenciales con firma digital, enviando el documento a terceras personas desde tu dispositivo móvil confirmando la solicitud de tu documento?					
16.- ¿Frecuentemente has enviado documento a terceras personas sin ser rechazado la solicitud de tus documento enviado desde tu dispositivo móvil?					
17.- ¿Frecuentemente encriptas y asignas una contraseña de seguridad, compartiendo tus tus datos de comunicación para envíos de archivo a terceras personas desde tu dispositivo móvil?					



SOLICITUD DE CONSTANCIA DE REALIZACIÓN DE ESTUDIO DE INVESTIGACIÓN
ETI-2019

Solicito: Autorización para la aplicación de instrumento de evaluación.

Estimado Sr. David Racchimick Pérez, Jefe CFP de Luis Cáceres Graziani SENATI ubicado en el departamento de Lima / Callao - distrito Centro de Lima.

En el presente me dirijo a usted para solicitarle la autorización de aplicar mi cuestionario para los estudiantes de la carrera de desarrollo de software, donde recolectare los datos encuestado para analizar y procesar la información que me permitirán determinar los niveles de riesgo y su relación con la seguridad en los dispositivos móviles, esta aplicación le beneficiara a la institución sobre la investigación que vengo realizando en mi proyecto de Tesis para fines de bienes lucrativo.

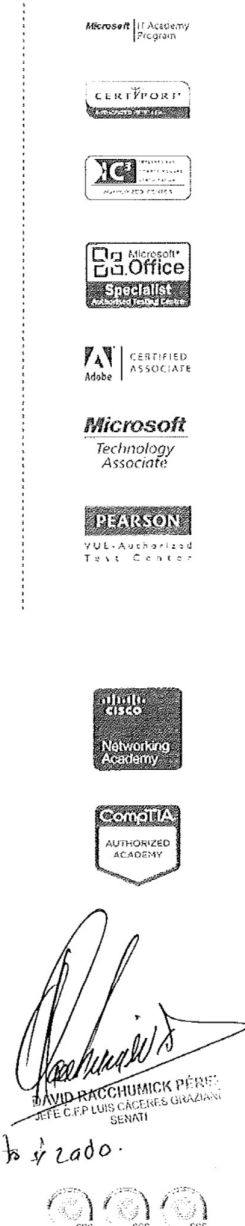
Por lo tanto: Ruego a usted sr. Racchumick a poder acceder a la aprobación de mi solicitud. Gracias.

Atentamente,

[Handwritten Signature]
Firma



Lic. Jose Tiznado Ubillus
Docente C.F.P. Luis Cáceres Graziani
Dirección Zonal Lima – Callao
(511) 622-3434
Av. 28 de Julio 715, Lima, Lima. Perú.
www.senati.edu.pe
f t in



[Handwritten Signature]
DAVID RACCHUMICK PÉREZ
JEFE C.F.P. LUIS CÁCERES GRAZIANI
SENATI
A la y rado.





Dictamen Final

Vista la Tesis:

“RIESGO Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES EN ESTUDIANTES DE LA CARRERA DE DESARROLLO DE SOFTWARE EN EL SENATI, 2019”

Y encontrándose levantadas las observaciones prescritas en el Dictamen, del graduando(a):

TIZNADO UBILLUS, JOSE ARMANDO

Considerando:


Que se encuentra conforme a lo dispuesto por el artículo 36 del REGLAMENTO DE INVESTIGACIÓN DE POSGRADO 2013 con RD N. ° 3902-2013/EPG-UCV, se DECLARA:

Que la presente Tesis se encuentra autorizada con las condiciones mínimas para ser sustentada, previa Resolución que le ordene la Unidad de Posgrado; asimismo, durante la sustentación el Jurado Calificador evaluará la defensa de la tesis y como documento respectivamente, indicando las observaciones a ser subsanadas en un tiempo máximo de seis meses a partir de la sustentación de la tesis.

Comuníquese y archívese.

Lima, 13 de enero del 2019


.....
Dr. César Humberto Del Castillo Talledo
Asesor de la tesis


.....
Dra. Roxana Beatriz Gonzales Huaytahuilca
Revisor de la tesis



Acta de Aprobación de originalidad de Tesis

Yo, **Isabel Menacho Vargas**, tomando conocimiento de la tesis de la estudiante **Jose Armando Tiznado Ubillus "Riesgo y seguridad en los dispositivos móviles en estudiantes de la carrera de desarrollo de software en el SENATI, 2019"**. Constató que la misma tiene un índice de similitud de **23%** verificable en el reporte de originalidad del programa turnitin.

La suscrita analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituye plagio. A mi leal saber y entender, la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la universidad César Vallejo.

Lima, 15 de junio de 2019



DNI: 09968395

Isabel Menacho Vargas

Feedback Studio - Mozilla Firefox
 https://ev.turnitin.com/app/carta/tes/18u=10680324888ro=1038lang=es

feedback studio | Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el...

Resumen de coincidencias 23 %

Se están viendo fuentes estándar

Ver fuentes en inglés (Beta)

Coincidencias	
1	Entregado a Universida... Trabajo del estudiante 9 %
2	repositorio.ucv.edu.pe Fuente de Internet 6 %
3	pt.scribd.com Fuente de Internet 3 %
4	docplayer.es Fuente de Internet 1 %
5	tesis.pucp.edu.pe Fuente de Internet 1 %

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
 Maestría en Ingeniería de Sistemas con mención en Tecnología de la Información

AUTOR:
 Br. José Armando Tiznado Ubillus

ASESOR:
 Dr. César Humberto Del Castillo Taliedo

SECCION:
 Ingeniería

LINEA DE INVESTIGACION:

Página: 1 de 59 Número de palabras: 12711 Text-only Report | High Resolution Activado

Inicio ENTREGA DE TESIS D... Feedback Studio - Mo... Registro - Hojas de C... Tesis poogrado MENDOZA_BA... comp... connetario Turnith... ES 14:55



UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. DATOS PERSONALES

Apellidos y Nombres: (solo los datos del que autoriza)

TIZNADO UBILLUS JOSE ARMANDO

D.N.I. : 43813470

Domicilio : Av. MICHAELA BASILDA - Condominio Torre del Campo F29-605

Teléfono : Fijo : Móvil : 930156057

E-mail : jose_ubillus@hotmail.com

2. IDENTIFICACIÓN DE LA TESIS

Modalidad:

Tesis de Pregrado

Facultad :

Escuela :

Carrera :

Título :

Tesis de Posgrado

Maestría

Grado : Ingeniería de Sistema Doctorado

Mención : Tecnología de la Información

3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres:

TIZNADO UBILLUS JOSE ARMANDO

Título de la tesis:

Riesgo y Seguridad en los Dispositivo Móvil

en los Estudiantes de la Carrera de

Desarrollo de Software en el Senati, 2019

Año de publicación : 2019

4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:

A través del presente documento, autorizo a la Biblioteca UCV-Lima Norte,
a publicar en texto completo mi tesis.

Firma :

Fecha : 25/05/2019



UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

ESCUELA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

Jose Armando Tiznado Ubillus

INFORME TITULADO:

Riesgo y Seguridad en los Dispositivo Móviles

en ESTUDIANTE DE LA CARRERA DE DESARROLLO DE SOFTWARE

en EL SENATI, 2019

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRIA EN INGENIERIA DE SISTEMA con Mención en
Tecnología de LA Información

SUSTENTADO EN FECHA: 29 de Enero del 2019

NOTA O MENCIÓN: APROBADO POR Mayoría



[Handwritten Signature]

FIRMA DEL ENCARGADO DE INVESTIGACIÓN