UNIVERSIDAD DE PANAMÁ
CENTRO REGIONAL UNIVERSITARIO DE VERAGUAS
FACULTAD DE INFORMÁTICA, ELECTRÓNICA Y COMUNICACIÓN

ELABORACIÓN DE POLÍTICAS DE CIBERSEGURIDAD ORIENTADAS A LOS ESTUDIANTES DE LA FIEC-CRUV

POR:
JESÚS JAMIL PINEDA GONZÁLEZ
09-00-0752-01853

TRABAJO DE GRADUACIÓN
PARA OPTAR POR EL TÍTULO DE
LICENCIATURA EN INFORMÁTICA
PARA LA GESTIÓN EDUCATIVA Y EMPRESARIAL

SANTIAGO, REPÚBLICA DE PANAMÁ

2026-02-01

PROFESOR ASESOR:
RAÚL ENRIQUE DUTARI DUTARI, M.SC.
PROFESOR TITULAR III
TIEMPO COMPLETO

CÁTEDRA DE:
REDES DE COMPUTADORAS, SISTEMAS OPERATIVOS
Y ARQUITECTURA DE LOS COMPUTADORES

AGRADECIMIENTO

Primeramente, agradecer a Dios por permitirme culminar con éxitos la Licenciatura.

A mi mamá María Isabel González Jiménez por su constante fe y apoyo desde el primer día.

Al profesor asesor Raúl Enrique Dutari Dutari por su colaboración, guía y apoyo.

RESUMEN DE LA INVESTIGACIÓN

Esta investigación logró identificar el nivel de conocimiento que poseen los estudiantes de la FIEC-CRUV en cuanto a políticas de ciberseguridad para contrarrestar el malware en sus dispositivos móviles y portátiles.

El estudio se desarrolló aplicando un modelo no-experimental. La población objetivo se estudió por medio de la aplicación de un censo. Los datos de la investigación se recolectaron aplicando una sola encuesta orientada a los estudiantes matriculados en todos los grupos de la Facultad de Informática, Electrónica y Comunicación, del Centro Regional Universitario de Veraguas.

Los resultados del censo se valoraron contra un modelo de evaluación basado en la distribución normal. Se comprobó que los estudiantes de la FIEC-CRUV registraron un nivel **alto** de conocimiento en políticas de ciberseguridad.

Palabras clave: nivel de conocimiento, políticas de ciberseguridad, malware, estudiantes de la FIEC-CRUV.

INVESTIGATION SUMMARY

This research successfully identified the level of knowledge that FIEC-CRUV students possess regarding cybersecurity policies to counter malware on their mobile and laptop devices.

The study was conducted using a non-experimental model. The target population was studied through a census. Research data was collected by administering a single survey to students enrolled in all groups of the Faculty of Informatics, Electronics, and Communication at the Veraguas Regional University Center.

The census results were evaluated against a model based on the normal distribution. It was found that FIEC-CRUV students demonstrated a high level of knowledge regarding cybersecurity policies.

Keywords: level of knowledge, cybersecurity policies, malware, FIEC-CRUV students.

ÍNDICE GENERAL

RESUMEN DE LA INVESTIGACIÓN IV

INVESTIGATION SUMMARY V

ÍNDICE GENERAL VI

ÍNDICE DE FIGURAS XIII

ÍNDICE DE TABLAS XIV

ÍNDICE DE GRÁFICOS XVIII

ÍNDICE DE ECUACIONES XXI

1. INTRODUCCIÓN 1

2. MARCO TEÓRICO 3

2.1 EL MALWARE O SOFTWARE MALICIOSO 3

2.1.1 TIPOS DE MALWARE O SOFTWARE MALICIOSO MÁS COMUNES 3

2.2 POLÍTICAS DE CIBERSEGURIDAD 6

2.2.1 EL PAPEL DE LA CIBERSEGURIDAD 7

2.2.2 LEYES EN LA CIBERSEGURIDAD 7

2.2.3 PLAN DE SEGURIDAD INFORMÁTICA 9

2.3 POLÍTICAS DE CIBERSEGURIDAD PERSONAL 12

2.3.1 RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DE DISPOSITIVOS PERSONALES 12

3. GENERALIDADES DEL PROBLEMA 28

3.1 DEFINICIÓN DEL PROBLEMA 28

3.1.1 EL RIESGO DE NO ESTAR PROTEGIDO ANTE EL MALWARE 30

3.2 OBJETIVOS DEL PROYECTO 35

3.2.1 GENERAL 35

3.2.2 ESPECÍFICOS 36

3.3 DELIMITACIÓN O ALCANCE 36

3.4 RESTRICCIONES 36

3.5 JUSTIFICACIÓN 37

3.5.1 ANTECEDENTES Y ESTUDIOS PREVIOS 38

3.6 CONSECUENCIAS DE LA INVESTIGACIÓN 42

3.7 FACTIBILIDAD DEL PROYECTO 42

3.7.1 RECURSOS HUMANOS 43

3.7.2 RECURSOS MATERIALES 43

3.7.3 RECURSOS FINANCIEROS 43

3.8 CRONOGRAMA DE ACTIVIDADES 44

4. MARCO METODOLÓGICO 48

4.1 TIPO DE INVESTIGACIÓN 49

4.2 DISEÑO DE LA INVESTIGACIÓN 50

4.3 CRITERIOS IDENTIFICADOS QUE CONFORMAN EL NIVEL DE CONOCIMIENTO EN CIBERSEGURIDAD EN LOS ESTUDIANTES DEL FIEC-CRUV 50

4.4 HIPÓTESIS DE TRABAJO 51

4.4.1 VARIABLES 51

4.4.2 DEFINICIÓN DE VARIABLES 52

4.5 DISEÑO DEL ESTUDIO 53

4.6 POBLACIÓN 53

4.7 MUESTRA 54

4.8 INSTRUMENTOS DE RECOLECCIÓN DE DATOS 54

4.8.1 ENCUESTA 55

4.8.2 OBSERVACIÓN..... 56

4.9 ANÁLISIS DE DATOS..... 56

4.9.1 PRUEBA DE HIPÓTESIS EN FUNCIÓN A LA HIPÓTESIS DE TRABAJO..... 56

4.10 DISEÑO DEL MODELO DE EVALUACIÓN DE LOS CONOCIMIENTOS QUE TIENEN LOS ESTUDIANTES DEL FIEC-CRUV EN CUANTO A POLÍTICAS DE CIBERSEGURIDAD..... 57

4.10.1 FUNDAMENTOS DEL MODELO DE EVALUACIÓN..... 58

4.10.2 INDICADORES DEL MODELO..... 58

4.10.3 INTERPRETACIÓN DE LOS PESOS QUE SE LE ASIGNÓ A CADA INDICADOR EN CUANTO A POLÍTICAS DE CIBERSEGURIDAD..... 59

4.10.4 MATRIZ DE PONDERACIÓN DE MODELO..... 59

5. PROCESAMIENTO, ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN..... 63

5.1 RESULTADOS DE LA INVESTIGACIÓN 63

5.1.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA..... 63

5.1.2 EXPOSICIÓN DE INFORMACIÓN PERSONAL EN INTERNET 65

5.1.3 TERMINOLOGÍA BÁSICA DE CIBERSEGURIDAD 66

5.1.4 CONOCIMIENTOS FORMALES DE SEGURIDAD INFORMÁTICA 67

5.1.5 CONTROL DE CLAVES DE ACCESO 68

5.1.6 MÉTODOS DE RECUPERACIÓN EFECTIVOS 69

5.1.7 SUPERVISIÓN DE INFORMACIÓN MEDIANTE APLICACIONES..... 70

5.1.8 IDEAS PARA SALVAGUARDAR DATOS PERSONALES..... 71

5.1.9 SOFTWARE DE APOYO CONTRA WEBS MALICIOSAS..... 72

5.1.10 IDENTIFICACIÓN DE MALFUNCIONAMIENTO EN SISTEMAS..... 73

5.1.11 ACTUALIZACIÓN DE SOFTWARE 74

5.1.12 GESTIÓN DE CONTRASEÑAS..... 75

5.1.13 RAZONAMIENTO ANTE ATAQUES POTENCIALES..... 76

5.1.14 COMODIDAD ANTE SOFTWARE DE DUDOSA PROCEDENCIA..... 77

5.1.15 RESPONSABLE PRINCIPAL ANTE SOFTWARE MALICIOSO 78

5.2 RESULTADOS GLOBALES 79

6. CONTRIBUCIONES, LIMITACIONES Y PROYECCIONES FUTURAS 82

6.1 APORTES CONCRETADOS 82

6.1.1 POLÍTICAS DE CIBERSEGURIDAD PERSONAL COMPENDIADAS 82

6.1.2 NIVEL DE CONOCIMIENTO EN POLÍTICAS DE CIBERSEGURIDAD PARA CONTRARRESTAR EL MALWARE 84

6.2 LIMITANTES RELEVANTES DENTRO DEL ESTUDIO 84

6.3 PROYECTOS DERIVADOS DE ESTA INVESTIGACIÓN 85

7. CONCLUSIONES 85

8. RECOMENDACIONES 87

9. REFERENCIAS BIBLIOGRÁFICAS 87

10. APÉNDICES 97

10.1 ENCUESTA APLICADA A LOS ESTUDIANTES DE LA FIEC-CRUV 97

10.2 RESULTADOS ACERCA DE LA ENCUESTA QUE SE APLICÓ A LOS ESTUDIANTES DE LA CRUV-FIEC CON RELACIÓN AL TEMA SOBRE EL NIVEL DE CONOCIMIENTO EN CIBERSEGURIDAD PARA CONTRARRESTAR EL MALWARE EN DISPOSITIVOS MÓVILES Y PORTÁTILES 102

10.3 SOLICITUD DE INFORMACIÓN ESTADÍSTICA DE LA POBLACIÓN DE LA FIEC-CRUV, A LA SECRETARÍA ACADÉMICA DEL CRUV..... 110

ÍNDICE DE FIGURAS

FIGURA 1: VENTA DE ACCIONES, BONO O INVERSIONES DEL BANCO GENERAL 23

FIGURA 2: DISTRIBUCIÓN NORMAL PARA LOS RANGOS DEL MODELO DE EVALUACIÓN 62

FIGURA 3: NOTA DE RESPUESTA DE LA SECRETARÍA ACADÉMICA DEL CRUV 110

ÍNDICE DE TABLAS

TABLA 1: PRESUPUESTO SEMANAL DE GASTOS DEL PROYECTO 44

TABLA 2: CRONOGRAMA DE ACTIVIDADES: SELECCIÓN DEL TEMA, REVISIÓN BIBLIOGRÁFICA, INVESTIGACIÓN DOCUMENTAL 45

TABLA 3: CRONOGRAMA DE ACTIVIDADES: ELABORACIÓN DEL MARCO TEÓRICO, PRUEBA DE CAMPO, ANÁLISIS ESTADÍSTICO 46

TABLA 4: CRONOGRAMA DE ACTIVIDADES: REVISIONES FINALES Y SUSTENTACIÓN..... 47

TABLA 5: CRONOGRAMA DE ACTIVIDADES: COSTO POR ACTIVIDAD 48

TABLA 6: PRESUPUESTO ESTIMADO POR TIPO DE GASTO 48

TABLA 7: DEFINICIÓN DE VARIABLES..... 52

TABLA 8: POBLACIÓN ESTIMADA OBJETO DE INVESTIGACIÓN..... 54

TABLA 9: INDICADORES DEL MODELO DE EVALUACIÓN..... 59

TABLA 10: MATRIZ DE PONDERACIÓN DEL NIVEL DE CONOCIMIENTO QUE TIENEN LOS ESTUDIANTES DEL FIEC-CRUV EN CUANTO A CIBERSEGURIDAD EN DISPOSITIVOS MÓVILES Y PORTÁTILES 60

TABLA 11: RESULTADOS PRINCIPALES GLOBALES 80

TABLA 12: PREGUNTA1: ¿RECONOCE EL CONCEPTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA?..... 103

TABLA 13: PREGUNTA 2: ¿IDENTIFICA LOS RIESGOS ASOCIADOS CON LA EXPOSICIÓN DE SU INFORMACIÓN PERSONAL O LA DE TERCEROS EN INTERNET? 103

TABLA 14: PREGUNTA 3: ¿CONOCE LA DEFINICIÓN DE AL MENOS UNO DE LOS SIGUIENTES TÉRMINOS KEYLOGGER, PHISHING, SPYWARE, RANSOMWARE, ADWARE, TROYANO, GUSANO INFORMÁTICO? 104

TABLA 15: PREGUNTA 4: ¿HA RECIBIDO CAPACITACIÓN FORMAL SOBRE SEGURIDAD INFORMÁTICA, YA SEA A TRAVÉS DE CURSOS, TALLERES, SEMINARIOS O PROGRAMAS DE FORMACIÓN? 104

TABLA 16: PREGUNTA 5: ¿MANTIENE O LLEVA ALGÚN TIPO DE CONTROL PARA GESTIONAR TODAS SUS CONTRASEÑAS EN CASO DE OLVIDARLAS? 105

TABLA 17: PREGUNTA 6: ¿UTILIZA ALGUNA DE ESTAS OPCIONES COMO COPIA DE SEGURIDAD EN CASO DE PERDER SU INFORMACIÓN PERSONAL O DE TERCERO? DISCOS EXTRAÍBLES, MEMORIAS USB, SISTEMA DE RESPALDO EN LA NUBE..... 105

TABLA 18: PREGUNTA 7: ¿REALIZA ESCANEOS CONSTANTES DE SUS CORREOS ELECTRÓNICOS, APLICACIONES O ARCHIVOS COMPARTIDOS, UTILIZANDO ALGÚN ANTIVIRUS O DE FORMA MANUAL? 106

TABLA 19: PREGUNTA 8: ¿CUENTA USTED CON ALGUNA ESTRATEGIA PARA POSIBLES INCIDENTES QUE AMENACEN EL ESTADO DE SU PRIVACIDAD O LA SEGURIDAD DE SUS DOCUMENTOS PERSONALES QUE SE PUEDAN ENCONTRAR EN DISPOSITIVOS MÓVILES O PORTÁTILES?..... 106

TABLA 20: PREGUNTA 9: ¿UTILIZA APLICACIONES O EXTENSIONES EN NAVEGADORES QUE LE FACILITEN SABER SI ESTÁ INTENTANDO ACCEDER A UNA PÁGINA WEB SOSPECHOSA?..... 107

TABLA 21: PREGUNTA 10: ¿ES USTED CAPAZ DE IDENTIFICAR CUANDO SU DISPOSITIVO MÓVIL O PORTÁTIL NO ESTÁ FUNCIONANDO DE MANERA ÓPTIMA? 107

TABLA 22: PREGUNTA 11: ¿CONSIDERA USTED QUE LOS SISTEMAS OPERATIVOS Y APLICACIONES NECESARIAMENTE DEBEN ESTAR ACTUALIZADOS A SU ÚLTIMA VERSIÓN?..... 108

TABLA 23: PREGUNTA 12: ¿QUÉ TAN DE ACUERDO ESTÁ USTED EN QUE LAS CONTRASEÑAS DEBERÍAN SER CAMBIADAS CADA 90 DÍAS?..... 108

TABLA 24: PREGUNTA 13: ¿QUÉ TAN PROBABLE ES QUE SEPA IDENTIFICAR CUANDO ESTÁ SIENDO TENTADO A UNA ESTAFA A TRAVÉS DE CORREOS ELECTRÓNICOS, PUBLICIDADES O ALGÚN OTRO MEDIO?..... 108

TABLA 25: PREGUNTA 14: ¿QUÉ TAN SEGURO Y CÓMODO SE SIENTE AL TENER INSTALADO APLICACIONES DE DUDOSA PROCEDENCIA EN SU DISPOSITIVO MÓVIL O COMPUTADORA PORTÁTIL? 109

TABLA 26: PREGUNTA 15: ¿QUIÉN CONSIDERA QUE ES MÁS IMPORTANTE PARA MANTENER EN BUEN ESTADO LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES O COMPUTADORAS PORTÁTILES, EL USUARIO, ANTIVIRUS O AMBOS? 109

ÍNDICE DE GRÁFICOS

GRÁFICO 1: ¿RECONOCE EL CONCEPTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA? 64

GRÁFICO 2: ¿IDENTIFICA LOS RIESGOS ASOCIADOS CON LA EXPOSICIÓN DE SU INFORMACIÓN PERSONAL O LA DE TERCEROS EN INTERNET? 65

GRÁFICO 3: ¿CONOCE LA DEFINICIÓN DE AL MENOS UNO DE LOS SIGUIENTES TÉRMINOS KEYLOGGER, PHISHING, SPYWARE, RANSOMWARE, ADWARE, TROYANO, GUSANO INFORMÁTICO? 66

GRÁFICO 4: ¿HA RECIBIDO CAPACITACIÓN FORMAL SOBRE SEGURIDAD INFORMÁTICA, YA SEA A TRAVÉS DE CURSOS, TALLERES, SEMINARIOS O PROGRAMAS DE FORMACIÓN? 67

GRÁFICO 5: ¿MANTIENE O LLEVA ALGÚN TIPO DE CONTROL PARA GESTIONAR TODAS SUS CONTRASEÑAS EN CASO DE OLVIDARLAS?..... 68

GRÁFICO 6: ¿UTILIZA ALGUNA DE ESTAS OPCIONES COMO COPIA DE SEGURIDAD EN CASO DE PERDER SU INFORMACIÓN PERSONAL O DE TERCERO? DISCOS EXTRAÍBLES, MEMORIAS USB, SISTEMA DE RESPALDO EN LA NUBE..... 69

GRÁFICO 7: ¿REALIZA ESCANEOS CONSTANTES DE SUS CORREOS ELECTRÓNICOS, APLICACIONES O ARCHIVOS COMPARTIDOS, UTILIZANDO ALGÚN ANTIVIRUS O DE FORMA MANUAL? 70

GRÁFICO 8: ¿CUENTA USTED CON ALGUNA ESTRATEGIA PARA POSIBLES INCIDENTES QUE AMENACEN EL ESTADO DE SU PRIVACIDAD O LA SEGURIDAD DE SUS DOCUMENTOS PERSONALES QUE SE PUEDAN ENCONTRAR EN DISPOSITIVOS MÓVILES O PORTÁTILES? 71

GRÁFICO 9: ¿UTILIZA APLICACIONES O EXTENSIONES EN NAVEGADORES QUE LE FACILITEN SABER SI ESTÁ INTENTANDO ACCEDER A UNA PÁGINA WEB SOSPECHOSA? 72

GRÁFICO 10: ¿ES USTED CAPAZ DE IDENTIFICAR CUANDO SU DISPOSITIVO MÓVIL O PORTÁTIL NO ESTÁ FUNCIONANDO DE MANERA ÓPTIMA? 73

GRÁFICO 11: ¿CONSIDERA USTED QUE LOS SISTEMAS OPERATIVOS Y APLICACIONES NECESARIAMENTE DEBEN ESTAR ACTUALIZADOS A SU ÚLTIMA VERSIÓN? 74

GRÁFICO 12: ¿QUÉ TAN DE ACUERDO ESTÁ USTED EN QUE LAS CONTRASEÑAS DEBERÍAN SER CAMBIADAS CADA 90 DÍAS? 75

GRÁFICO 13: ¿QUÉ TAN PROBABLE ES QUE SEPA IDENTIFICAR CUANDO ESTÁ SIENDO TENTADO A UNA ESTAFA A TRAVÉS DE CORREOS ELECTRÓNICOS, PUBLICIDADES O ALGÚN OTRO MEDIO? 76

GRÁFICO 14: ¿QUÉ TAN SEGURO Y CÓMODO SE SIENTE AL TENER INSTALADO APLICACIONES DE DUDOSA PROCEDENCIA EN SU DISPOSITIVO MÓVIL O COMPUTADORA PORTÁTIL? 77

GRÁFICO 15: ¿QUIÉN CONSIDERA QUE ES MÁS IMPORTANTE PARA MANTENER EN BUEN ESTADO LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES O COMPUTADORAS PORTÁTILES, EL USUARIO, ANTIVIRUS O AMBOS? 78

ÍNDICE DE ECUACIONES

ECUACIÓN 1: PRUEBA DE HIPÓTESIS EN FUNCIÓN DE LA HIPÓTESIS DE TRABAJO 57

1. INTRODUCCIÓN

El constante avance de la tecnología ha provocado que un número creciente de individuos adquieran dispositivos móviles y portátiles en los que puedan realizar sus labores o estudios, sobre todo si se trata de utilizarlos diariamente como es el caso de usuarios que quieran adentrarse en su totalidad al mundo de la informática.

Ante esta realidad, la gran mayoría de ellos desconoce los peligros potenciales a los que están expuestos sus datos por culpa del malware o software malicioso, que son aplicaciones diseñadas con el propósito de corromper o dañar cualquier programa, dispositivo, servicio o red de personas individuales o instituciones públicas o privadas, así como afectar la privacidad de los usuarios. A pesar de que existen métodos que ayudan a impedir el ingreso del malware a los sistemas tecnológicos, lo cierto es que ellos evolucionan y en otras instancias se crean nuevas variantes con alguna finalidad para cumplir con su función (Bhooshan Gupta, 2022).

Por otro lado, existen quienes aprovechan la delincuencia informática transformándola en una profesión para generar dinero en la red de manera ilegal. Comúnmente estas prácticas están dirigidas a los robos de cuentas de banco y credenciales para todo tipo de dispositivo a través del malware conocido como Phishing, extorsiones y amenazas por medio de correos electrónicos, SMS, redes sociales entre otros. Las opciones en las que un ciberdelincuente pague por sus fechorías son escasas ya que ellos se asocian con profesionales del tema haciéndolo aún más complicado para las autoridades digitales (Goutam, 2021).

Por ende, en épocas recientes resulta casi imposible navegar con total confianza en la Web, ya que la seguridad de los dispositivos y datos personales puede ser

comprometida por un simple clic del mouse. De esta manera los ciberdelincuentes esperan que sus aplicaciones maliciosas surtan efecto.

En consecuencia, esta investigación tiene como objetivos principales el establecimiento de un estado del arte sobre el conocimiento que tienen los estudiantes de la FIEC-CRUV acerca de políticas de ciberseguridad que les sean aplicables; así como el planteamiento de alternativas de solución a los problemas potenciales que se pudieran detectar en dicha población.

La idea central del proyecto radica en que los usuarios informáticos tendrán a su disposición estrategias efectivas para que sus dispositivos tantos móviles como portátiles no tengan vulnerabilidades en las cuales el ciberdelincuente o malware pueda acceder de forma fácil y de esta manera logre su cometido.

Este documento está estructurado con las partes que se detallan a continuación: marco teórico, definición del problema, objetivos, hipótesis, marco metodológico, delimitación o alcance, restricciones, justificación, factibilidad del proyecto, consecuencias y cronograma de actividades.

La perspectiva de esta investigación aplicará metodologías de tipo exploratorio y descriptiva. Por cuanto que los antecedentes recabados no reflejan en el tema a tratar de forma precisa, se considera exploratoria. Por otro lado, dado que se pretende caracterizar el nivel de conocimiento en ciberseguridad de los estudiantes de la FIEC-CRUV y a la vez poder identificar las posibles consecuencias por las cuales ellos son víctimas de toda clase de programas malignos, este estudio se considera descriptivo. Como instrumento de recopilación de datos se utilizará a una encuesta.

Finalmente, la investigación tiene como finalidad contribuir a que los estudiantes la FIEC-CRUV logren reducir en alguna medida los riesgos potenciales a los que

están expuestos cuando realizan sus diferentes actividades al frente de sus dispositivos móviles y portátiles.

2. MARCO TEÓRICO

A continuación, se detalla el marco teórico de este anteproyecto.

2.1 EL MALWARE O SOFTWARE MALICIOSO

Mantener con total seguridad los documentos importantes y los de carácter personal probablemente resulte ser una tarea sencilla a simple imaginación. No obstante, en el mundo de la informática el usuario puede llegar a encontrarse con pequeños problemas que le impidan la asignación mencionada. Como es el caso de los **malwares o los softwares maliciosos**, los cuales tienen la capacidad de violar la seguridad de los dispositivos informáticos realizando ataques sin ningún tipo de autorización de tal manera que accedan a los datos protegidos, los roben y hagan con ello lo que desean. Esta mala práctica cada vez está subiendo niveles por lo que resulta ser preocupante (Lukings & Habibi Lashkari, 2022).

2.1.1 TIPOS DE MALWARE O SOFTWARE MALICIOSO MÁS COMUNES

Dentro de la definición del malware se encuentran muchos softwares clasificados por categoría o método de propagación, con potencial alto para afectar a los usuarios informáticos como por ejemplo espiar, robar y ganar dinero a través de ellos. Cabe recalcar que existen diferentes medios digitales que utilizan sus propias lógicas pequeñas para nombrar un malware de otro. Es por eso que se enlistará a los nombres más comunes o aquellos con alta tasa de infección (Kleymenov & Thabet, 2022).

2.1.1.1 SPYWARE

Este malware es bastante común debido a su capacidad para espiar y guardar la información que se obtiene mediante las pulsaciones del teclado, capturas de pantalla, revisión de aplicaciones instaladas etc. De esta forma es como el ciberdelincuente hurta las contraseñas de cualquier sitio web o aplicación del usuario infectado (Belous & Saladukha, 2020).

2.1.1.2 RANSOMWARE

Se dedica a impedir que el equipo infectado pueda usar ciertos archivos bloqueándolos de esta manera. Existe otra forma su derivada de este mismo, haciéndole creer al usuario que tiene la esperanza de volver a tener acceso a sus archivos mediante un rescate o pago adelantado de ellos. Una vez realizado el pago, los usuarios tendrían libre acceso a sus archivos, sin embargo, no siempre se presenta esta situación (Kleymenov & Thabet, 2022).

2.1.1.3 DOWLOADER

Su propósito es hacerle creer al usuario que ha descargado e instalado un programa útil, cuando es realidad se trata de un programa que se enlaza de manera automática con otros malwares para descargarlos al dispositivo, logrando infectarlo totalmente (Kleymenov & Thabet, 2022).

2.1.1.4 BACKDOOR

Son aquellos que utilizan alguna vulnerabilidad en los sistemas de dispositivos móviles y portátiles y se adentran al equipo. El ciberdelincuente tiene el control

del malware de forma remota para realizar acciones que perjudiquen al equipo infectado (Kleymenov & Thabet, 2022).

2.1.1.5 ADWARE

Otro software malicioso bastante común y en el que muchos usuarios suelen caer es el adware, apareciendo en algunos casos en forma encubierta como si se tratase de un anuncio de medio local y en otros casos mostrando amenazas agresivas. En ambos resulta ser difícil encontrar alguna manera de lograr eliminarlos (Kleymenov & Thabet, 2022).

2.1.1.6 VIRUS

Quizás sea el malware más conocido de todos por el simple hecho de llamar **virus** cuando un dispositivo no funciona correctamente, sim embargo, obtiene dicho nombre debido a que su método de propagación es similar a los virus gripales, ya que se expande de un programa a otro o en otros casos de un equipo a otro con además la capacidad de autorreplicarse e insertar posteriormente su código propio con intencionales maliciosas (Lukings & Habibi Lashkari, 2022).

2.1.1.7 TROYANO

Un troyano es aquel programa malicioso que el usuario descarga en su dispositivo sin saberlo, con el único propósito de que este lo ejecute en algún momento haciéndole creer que es una aplicación útil para posteriormente llevar a cabo las acciones por la cual fue creado. Este tipo de malware se obtienen a través de diversos métodos siendo el sistema de correos electrónicos, mensajes engañosos y redes Wi-Fi piratas las técnicas más empleadas para infectar al usuario informático (Lukings & Habibi Lashkari, 2022).

2.1.1.8 SPAM

El spam es todo aquel mensaje publicitario engañoso de cualquier tema que nunca fue solicitado, comúnmente estos mensajes llegan a través de correos electrónicos relacionados con lotería, phishing o los ya mencionados virus. Existen otros tipos de spam que tienen que ver con los ataques por medio de comentarios en redes sociales, ataques de bots entre otros (Lukings & Habibi Lashkari, 2022).

2.1.1.9 PHISHING

El phishing es una práctica maliciosa por medio de un ciberdelincuente que trata de engañar a los usuarios haciéndose pasar por entidades, empresas o locales oficiales para que les suministre información y de esta manera robe, así como también tener el acceso privado como lo son los datos personales, datos de tarjetas de créditos, cuentas privadas etc. El atacante actúa por medio de correos electrónicos, sitios webs, redes sociales o publicidad engañosa (Rains, 2023).

2.2 POLÍTICAS DE CIBERSEGURIDAD

Las políticas de ciberseguridad en principio fueron diseñadas para la protección de la confidencialidad, integridad y disponibilidad de la información en las organizaciones. Actualmente estas técnicas no logran garantizar al cien por ciento la seguridad, debido a que la ciberdelincuencia está en constante crecimiento y evolución, generando alertas de malware para todo tipo de organizaciones incluyendo a los independientes quienes monitorean las irregularidades que posiblemente ocasionen activar los protocolos de prevención, detención y respuesta que atentan contra los equipos informáticos (Santos, 2019).

No obstante, las técnicas de protección no dejan de ser útiles, en función a que por lo menos en algún momento surtan algún tipo de efecto que contrarreste las principales amenazas en los dispositivos móviles y portátiles.

2.2.1 EL PAPEL DE LA CIBERSEGURIDAD

Las políticas de ciberseguridad surgen como una herramienta que permite proteger los recursos críticos, así como las libertades que son base en la creación de un mundo mejor. Sin políticas se generaría un nivel de caos e incertidumbre, que pondría en riesgo los derechos fundamentales que tienen los usuarios en el mundo (Santos, 2019).

2.2.2 LEYES EN LA CIBERSEGURIDAD

(Lukings & Habibi Lashkari, 2022) señalan que la ley en la ciberseguridad no se trata solamente de sistemas legales implicados a la protección de datos personales, sino que también fueron creadas para cumplir y abordar actividades criminales mediante el uso de redes de la tecnología llamados generalmente como **delitos cibernéticos**. Dedicados a la protección de información interpersonal, violaciones de datos, infracciones a los derechos reservados de un autor, entre otras actividades más que se desarrollen haciendo uso de los dispositivos móviles o portátiles conectados a la red.

2.2.2.1 CIBERCRÍMENES EN LA CIBERSEGURIDAD

(Lukings & Habibi Lashkari, 2022) estructuran a la ciberseguridad y a los cibercrímenes en diferentes secciones, identificando cada caso para los diferentes fraudes que existen actualmente.

2.2.2.1.1 DELITOS CIBERNÉTICOS

También conocido como cibercrimen, consiste en todo acto reprensible para la sociedad realizados en la red mediante el apoyo de dispositivos electrónicos digitales conectadas a la Internet. (European Commission, 2021).

Esta acción se manifiesta por medio del ciberdelincuente para hacerse con el nombre, cuenta, contraseña, entre otros datos para obtener beneficios como información personal de interés, robos bancarios digital junto a su tarjeta de crédito de la víctima. El malware usado para el robo de identidad es llamado como phishing, el cual es un método practico para extraer los datos necesarios (Lukings & Habibi Lashkari, 2022).

2.2.2.1.2 DELITOS CIBER DEPENDIENTES

Generalmente consiste en un delito tradicional, conectado a la red para el robo, acoso, explotación infantil o fraude. Estas prácticas actualmente tienen una huella digital, ya sea que estén ubicadas en la comisión del delito, la preparación previa o en el encubrimiento posterior para que los oficiales encargados logren atrapar al usuario responsable (Eolas, 2021).

A diferencia de los delitos cibernéticos, los delitos ciber pendientes tienen como objetivo el comprometer la confidencialidad, integridad y disponibilidad de los sistemas e información en la red, haciendo actividades de piratería informática, violando los accesos restringidos, modificando e interceptando datos y por último los ataques que ocasionan la saturación en la red o servidores más conocidos como DoS y DDoS (Lukings & Habibi Lashkari, 2022).

2.2.2.1.3 DELITOS CONTRA LA SEGURIDAD NACIONAL

Conocido generalmente como **ciberterrorismo**, es un delito con tecnología informática procesable que acoge victimas en grandes cantidades generando pérdidas económicas con la intención de dañar la moral de las personas física como psicológicamente donde destaca principalmente el estrés y ansiedad. Ocasionando de este modo la desconfianza de las victimas hacia diferentes instituciones de un gobierno con respecto a la economía y política (Gross, Canetti, & Vashdi, 2017).

Algunas otras facetas del ciberterrorismo para causar desastre entre la sociedad son: incursión (entradas hostiles a sitios web), destrucción, desinformación, denegación de servicio y desconfiguración de sitios web (Lukings & Habibi Lashkari, 2022).

2.2.3 PLAN DE SEGURIDAD INFORMÁTICA

La preocupación que la gran mayoría de empresas, instituciones y personas enfrentan hoy en día es sobre el tema de la ciberseguridad, sobre todo si se tienen equipos, software o datos sensitivos. Las soluciones más comunes en estos tiempos para evitar fallas en los sistemas son los respaldos en las nubes y los almacenamientos ubicados en una sola área específica. Estas prácticas ocasionan que los delincuentes informáticos tengan un camino más sencillo hacia sus ataques (Saeed, Almuhaideb, & Others, 2023).

En consecuencia, ante la posibilidad de ser víctima de cualquier tipo de fechoría informática, conviene de gran manera contar con servicios y mecanismos informáticos que ayuden en un hipotético caso, a la protección de recursos en

estados vulnerables. En particular, la disposición de un plan de seguridad informática resulta de gran utilidad (Stallings & Browm, 2018).

2.2.3.1 PREVENCIÓN

Un esquema de seguridad ideal es aquel en el que ningún ataque tiene éxito. Aunque esta meta es prácticamente imposible de lograr en el 100% de los casos, existe una amplia gama de amenazas en las que la prevención es un objetivo razonable. Por ejemplo, considera la transmisión de datos cifrados. Si se utiliza un algoritmo de cifrado seguro y si se han implementado medidas para prevenir el acceso no autorizado a las claves de cifrado, entonces se evitarán los ataques a la confidencialidad de los datos transmitidos.

Un ejemplo de medida de prevención es la copia de seguridad de datos, cada vez que se haga una modificación o anexo a los archivos que se consideren importantes, sim embargo resulta ser más practico que el respaldo se haga fuera de toda conexión a internet debido a que es más complicado afectar la vulnerabilidad de los equipos personales para los malware de la familia ransomware. Otro ejemplo es la constancia de mantener actualizados a la última versión de cada software instalado en el dispositivo, suele ser siempre una garantía de seguro (Volynkin, Horneman, & Morales, 2017).

2.2.3.2 DETECCIÓN

Una vez se tenga un plan de prevención en ciberseguridad, el siguiente paso es detectar las posibles amenazas que atentan con la información privada. Existen diversos sistemas diseñados especialmente en la detección de intrusos o visitas no esperadas, de esta forma se salvaguardan los datos en los que puedan ser expuestos.

Un programa de detección antimalware es lo básico a tener en cuenta en los dispositivos personales, no obstante es claro mencionar que existen malware posiblemente indetectables y por lo tanto se debe ser cauteloso, como es el caso que posteó el periodista **Brian Krebs** en su sitio web sobre las amenazas por correos electrónicos con respecto a los phishing, el usuario afectado cuenta que el mensaje tipo estafa (aparentemente proveniente de Microsoft) le llegó a su bandeja de entrada a pesar de contar con sus aplicaciones de detección sospechosa y lo redireccionaba a otros sectores esperando obtener sus credenciales (Krebs, 2023).

2.2.3.3 RESPUESTA

Un plan de respuesta a los ataques informáticos en curso (sobre todo si es una denegación de servicio) evade toda oportunidad de ocasionar daños considerables a la información valiosa personal y resulta ser practico en caso de experimentar nuevamente un suceso idéntico.

Es esencial reconocer las principales amenazas que atentan contra los equipos sobre todo si anteriormente se detectó alguno de ello, se deberá fortalecer las vulnerabilidades que ya se conocen y las cuales fueron blanco sencillo para los ciberdelincuentes, realizando los cambios correctos si se tratase de una empresa donde existen informaciones de caracteres confidenciales bajo una persona responsable (Toth, 2019).

2.2.3.4 RECUPERACIÓN

Por último, existe una solución en caso de que el plan de respuesta haya fallado, es algo muy común debido a la mutación de los virus informáticos. Los sistemas de respaldos son una gran alternativa cuando los datos son comprometidos, se

pueden recargar copias previas y continuar con los objetivos prestablecidos por parte del usuario.

Incluso en la recuperación de datos perdidos existen artimañas que si se siguen puede llegar a significar un esfuerzo totalmente en vano. (Markley, 2023) en su sección de noticias y tendencias, explica que existen algunas trampas al momento de realizar una recuperación de datos, entre ellas la de pagar rescate ya sea porque los afectados no reciben en su totalidad los archivos o pueden ser víctimas de un nuevo ataque a través del mismo ladrón o de uno nuevo quien tiene conocimiento de lo sucedido. Otro descuido muy común es confiar y mantener una sola copia de seguridad, el autor recomienda poseer más de una copia aplicando distintas reglas como por ejemplo una donde estén los datos fuera de toda conexión a la red.

2.3 POLÍTICAS DE CIBERSEGURIDAD PERSONAL

Según (Waschke, 2017) para los usuarios personales no existe una manera de poseer un control que procese y almacene las vulnerabilidades que afectan a los sistemas informáticos, a diferencia de las empresas que si los tienen y previenen los robos por parte de los ciberdelincuentes de manera masiva.

2.3.1 RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DE DISPOSITIVOS PERSONALES

La seguridad tanto del hardware como software perteneciente a un usuario personal resulta ser un problema extenso donde se involucra a las tantas formas de datos controlados, desde robo hasta destrucción de archivos accidental o maliciosamente (Stallings & Browm, 2018).

En consecuencia, se pueden establecer una serie de recomendaciones generales en aspectos concretos que ayuden a salvaguardar los datos e información que se consideren sumamente valiosos o de carácter privado. A fin de intentar llegar a maximizar los niveles de seguridad a nivel personal dentro de los dispositivos de mayor uso.

2.3.1.1 MODELO DE GESTIÓN DE CONTRASEÑAS

Un buen protocolo en ciberseguridad tiene que incluir el siempre molesto tema de las contraseñas. (Waschke, 2017) menciona lo preferible que resulta ser minimizar las molestias causadas por los delincuentes informáticos en el tema de ciberseguridad ya que es casi imposible detenerlos. En consecuencia, es importante dedicar esfuerzos en construir un anillo de seguridad fundamental donde se logre un compromiso entre aceptar ciertos riesgos que no comprometan a extraviar lo que el usuario considere valioso; en tanto que, a la vez, se adquiere un seguro contra accidentes, sobre todo en lo que al manejo financiero o información personal confidencial que circule a través de internet.

(Waschke, 2017) establece algunas reglas básicas para generar contraseñas, que se establecen a continuación:

2.3.1.1.1 PORQUE NUNCA REUTILIZAR LAS CONTRASEÑAS

Resulta ser demasiado peligroso el utilizar las mismas contraseñas en diferentes sitios en la Internet, sobre todo si se comparten cuentas de usuario donde se ubique información privada, datos bancarios, páginas de compras etc. Para el hacker informático es muy fácil descifrarlas con algún registrador de las teclas que se pulsan en los dispositivos, también conocido como keyloger, o aplicando técnicas de ingeniería social. Por ende, **no se recomienda el reciclado de**

contraseñas entre cuentas, ya que una vez se compromete una contraseña compartida, la seguridad de múltiples cuentas queda en entredicho.

2.3.1.1.2 REEMPLAZO PERIÓDICO DE LAS CONTRASEÑAS

Las contraseñas requieren ser cambiadas por lo menos cada mes bajo algún motivo, ya sea porque existen cuentas más importantes que otras debido al valor que el usuario suele resguardar en ellas, también se recomienda que las nuevas contraseñas no sean cortas ni mucho menos estén clonadas en otros sitios, ya que resulta más sencillo ser otra víctima más de alguna clase de malware. Por otra parte, si el usuario está rodeado de personas diariamente en su ambiente laboral, es prudente que por lo menos se cambie la clave de cualquier acceso frecuentemente.

Hay que recordar que las contraseñas siempre tienen que mantener una creatividad única que solo el mismo usuario sea capaz de pensar y adivinar, minimizando las prácticas que originan contraseñas dependientes del entorno del usuario y que no poseen un nivel de fortaleza aceptable.

A continuación, se establecen algunas reglas básicas que se deben seguir para establecer contraseñas (Waschke, 2017):

- Las contraseñas generadas de forma aleatoria son significativamente más seguras.
- Mucho más efectivo las contraseñas con frases largas y memorables.
- No usar contraseñas generadas/sacadas de Google.

- No es recomendable las contraseñas repetitivas, sobre todo en cuentas importantes.

- Si existe algún incumpliendo en cuentas importantes, inmediatamente se debe cambiar la contraseña.

2.3.1.1.3 ESTRATEGIAS PARA ALOJAR CONTRASEÑAS

Poseer múltiples cuentas en la red suele ser una tarea bastante complicada en el sentido de que cada sitio web se accede con contraseñas, si los individuos contaran con memoria fotográfica sería la mejor solución de todas, ya que es el mejor almacenamiento donde nadie más pueda tratar de hackearlo, sin embargo, esta no es una solución realista en la inmensa mayoría de los casos.

En consecuencia, diversos grupos dedicados a la ciberseguridad como es el caso de **National Cybersecurity Alliance** recomiendan no dejar de contar con un procedimiento que posibilite el almacenamiento de las claves. Por ejemplo, al considerar herramientas encargadas de administrar múltiples contraseñas; sobre todo si son largas, complejas y donde también la gran mayoría de estas aplicaciones permiten generarlas en caso de tener poca creatividad; como lo hacen la gran mayoría de usuarios en línea quienes se dan por vencidos y optan por utilizar una única clave de acceso; de esta forma no existe necesidad de recordar todas las contraseñas. Esta regla tiene como excepción el caso donde se debe recordar la clave que abre o inicia sesión en el software de alojamiento de contraseñas, ya que esta debe ser inigualable y su función es la de proteger a las demás credenciales de acceso (National Cybersecurity Alliance, 2022).

Otro aspecto fundamental que señala (Waschke, 2017) consiste en disponer de una persona de confianza que tenga el acceso a las contraseñas en caso de algún accidente grave, por ejemplo, que inhabilite al propietario de las cuentas de su

uso, de esta manera alguien confiable estará en su representación para cualquier eventualidad.

Es de vital importancia recordar que la seguridad es prioritaria para salvaguardar los datos necesarios con contraseñas seguras, extensas y bien administradas por programas o personas responsables.

2.3.1.1.4 PRIORIZAR LAS CUENTAS QUE SE CONSIDEREN MAS IMPORTANTES

No existe la necesidad de aplicar la misma lógica de las diferentes estrategias que el usuario practique respecto a sus cuentas. Esto debido a que algunas no sean de carácter prioritario como si lo suelen ser las cuentas bancarias, servidores de pago como PayPal, sitios webs de compras por Internet (sobre todo si las tarjetas de crédito están vinculadas). Conviene a gran medida observar la actividad más reciente de las cuentas impidiendo un posible cambio de clave a pesar de que no se detecten cambios, por la razón de que el delincuente informático actúa a según su conveniencia. En cambio, cuentas asociadas a juegos como actividad puramente lúdica y sin importancia para el usuario, no requieren de los mismos niveles de rigor en su administración que las credenciales empleadas en actividades relevantes del usuario.

2.3.1.1.5 APOYO DE HERRAMIENTAS PARA ADMINISTRAR CONTRASEÑAS

Tanto a nivel local como en la nube existen formas de cifrar, crear y almacenar contraseñas donde el usuario tenga la total facilidad de no exigirse mucho en el pensar de una clave única. Las ventajas de las aplicaciones le muestran al dueño las contraseñas repetidas, las que deben cambiarse entre otras opciones más. La

consecuencia de usar estas herramientas es la de ser vulnerable a un ataque de hacker y robe toda la información alojada a la nube, por la centralización de esta información.

2.3.1.2 IMPORTANCIA DE LA AUTENTICACIÓN DE USUARIO

La autenticación de usuario se considera un mecanismo de seguridad avanzada entre el usuario y dispositivo, donde se busca obtener una verificación exitosa al acceso que se está solicitando a la red social o web en específico por medio de una clave única e irrepetible para cada vez que se intente acceder o bien si un delincuente informático/persona con intenciones poco éticas desea obtener el ingreso a la propiedad privada. En ocasiones esta clave suele tener un periodo vencimiento, dándole al usuario mejor seguridad.

No siempre se suelen usar las interacciones entre el usuario y el dispositivo, también existen otros esquemas de autenticación de usuario donde solo también son participes las huellas digitales, dando como resultado una categoría de tres factores o un solo factor donde se haga manejo de solamente el dispositivo (Kumar, Saini, & Cuong, 2021).

2.3.1.3 USO RESPONSABLE DEL RESPALDO EN LA NUBE

Un usuario que vele por su información y sea responsable debe establecer un uso correcto del alojamiento en la nube debido a los múltiples riesgos que conllevan al optar por el servicio mencionado. Es una responsabilidad mutua entre el usuario y el proveedor que escoja para sus servicios.

2.3.1.3.1 NORMATIVAS DEL RESPALDO EN NUBE

Principalmente es el usuario quien debe conocer las ganancias y contras de preferir al proveedor de servicios en la nube. A continuación, se establecen las recomendaciones más relevantes que se pueden aplicar a los usuarios personales en cuanto a este mecanismo de respaldo (ISO, 2022).

- Leer detalladamente los criterios principales al unirse y el alcance por ejemplo del espacio que obtendrá el usuario para almacenar sus documentos al servicio en la nube.

- Comprender cabalmente la forma en que se manifestará la empresa encargada en caso de accidentes o robos por parte de hackers, cuales garantías obtendrá el usuario.

- Tener conocimiento de los procedimientos que sigue el servicio en la nube, en el escenario del control de incidentes de ciberseguridad.

- Ser consciente de las posibilidades y limitaciones existentes al momento de cambiar la información almacenada o bien darse de baja de los servicios en la nube.

2.3.1.4 ESCANEO MODERADO DE ARCHIVOS Y CORREOS ELECTRÓNICOS

Existen escenarios en los que el usuario desconoce si un archivo es totalmente seguro a la hora de ejecutarlo en su dispositivo personal, esto crea gran incertidumbre, sobre todo si no se cuenta con los cuidados y prevención para realizar dicha acción. En caso de ser un software malicioso se necesita conocer

la intención del programa para así contar con una idea hacia donde se dirige el posible ataque dentro de los dispositivos móviles y portátiles (Smith, 2022).

Dado que existen archivos a los cuales se les debe considerar una supervisión cuidadosa también se encuentran otras formas de afectar al usuario, por ejemplo, a través de correos electrónicos haciéndose pasar por compañías conocidas o asociadas a la víctima asustándola con noticias o advertencias sobre actualización de datos que tenga con ver con tarjetas de créditos y banco, con la intención de robar las credenciales principales como cuentas, contraseñas, números de banco etc.

Cabe aclarar que estos correos electrónicos con dicha finalidad se les llama **Phishing** y en ocasiones, resulta muy complicado diferenciarlos de un email real, ya que existen muchas similitudes salvo por algunos detalles como los saludos genéricos que no suelen usar las empresas reales y piden actualizar datos recurrentemente a tan solo un clic. Para evitar una futura estafa de estas La Comisión Federal de Comercio plantea algunas recomendaciones generales (Federal Trade Commission, 2022):

- Mantener constantemente el equipo informático actualizado y protegido con software antimalware, de esta manera, ante el surgimiento de nuevas amenazas, el dispositivo estará preparado para afrontarlo bajo la supervisión del usuario.

- Utilizar diversos sistemas de autenticación para mantener el equipo protegido, ante una inminente amenaza de robo se le pedirá al usuario un código de acceso que solamente él puede saber y no el ciber delincuente.

- Es importante reconocer que en general resultará complicado mantener al sistema protegido con las últimas versiones de las aplicaciones que se

utilizan, por ende, siempre existe la posibilidad de ser afectado por los delincuentes informáticos. En consecuencia, nunca deja de ser importante la alternativa de crear y mantener copias de seguridad que blinden los datos más esenciales, ya sea por medio de la nube y discos externos.

2.3.1.4.1 SOFTWARE ANTIMALWARE

A la hora de escanear el dispositivo móvil o portátil se debe contar con un software antimalware que cumpla cabalmente con su objetivo primordial, la detección de programas malignos existentes y las posibles futuras amenazas. Desde monitorear el sistema en busca de actividades sospechosas hasta su eliminación. Se debe contar con que el software esté actualizado a la versión más reciente para obtener mejores resultados (Smith, 2022).

2.3.1.4.2 ESCANEAR SITIOS WEB

El autor señala el escaneo constante de sitios web en empresas en busca de vulnerabilidades que expongan los datos personales, posibles ataques tanto a clientes como los visitantes, no obstante, esta práctica también puede ser utilizada para usuarios personales, el apoyarse en herramientas que detecten sospechas de malware en las páginas web visitadas constantemente, recomendadas por otros usuarios o de dudosa procedencia (Smith, 2022).

2.3.1.5 APLICACIONES EN ABANDONO

Mantener aplicaciones instaladas sin uso alguno durante largos periodos de tiempo en los dispositivos conlleva a posibles riesgos, conviene desinstalarlas si se sabe que no se le dará manejo. Un ejemplo claro es el que informa **Malwerebytes** (Collier, 2021) sobre la aplicación **Barcode Scanner** que después

de una inactividad recibió una actualización la cual contenía malware, y aunque la tienda de aplicaciones la retiró no serviría de mucho si aún se mantiene instalada en el dispositivo.

En consecuencia, no se debe confiar ciegamente en las aplicaciones del teléfono, aun sabiendo que provienen de tiendas mayormente populares, la ciberseguridad tiene que estar presente en todas partes con tal de salvaguardar la privacidad e información personal.

2.3.1.6 APLICACIONES QUE RECOLECTAN DATOS EN REDES SOCIALES

Dentro de las redes sociales los usuarios pueden comunicarse e informarse con sus amistades siendo una forma de distraerse o liberar estrés. Existen quienes no son conformes con las mecánicas y novedades que ofrecen las aplicaciones de redes sociales a tal grado de utilizar programas de terceros que ayudan a cumplir los requerimientos del usuario, como por ejemplo los que necesitan saber qué persona ya no te sigue, quien te bloqueó o ya sea algún interés más. Estas aplicaciones en ocasiones suelen “cumplir su función” y en otros casos terminan siendo un total engaño, inventándose datos que al mismo tiempo va accediendo a los personales.

Una de las aplicaciones móviles más populares en cuanto a lo descrito es **Instagram Wrapped**, elevando cada vez más su popularidad en las tiendas móviles y a la misma vez difundiéndose dudas acerca de la seguridad que puede llegar a tener principalmente porque no está creada por el grupo Meta, que son los propietarios de redes sociales como WhatsApp e Instagram (Merino, 2023).

Además de estas advertencias, aplicaciones como Instagram Wrapped suelen realizar otros tipos de engaños tales como:

- Solicitan inicios de sesión a la aplicación para otorgar los beneficios que llaman la atención de los usuarios, de esta manera igualmente acceden a las credenciales privadas como fotos y mensajes con altas posibilidades de ser divulgadas con quienes se dediquen a poseer datos.

- Estas aplicaciones realmente no están relevando los datos de Instagram como la revisión de perfiles o quien dejo de seguirte entre otros casos. Primero porque la red social no comparte con nadie estas clases de informaciones, lo que lleva al segundo punto donde múltiples usuarios se dan cuenta que el análisis realizado por la aplicación en el día uno no es igual al de los siguientes días, por lo tanto, son un total engaño.

2.3.1.7 ESTAFAS ECONÓMICAS ENCONTRADAS EN REDES SOCIALES

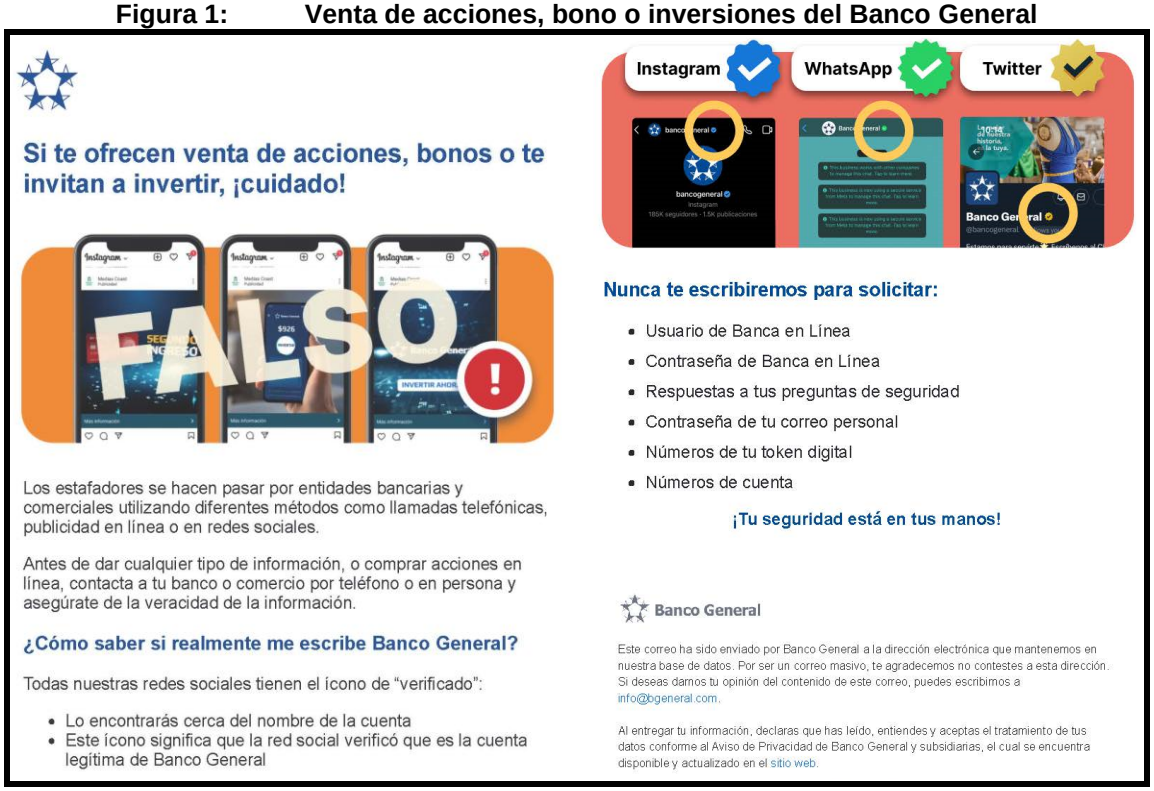
Como resultado de tener en cuenta la desconfianza al intentar adquirir bienes como por ejemplo a mejor precio se evitan casos de hurtos por redes sociales, en caso contrario si no se es precavido ocurren estafas como las de comprar paquetes vacaciones a menor costo, simplemente porque se cree que ahorrándose unos pequeños dólares es posible librarse de empresas confiables y con altos renombres. La sorpresa que se llevan algunos usuarios es cuando realizan el depósito por adelantado y no obtienen más respuestas que saber que han sido estafados, bloqueándolos de las redes sociales u otro tipo de contacto. Aunque varias personas han sido arrestadas en varias provincias de Panamá, lo cierto es que todavía quedan libres quienes siguen promoviendo esta clase de hurto donde más 3,568 son los afectados (Redacción de TVN Noticias, 2023).

Otro escenario donde se presenta esta problemática se observa en las tentativas de fraudes en inversiones económicas, ya que actualmente las personas buscan

generar ingresos adicionales a través de inversiones en línea, así como la compra de acciones o bonos. En consecuencia, los estafadores actualizan sus maneras de hurtar conforme la tecnología avanza y se moderniza. Es común que los ciberdelincuentes se hagan pasar por diferentes entidades bancarias y comerciales, seduciendo a sus víctimas a través de llamadas telefónicas, publicidad o anuncios en redes sociales para que de esta manera realicen compras engañosas, con la consiguiente pérdida monetaria.

Es importante recordar que las empresas utilizadas como fachada para estas estafas, realizan constantemente llamados de atención a sus clientes mediante múltiples comunicados con la finalidad de que ellos no sean víctimas de estos atracos, tal como se puede observar en la Figura 1.

Figura 1: Venta de acciones, bono o inversiones del Banco General



Fuente: El autor

De la Figura 1 se pueden extraer algunas características claves para establecer la veracidad de la publicidad en línea (B. General, correo electrónico, 22 de octubre, 2023):

- Las empresas auténticas siempre tendrán un símbolo de verificado junto a sus nombres en sus redes sociales.

- Jamás solicitaran al cliente el usuario, contraseña y cuenta bancaria de su banco de preferencia, en caso de conflictos únicamente se le solicitarán datos como nombre, cedula y los últimos cuatro dígitos de la tarjeta que maneje el cliente.

- Las preguntas de seguridad y tokens que por general han implementado los bancos son de carácter personal, lo que significa que nunca se la pedirán a sus clientes.

2.3.1.8 HURTO DE CREDENCIALES EN TIENDAS VIRTUALES

Comprar por Internet se vuelve cada vez más una tendencia que todos lo que tienen tarjetas de crédito han experimentado alguna vez por lo menos. Por lo tanto, es de suma importancia estar seguro en cuales tiendas online comprar y cuáles no, reconocer su reputación y también la de evitar falsos comercios de compras.

Para conocer más sobre este tipo de estafas **Welivesecurity by ESET** realizó una campaña orientada a la concientización en la detección de sitios web falsos de compras a través de programas maliciosos para Android, similares a los originales.

La empresa pudo comprobar diferencia a los sitios originales por sus dominios y también la opción de comprar los productos ya que el botón encargado de finalizar la compra redirigía a servidores para descargar una aplicación adicional solicitando a la víctima inicios de sesión, de esta manera los delincuentes informáticos se adueñan de las credenciales bancarias de los usuarios, haciéndoles creer que los datos introducidos son erróneos a la espera de aprovecharse también de los códigos de autenticación en dos pasos para dar como finalizado el robo en su totalidad.

Como recomendación la compañía indica que se debe verificar la URL de los comercios electrónicos iniciando siempre con **https://**, así como mantener la precaución al hacer clic en anuncios que dirigen a sitios webs falsos, es más seguro ser redireccionado a tiendas de aplicaciones oficiales como Play Store (Stefanko, 2022).

2.3.1.9 SUPLANTACIÓN DE IDENTIDAD

Recibir cualquier tipo de mensaje de una persona extraña se podría considerar como una equivocación de carácter humana, ya sea por ejemplo un mal digito introducido en el número de teléfono. Esto en la mayoría de los casos resulta ser común. No obstante, existe otro sector de la población que no está equivocado y tiene clara sus intenciones como es el caso del ministro de Vivienda y Ordenamiento Territorial Rogelio Paredes quien confirmó que su identidad está siendo usada para solicitar dinero por medio del servicio de mensajearía WhatsApp mediante un teléfono celular perteneciente a la Institución de Gobierno la cual aparentemente fue hackeada (TVN Noticias, 2024).

Es de mayor prioridad recalcar que este tipo de estafas están siendo la manera más sencilla de robar de los ciberdelincuentes haciéndose pasar por entidades del estado o personas de renombre dentro del territorio nacional. Por lo cual

siempre se debe tener mucho cuidado y asesorarse con quien realmente se está intercambiando mensajes a través de redes sociales.

Conforme a la circunstancia mencionada también queda mencionar a la estafa evolucionada de la mensajería, la cual es los **deepfakes** en tiempo real utilizando dos dispositivos a la vez para sincronizar los cambios de rostros y voces. Los estafadores realizan videos o videollamadas a las víctimas mediante filtros de cambios de rostros por personas reconocidas ofreciendo en su mayoría de casos muestras de amor y promesas falsas. Expertos del FBI mencionan que se podría aproximar grandes cifras de hurtos a través de esta clase de modalidad, por lo que solo queda ser cauteloso ante cualquier caso idéntico o similar (Roman, 2024).

2.3.1.10 USO DE SOFTWARE ILEGAL O DE TERCERAS FUENTES

La piratería digital es un tema de nunca acabar, las compañías hacen todo lo posible por tratar de disminuir su efecto debido a que perjudica sus ingresos, los culpables tras este delito ofrecen a sus clientes mejores tratos en cuanto a menores cantidades de pagos mensuales con respecto a los servicios originales.

Al principio los usuarios no experimentan fallas ni tampoco inconvenientes, lo que no saben ellos es que sus pagos en ocasiones son redirigidos a cuentas de banco ilegales para después realizar blanqueo de capitales, de esta manera los delincuentes informáticos hacen fortunas para posteriormente darle de baja a los servicios de sus clientes sin ningún tipo de aviso ni mucho menos brindándoles la opción de reembolsos. Cabe aclarar que no solo se trata de estafas de esta clase sino también en ocasiones los piratas venden sus servicios ilegales a través de apps, sitios webs y P2P, lo que conlleva a un potencial riesgo de software

malicioso que dañe o extraiga datos personales del usuario en el dispositivo móvil o portátil.

Consecuentemente, estas actividades no solo están ligadas a la ganancia de dinero sino también vinculadas a delitos como juegos en líneas, explotación infantil, sexual, drogas, trata de personas y armas, entre otros casos (Interpol, 2024).

De este modo, diversas fuentes recalcan la importancia de cuidar los dispositivos personales al piratear software sobre todo aquellos que son muy populares entre la comunidad informática, muchos repitiendo la frase de **no hay nada gratis en Internet**. Esto lleva a conocer una aplicación que viene siendo desde hace años una gran alternativa al evitar los pagos de licencia oficiales, el programa llamado **KMSPico**, quien se dedica a falsificar las licencias tanto de Windows como de Office conectándose momentáneamente con los servidores de Microsoft para de esta manera hacerles creer que es una activación real cuando en realidad es una clave VL genérica.

Por las razones antes planteadas, utilizar este tipo de herramienta solo puede traer un riesgo enorme a la seguridad de los dispositivos, no solamente por ser simplemente software pirata sino también por estar asociado a tipos de software maligno como adware, troyanos, spyware etc., programas como KMSPico violan los términos de servicio de las empresas oficiales, afectando la economía de ellos y la seguridad como privacidad de los usuarios quienes hacen uso de ellas (Umawing, 2022).

3. GENERALIDADES DEL PROBLEMA

En el siguiente capítulo, se analizarán diferentes aspectos que son esenciales para dar por finalizado el problema de investigación de forma detallada haciendo énfasis en la definición del problema en conjunto con su justificación, sus objetivos tanto general como específicos, su metodología a implementar, su descripción de la investigación, así como también otros tópicos importantes.

3.1 DEFINICIÓN DEL PROBLEMA

La gran aceptación de las tecnologías de la información y comunicación (TIC) por parte de la población ha hecho que otra clase de usuarios en la Internet se dediquen a realizar ataques informáticos con un propósito malintencionado. Quienes hacen uso de las TIC en el diario vivir para manejar sus datos personales o de interés están expuestos a sufrir pérdidas por múltiples riesgos (Guapacha, 2017).

Ante esta situación, si una persona decide entrar al mundo de las tecnologías por medio de una carrera universitaria relacionada con las TIC debe tener en cuenta conocimientos básicos sobre orden y protección suficientes para que le ayuden a evitar ser víctima en estas malas prácticas que poco a poco se vuelve una tendencia. Como lo establece (Cabrera, 2015), para navegar de forma segura se necesita tener sentido pedagógico haciendo uso de las nuevas tecnologías es posible utilizar programas que realicen la función de bloquear, examinar y clasificar el contenido que manejamos en sitios webs, neutralizando de este modo todo peligro.

¿Porque es tan importante estar protegido de amenazas informáticas en la Internet? Es de suma importancia mantener los dispositivos constantemente

actualizados, no solo porque corrigen problemas de rendimiento sino también incorporan parches de seguridad con nuevas funcionalidades, que incluso en ocasiones introducen sistemas de verificación de seguridad que fortalecen la información personal puesta en los correos electrónicos, redes sociales y otros sitios webs que maneja el usuario y en algunas instancias también la de los familiares (Muncaster, 2023).

También (Roa Buendía, 2013) dice en su libro que la mayoría de los usuarios que tienen ordenadores y dispositivos portátiles como móviles tienen sus antivirus caducados lo cual expone el equipo sin importar que tan potente sea o cuanto haya costado debido a que constantemente se está enviando mensajes con aplicaciones IP (E-Mail, WhatsApp etc.), se realizan compras, se estudia y se está en contacto con determinadas empresas en Internet.

El otro lado de la moneda de los antivirus es que los usuarios dependen mucho de ellos y no se dan cuenta que las amenazas han ido evolucionando a través de los años. Por lo que gracias a ello tener una aplicación que se encargue de vigilar al dispositivo personal ya no es suficiente. Tal como lo explica Evan Davidson (*en la presentación mundial de neutralización de ransomware en tiempo real*) expresa que los antivirus tradicionales no son muy sofisticados ya que ellos necesitan que el humano esté involucrado para ejercer sus acciones, entre otras razones más se menciona que el equipo debe estar infectado primero para luego protegerlo, así como también la regla que hay en las mutaciones de los virus lo que hace más difícil de controlar para los antivirus. (Pizarro, 2016).

3.1.1 EL RIESGO DE NO ESTAR PROTEGIDO ANTE EL MALWARE

Ser perjudicado por algún tipo de ataque de malware representa pérdidas de información como también en el ámbito económico. La encuesta recogida en Sophos News sobre el estado del ransomware en el año 2021 (Sophos Ltd, 2021) muestra que para las empresas pequeñas es un problema demasiado serio por el tan elevado costo de recuperación llegando a cifras de cinco dígitos. En total fueron 357 las empresas encuestadas que hicieron el pago para que les devolvieran sus pertenencias en donde 282 informaron cuanto fue que se pagó. Se dividió en tres escalas, el coste medio por 170.404 dólares, el coste común por 10.000 dólares y el más elevado por 3.2 millones de dólares. Lo que destaca de esta última cifra es que solamente dos empresas decidieron pagar el rescate.

Si bien las cifras mostradas anteriormente representan a empresas, también es bueno saber que estos ataques no están diseñados para un solo sector de la población. Más bien resulta ser una amenaza global, donde cualquiera que esté iniciando en el mundo de las tecnologías o no tenga conocimientos adquiridos para protegerse está en alerta y debe mantener precaución.

Esa afirmación lleva a conocer diferentes clases de malware, especialmente los que tratan sobre robos de identidad personal, **phishing** como se les conoce. Un ejemplo actual de ello trata sobre quienes se hacen pasar por autoridades judiciales enviando citaciones por medio de correo electrónico a sus posibles víctimas, buscando la manera de hurtar desde información privada hasta datos bancarios a través de enlaces (TVN Noticias, 2023).

En particular, **CryptoWall**, es uno de muchos malwares que encriptan todo tipo de información casi imposible de recuperar por parte del afectado. Este software

malicioso afectó a una persona a la cual le pedían pagar 500 dólares la primera semana y 1.000 dólares la siguiente (*cabe destacar que la única forma de pago se debía hacer por medio de Bitcoin*) para devolverle los 5.726 archivos afectados. Al final la victima optó por pagar el rescate porque no soportaba perder todos sus recuerdos (Dascalescu, 2020).

En general, los delincuentes informáticos no solo buscan datos personales para obtener algún monto económico considerable, ellos también atacan directamente el dinero, sobre todo si este es virtual, por ejemplo: **Satacom** es un malware que se ha estado popularizando a mitad de 2023, esta herramienta que se instala mediante extensiones para navegadores Chromiun, el método que utiliza hace una modificación en páginas webs donde se hace pasar por los típicos botones de “descargar” a lo que lleva al usuario a bajar de Internet un archivo ZIP con una aplicación ejecutable, dentro del código JS se encuentra un fragmento que hace la función de transferir la moneda Bitcoin de la víctima al atacante. (Zigel & Kupreev, 2023).

En cuanto a dispositivos móviles, el informe recogido por Kaspersky Security Network (Shishkova, 2022) se puede observar que al ser una tecnología muy utilizada se tienen números elevadas (*a pesar de que en el 2022 se ha estado disminuyendo*). Durante el segundo trimestre del 2022 se neutralizaron 5,520,908 ataques de malware donde destacan los adware o software no deseado, A pesar de ello el lado negativo sigue siendo la instalación de paquetes maliciosos, la empresa obtuvo una cifra de 405,684 y se señala que estas aplicaciones al ser instaladas se les da permiso de acceso a los contactos como también a fotos del usuario. Las más utilizadas resultan ser troyanos de aplicaciones modificadas de WhatsApp (*por ejemplo, la versión plus*), los que envían SMS y muestran anuncios en el teléfono ocultando el icono en el inicio.

Cuando el dispositivo de una persona es afectado por un malware, sobre todo si se trata de aquellos que actúan secuestrando documentos digitales, lo mejor es asumir la perdida y no alimentar de dinero a los ciberdelincuentes, así como lo menciona en la revista digital (Méndez, 2018) porque principalmente no existe una garantía de que los responsables cumplan su palabra de brindar el descifrador una vez que se haya hecho el pago de rescate, además de eso al realizar dicho pago se está financiando y promoviendo a que los criminales informáticos continúen con sus ataques. Adicionalmente, como lo menciona (Lizano Mora, 2022) siempre que se encuentra al culpable alguien más toma su lugar para seguir el camino, por lo que un esfuerzo para reforzar la seguridad en nuestras computadoras/dispositivos móviles es primordial.

Para los usuarios documentados en seguridad informática, que se apegue oportunamente a las recomendaciones planteadas por las organizaciones y empresas de seguridad informática, se puede librar de la mayoría de los ataques de malware, lo que supone que sus archivos digitales guardados en computadoras están relativamente seguros. Sin embargo, existe otro sector de la población (tanto a nivel personal como organizacional o empresarial) que desconoce los principios más básicos que se deben seguir para salvaguardar sus datos, identidad, e información bancaria, de las amenazas provenientes de los grupos organizados del crimen digital (*sobre todo en el caso del ransomware*, que es la amenaza más difundida en la actualidad).

En este escenario, el acceso a los dispositivos, por parte de los delincuentes se ve facilitado por la ignorancia de los usuarios, al momento de conceder permisos de instalación de aplicaciones, lo que provoca que los equipos se infecten con aplicaciones maliciosas (Malwarebytes, 2022). El último comportamiento por parte de los usuarios, también se ve reforzado frecuentemente por las recomendaciones de amigos o familiares, acerca de aplicaciones o páginas web de origen dudoso, únicamente porque en su experiencia, aún no han vivido problemas significativos

de ataques de malware. Este suceso se podría asociar con el ejemplo de la reputación sobre un vendedor hacia el cliente, en la cual este último se deja sobrellevar en la mayoría de las veces debido a que existen opiniones de “expertos” o de consumidores anteriores que contribuyen a la compra confiada de un producto en la Internet (Sanchez & Montoya, 2017).

Muchas empresas de seguridad ponen en contexto las situaciones antes expuestas acerca de los ataques de malware, publicando multiplicidad de recomendaciones y consejos, dirigidos a las personas y organizaciones, para minimizar la posibilidad de ser afectado por estas amenazas. Entre ellas, destaca la necesidad constante de mantener respaldos actualizados de toda la información que se considera importante, indiferentemente del medio que emplea para realizarlo[1], ya que cada tipo de medio ofrece ciertas ventajas, así como adolece de algunas desventajas, pero siempre teniendo presente que un solo respaldo no es suficiente (Martin, 2015).

Sin embargo, se presentan ocasiones en las que los usuarios omiten dichas recomendaciones y prosiguen sus rutinas cotidianas haciendo uso de la Internet porque, ya sea porque no se sientan amenazados o no les dan credibilidad a las fuentes de información, cada vez que se ven abordados sobre el tema.

Esta dificultad se identifica con la encuesta recogida por (Kriscautzky & Ferreiro, 2014) quienes establecen que la confiabilidad y credibilidad tienen vinculación con un listado de características que posee mensajes confiables o creíbles, en las listas que suelen ser muy largas aparecen propiedades relacionadas con el

---

[1] memorias USB, discos externos, alojamientos en la nube, entre otras posibilidades.

receptor, emisor y el mismo mensaje, como también las típicas opiniones de personajes en el entorno cercano con experiencias previas en el uso de la Internet.

El uso de las tecnologías de la información y la comunicación, de forma deficiente en el sentido de que no se siguen políticas adecuadas de ciberseguridad está creciendo a medida que transcurre el tiempo. El riesgo de delitos por ciberseguridad se incrementó en un 12.4%, además que el pronóstico hasta el 2024 es un 19.5% (World Economic Forum, 2022).

Para una población más específica (jóvenes a punto de ingresar a la Universidad) el conocimiento en el tema de la seguridad informática y lo que representa debe ser mayormente esencial en el mundo tecnológico actual. El estudio realizado en un instituto de bachillerato de México entre 112 encuestados dice que, el 42.9% desconoce las nociones básicas relacionadas a la seguridad de la información en Internet, sin embargo, el 86.6% conocen los riesgos inherentes a los que está expuesta su información y el 56.3% no desconoce las medidas básicas que se deben aplicar a fin de proteger adecuadamente su información (Martínez & Martínez, 2018).

Los porcentajes citados anteriormente, para el estudio realizado en México, resultan preocupantes, debido a que la Internet es una herramienta que se utiliza a diario, para trabajo, estudio y entretenimiento, indistintamente y la investigación establece que un porcentaje significativo de individuos desconoce los riesgos a los que están expuestos, y tampoco saben cómo resolver los problemas inherentes, al momento en que se les presenten. En consecuencia, dado que el uso de internet es un fenómeno global, dentro del mundo libre, por lo que señalan (World Economic Forum, 2022) y (Martínez & Martínez, 2018), es de suponer que, en el medio local, los niveles de desconocimiento sobre el tema deben ser similares.

Finalmente, la investigación titulada: **Percepción de la ciberseguridad: ciberdelitos, normas legales y políticas de seguridad**, establece en sus conclusiones que se necesita implementar programas de capacitación que generen conciencia en ciberseguridad, como también logren nuevas políticas de seguridad capaces de salvaguardar la información de los usuarios personales. Es importante recalcar que esta investigación se enfocó en estudiar una población compuesta por especialistas en informática de la Universidad de Panamá, que supuestamente deberían dominar las técnicas y procedimientos inherentes a la problemática de la ciberseguridad, por lo que, si entre los expertos existe la necesidad de formación en seguridad informática, solo se puede esperar que la situación sea más grave entre sus estudiantes (Rodríguez C, y otros, 2022).

Considerando toda la situación previamente expuesta, queda en evidencia que existe un problema por cuanto que **se desconoce, a ciencia cierta, el nivel de conocimientos en políticas de seguridad informática que tienen los estudiantes FIEC-CRUV**.

3.2 OBJETIVOS DEL PROYECTO

En este proyecto de investigación se proponen los siguientes objetivos:

3.2.1 GENERAL

1. Elaborar un estudio de necesidades de capacitación en el establecimiento de políticas de ciberseguridad para dispositivos móviles y portátiles, dirigidas a los estudiantes de la FIEC-CRUV, con base en la realización de un diagnóstico de esta problemática aplicado sobre dicha población.

3.2.2 ESPECÍFICOS

1. Documentar el estado del arte relacionado a las políticas de ciberseguridad, aplicables a los usuarios personales.

2. Diseñar un modelo de evaluación para valorar los conocimientos que poseen los usuarios personales con respecto a las principales amenazas de programas maliciosos.

3. Determinar el grado de conocimiento, en cuanto a políticas de ciberseguridad entre los estudiantes de la FIEC-CRUV.

4. Proponer cuando menos, una alternativa de solución a los problemas. potenciales que se detecten en la población sujeto de estudio.

3.3 DELIMITACIÓN O ALCANCE

Con el desarrollo de este proyecto, se lograrán las metas que se exponen a continuación:

- Se aplicará una encuesta cerrada para todos los grupos que estén interesados en participar. Los estudiantes pertenecerán a la FIEC-CRUV.

- El estudio procurara analizar las principales amenazas de ciberseguridad a las que están expuestos los estudiantes y cómo pueden afectar su información confidencial.

3.4 RESTRICCIONES

Este proyecto será completado dentro de las siguientes restricciones:

- Este estudio no se enfoca en analizar las políticas relacionados a la ciberseguridad en empresas, debido a que hay diferencia notoria entre un usuario personal que necesita de recursos limitados para evitar la entrada de programas maliciosos en los dispositivos móviles y portátiles, y de un usuario que trabaja para una empresa en donde existen artículos, leyes y políticas más complicadas de sobrellevar, por ejemplo, en software verificados únicamente para compañías.

- No se abordará en el tema sobre espionajes gubernamentales, ya que resulta ser un hecho casi imposible de evitar debido que existen leyes en las que un usuario personal no puede oponer resistencia en lo que a ciberseguridad se refiere, por lo tanto, se tienen que respetar los mandatos por parte del Gobierno.

- En el aspecto concerniente a las redes sociales no se tomará en cuenta el manejo básico de estas aplicaciones debido a que el usuario promedio debe por lo menos conocer cómo se utilizan.

- A nivel de sistemas operativos, el estudio se restringirá a las plataformas iOS y Android, a nivel de dispositivos móviles; en tanto que, a nivel de computadoras personales, únicamente se considerarán los equipos que utilizan MS-Windows.

3.5 JUSTIFICACIÓN

Este proyecto de investigación tiene como finalidad, que los estudiantes de la FIEC-CRUV logren minimizar los riesgos y amenazadas de ataques en ciberseguridad a su información, al momento de realizar sus labores académicas, personales o profesionales a través de la aplicación de las políticas de seguridad producto de esta investigación. Como resultado colateral, se espera que

disminuyan significativamente las pérdidas de información asociadas a los ataques de malware.

Se puede considerar a los estudiantes de la FIEC-CRUV como beneficiarios directos de esta investigación. Adicionalmente, dado que el informe de este proyecto será de acceso público, se puede considerar como beneficiarios indirectos a todos aquellos individuos interesados en documentarse en políticas de ciberseguridad y que hagan uso de dispositivos móviles y portátiles.

3.5.1 ANTECEDENTES Y ESTUDIOS PREVIOS

Es importante resaltar que, ante esta investigación no se encontraron estudios directamente vinculados al tema propuesto.

Para reforzar esta afirmación, se realizó una búsqueda documental de manera directa a los recintos bibliotecarios de las diferentes universidades, realizando de manera virtual una búsqueda en todo el país y de manera presencial en la ciudad de Santiago, provincia de Veraguas, con el objetivo de encontrar la posible existencia de proyectos previos correlacionados en el tema de investigación.

Mediante búsquedas de web no se lograron encontrar proyectos de investigación exactamente en el mismo ámbito de conocimiento de acuerdo con el tema enfocado en establecimientos de políticas de ciberseguridad; a continuación, se plantea una síntesis de los documentos más relacionados a la temática en desarrollo:

En primer término, la investigación por (Montero Salinas, 2021) titulada “**Manejo virtual en tiempos de pandemia, relacionado a las competencias personales, Estudiantes, Escuela Cerro Algodón**”, específicamente en el área del Marco Teórico señala aspectos sobre la seguridad de la información, donde **los niños a**

partir de temprana edad hacen uso de las herramientas tecnológicas perfectamente, reforzando la conducta desde corta edad, en la cual el usuario promedio se siente libre de navegar en cualquier sitio de Internet. No obstante, es importante entender que se debe **tener cuidado con algunas aplicaciones y usuarios que aparentan tener buenas intenciones, pero que, en realidad, estén en búsqueda de realizar acciones de ciberdelitos y ciberacoso online**.

En otro orden de ideas, la investigación titulada "**Ambiente simulado con malware para entrenamiento de usuarios regulares**", desarrolla una serie de fases, redactando paso a paso las formas en las que, por medio de herramientas de software funcionan cada uno de los malware más populares. Su objetivo es que los usuarios sean capaces de afrontar los peligros al infectarse sus dispositivos, utilizando técnicas con relación al uso de software, por ejemplo: el ransomware, para encriptar y desencriptar archivos, con la herramienta **hidden tear** bajo el algoritmo de AES. El uso de Spyrix keylogger para casos de malware llamados Spyware, el cual permite registrar todo tipo de evento para el posterior hurto de usuarios y contraseñas. El autor concluye que (Ramos Gómez, 2019):

- Los usuarios encuestados no sienten los ataques informáticos como una problemática como personas naturales, por lo que los inicios de sesión de Google están cada vez más al alcance de los ciberdelincuentes.

- El conocimiento que se adquiere destaca la manera con la que se navega de forma libre en Internet, evitando todo tipo de malware.

- El documento no tiene herramientas para la seguridad en dispositivos móviles.

- Resalta la importancia de añadir más herramientas para la detección y prevención de malware en la actualidad.

Por otro lado, (Vizuete Salazar, 2020) realizó un estudio para pequeñas y medianas empresas, llamado: “**Implementación de políticas de seguridad en dispositivos móviles para el manejo de la información en Pymes**”, el objetivo consistió en implementar políticas de seguridad basada en la normativa ISO en la empresa TELECOMEXPERT. Dicho estudio analizó aspectos esenciales como los riesgos, amenazas y vulnerabilidades, su población total se representó en 11 empleados, en la cual se encontraron debilidades en el manejo del acceso a las redes de la empresa relacionados con los dispositivos personales, falta de restricciones y prohibiciones en zonas interiores como también del listado de aplicaciones. Vizueta aporta 44 artículos de apoyo, concluyendo que el uso de esta eleva hasta en un 42.41% la seguridad de la empresa, los miembros mejoraron la confiabilidad en transmisión de datos por dispositivos móviles en un 36.36%.

En otro orden de ideas (Martínez & Martínez, 2018) en México llevaron a cabo su investigación sobre ciberseguridad llamado: **Los jóvenes y la ciberseguridad en zonas rurales del estado del Oaxaca Caso: instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165** para estudiantes de escolaridad en nivel medio, el propósito de esta tiene que ver con la utilidad que los jóvenes dan cuando se conectan vía Internet, accidentalmente muestran su información y datos personales. El plantel de estudio 165 del Instituto de Bachilleratos del Estado de Oaxaca fue el encargado de ser encuestado mediante una muestra no probabilística por conveniencia, 112 estudiantes representaron el 100% de encuestados. Las autoras del trabajo concluyen la importancia de un plan de estudios con asignaturas dirigidas en seguridad informática (algunos estudiantes de zonas rurales desconocen el tema), exaltando a la educación como el factor clave inicial para la seguridad digital, invitando al sector privado en Internet y al Gobierno a reforzar la seguridad y privacidad de la información, a través de su punto de vista.

Adicionalmente, (Rodríguez C, y otros, 2022) en su artículo: **Percepción de la ciberseguridad ciberdelitos, normas legales y políticas de seguridad**, investigaron en la Universidad de Panamá con Sede en Veraguas, las practicas que emplean los coordinadores, pertenecientes a la facultad de Informática, como también quienes están asociados a la Escuela de Informática para la Gestión Educativa y Empresarial en cuanto a ciberseguridad, ciberdelitos, normas legales vigentes y las políticas asociadas a los medios electrónicos. Los resultados se recogieron por medio de encuestas en línea entre los meses de junio-julio 2022. El 96.96% de los 25 docentes que respondieron, piensan que es necesario solicitar acciones que tengan que ver con el reforzamiento en nuevas políticas de ciberseguridad tanto para el uso como manejo en todo el ámbito que rodea a la informática general, esto debido a la alta tasa de consumo tecnológicos en los que tenga que ver con procesos y actividades al interactuar e intercambiar información a través de Internet. Concluyen con diversas ideas, entre ellas las de desarrollar programas de capacitación en ciberseguridad y políticas que se adapten a las temáticas propuestas en la investigación.

Finalmente, Kaspersky en uno de sus diversos estudios relacionados a las temáticas de la ciberseguridad, nombrado **Evolución de las ciber amenazas en el segundo trimestre de 2022. Estadísticas de amenazas móviles**, evalúa las amenazas móviles alrededor del mundo. Señala la neutralización de 5 millones y medio de software malicioso, de la cual más de 400 mil tiene que ver con las instalaciones de aplicaciones de dudosa procedencia, destacando un listado de diversos troyanos con múltiples permisos sin el consentimiento del usuario únicamente para tener intenciones de robar información personal gracias a software modificados de mensajerías instantáneas y robos bancarios (Shishkova, 2022).

En consecuencia, se puede observar que las evidencias de proyectos anteriormente mencionados y que están relacionados a la ciberseguridad tienden

a ser más enfocados para las áreas empresariales como también (*en un pequeño número*) para aquellas personas que aún desconocen en su totalidad la seguridad de la información, llámese estudiantes de niveles escolares o administrativos de centros Medios y Universitarios. Se desea llevar protocolos de protección antimalware a una población en general, sobre todo para estudiantes de carreras universitarias dedicadas a la Informática, esto porque actualmente no existen proyectos dedicados a quienes se van adentrando a la computación.

Por lo tanto, es de gran interés que para la población objetivo se les pueda transmitir los conocimientos necesarios en la protección de datos personales ubicados en sus dispositivos tecnológicos, ofreciendo a la problemática mecánicas novedosas para que eviten ser expuestos a tal rango de perder su valiosa información por parte de los delincuentes que usan el malware para fines poco éticos.

3.6 CONSECUENCIAS DE LA INVESTIGACIÓN

Este proyecto de investigación aportará un conjunto de políticas de ciberseguridad que beneficiarán tanto al estudiante de la FIEC-CRUV como también todo aquel usuario informático promedio que desee documentarse en el tema, a fin de minimizar el riesgo potencial de ser víctima de ataques de malware en sus dispositivos móviles o portátiles.

3.7 FACTIBILIDAD DEL PROYECTO

La investigación puede llevarse a cabo, ya que se dispone de los recursos requeridos, que son los siguientes:

3.7.1 RECURSOS HUMANOS

- Se contará con la guía y apoyo de un profesor asesor experto en el tema, quien desempeñará un papel fundamental al brindar docencia y orientación durante la realización de la investigación.

- Recintos universitarios virtuales ubicados en distintos puntos de la provincia de Veraguas como apoyo en las búsquedas de investigaciones similares.

- Estudiantes pertenecientes a la carrera Universitaria de Informática. Son quienes prestarán su tiempo para proceder a contestar en base a sus conocimientos y experiencias la encuesta sobre la ciberseguridad.

3.7.2 RECURSOS MATERIALES

Principalmente:

- **Literatura especializada en el tema:** Fuente valiosa de información que permitirá identificar las áreas que requieren más investigación y a la misma vez reforzará el levantamiento del marco teórico.

- **Internet:** Para conseguir datos en línea de carácter notable, confiable y correlacionado al tema sujeto de estudio.

3.7.3 RECURSOS FINANCIEROS

La implementación de este proyecto de investigación se está sufragando con recursos propios del investigador.

La financiación del proyecto necesitará un aproximado de B/. 611.80 con la cual supone, cubrirá el consumo de la realización del proyecto. Los detalles de gastos están sustentados dentro de los cronogramas de actividades que se exponen a continuación.

Seguidamente, se mostrará el presupuesto semanal que se está ejecutando.

Tabla 1: Presupuesto Semanal de Gastos del Proyecto

Gastos:	Costo
Transporte por semana	B/. 6.60
Alimentación por semana	B/. 2.50
Refrigerio por semana	B/. 1.80
Total de gastos por semana	**B/. 10.90**

Fuente: Recopilación del autor

A la fecha de confección de este presupuesto semanal de gastos, el autor de la investigación está en posibilidad para enfrentar el desafío económico.

3.8 CRONOGRAMA DE ACTIVIDADES

Enseguida, se muestra el cronograma de actividades mensuales detallando cada uno de los movimientos/gastos en el tiempo que se lleva elaborando el proyecto de investigación.

Tabla 2: Cronograma de Actividades: Selección del Tema, Revisión Bibliográfica, Investigación Documental

	ACTIVIDADES			
MES	**1.SELECCIÓN DEL TEMA**	**2.REVISIÓN BIBLIOGRÁFICA**	**3.INVESTIGACIÓN DOCUMENTAL**	**SUB TOTAL**
MES 1	B/. 45.90			B/. 78.60
	B/. 10.90			
	B/. 10.90			
	B/. 10.90			
MES 2		B/. 10.90		B/. 76.30
		B/. 10.90		
		B/. 10.90		
MES 3		B/. 10.90		
		B/. 10.90		
MES 4		B/. 10.90		
MES 5		B/. 10.90		
MES 6			B/. 10.90	B/. 130.80
			B/. 10.90	
			B/. 10.90	
			B/. 10.90	
MES 7			B/. 10.90	
			B/. 10.90	
			B/. 10.90	
MES 8			B/. 10.90	
MES 9			B/. 10.90	
			B/. 10.90	
MES 10			B/. 10.90	
			B/. 10.90	

Fuente: Recopilación del autor

Tabla 3: Cronograma de Actividades: Elaboración del Marco Teórico, Prueba de Campo, Análisis Estadístico

	ACTIVIDADES			
MES	**4.ELABORACIÓN DEL MARCO TEORICO**	**5.PRUEBA DE CAMPO**	**6. ANÁLISIS ESTADÍSTICO**	**SUB TOTAL**
MES 10	B/. 10.90			B/. 65.40
	B/. 10.90			
	B/. 10.90			
MES 11	B/. 10.90			
MES 12	B/. 10.90			
	B/. 10.90			
MES 13		B/. 10.90		B/. 65.40
		B/. 10.90		
		B/. 10.90		
		B/. 10.90		
MES 14		B/. 10.90		
		B/. 10.90		
MES 15			B/. 10.90	B/. 43.60
			B/. 10.90	
			B/. 10.90	
			B/. 10.90	

Fuente: Recopilación del autor

Tabla 4: Cronograma de Actividades: Revisiones Finales y Sustentación

	ACTIVIDADES		
MES	**7. REVISIONES FINALES**	**8. SUSTENTACIÓN**	**SUB TOTAL**
MES 16	B/. 10.90		B/. 98.10
	B/. 10.90		
	B/. 10.90		
	B/. 10.90		
MES 17	B/. 10.90		
	B/. 10.90		
	B/. 10.90		
	B/. 10.90		
MES 18	B/. 10.90		
		B/. 10.90	B/. 53.60
		B/. 10.90	
		B/. 31.80	

Fuente: Recopilación del autor

Por ende, el coste por actividad, así como también el total estimado durante toda la elaboración del proyecto se visualiza en el siguiente cuadro:

Tabla 5: Cronograma de Actividades: Costo por Actividad

ACTIVIDAD	COSTO POR ACTIVIDAD
1.SELECCIÓN DEL TEMA	B/. 78.60
2.REVISIÓN BIBLIOGRÁFICA	B/. 76.30
3.INVESTIGACIÓN DOCUMENTAL	B/. 130.80
4.ELABORACIÓN DEL MARCO TEORICO	B/. 65.40
5.PRUEBA DE CAMPO	B/. 65.40
6. ANÁLISIS ESTADÍSTICO	B/. 43.60
7. REVISIONES FINALES	B/. 98.10
8. SUSTENTACIÓN	B/. 53.60
TOTAL	**B/. 611.80**

Fuente: Recopilación del autor

Finalmente, el cuadro a continuación presenta los tipos de gastos estimados durante la elaboración del proyecto:

Tabla 6: Presupuesto Estimado por Tipo de Gasto

TIPO DE GASTO	GASTO UNITARIO	CANTIDAD	SUB TOTAL
COMPRA DE DISCO EXTERNO	B/. 25.00	1	B/. 25.00
COMPRA DE INTERFAZ SATA A USB 3.0	B/. 10.00	1	B/. 10.00
TRANSPORTE DESDE SANTA FE HASTA EL CRUV-FIEC Y VICEVERSA	B/. 6.60	51	B/. 336.60
ALIMENTACIÓN POR SEMANA	B/. 2.50	51	B/. 127.50
REFRIGERIO POR SEMANA	B/. 1.80	51	B/. 91.80
IMPRESIÓN DOCUMENTOS	B/. 20.90	1	B/. 20.90
TOTAL			**B/. 611.80**

Fuente: Recopilación del autor

4. MARCO METODOLÓGICO

A continuación, en este capítulo se empezarán a describir tópicos como los cuales son: tipo de investigación, diseño de investigación, la población, hipótesis de trabajo, variables y definición de variables, instrumentos de recolección de datos,

las técnicas de procesamiento y análisis de datos y por último el análisis de los resultados

4.1 TIPO DE INVESTIGACIÓN

Esta investigación, presenta un alcance que se enmarca en los niveles exploratorio y descriptivo ya que (Baiaragi & Munot, 2019).

- Se efectúa un estudio exploratorio generalmente cuando se estudian áreas que han recibido escasa atención o también en las situaciones donde se busca realizar investigaciones para perfeccionar el avance de dominio en el tema de estudio centrado.

- Los estudios descriptivos se realizan cuando se intenta representar o analizar los hechos anteriores y/o actuales. Estas investigaciones se caracterizan, sobre todo, porque no conlleva a tener ningún control sobre las variables que se están utilizando.

Sabiendo que:

1. Con base en el contexto previo, esta investigación se puede catalogar como de tipo **exploratorio** porque los estudios mencionados en el apartado de antecedentes (sección 3.5.1) no reflejan ni tampoco desarrollan la temática exacta que se desea analizar la cual es: **establecer el nivel de conocimiento en políticas de ciberseguridad para contrarrestar el malware en dispositivos móviles y portátiles orientadas a los estudiantes de la FIEC-CRUV**.

2. Como complemento, el estudio puede ser considerado como **descriptivo** ya que permitirá identificar las posibles circunstancias por las cuales los

dispositivos móviles y portátiles de los estudiantes FIEC-CRUV, pueden ser blanco de programas maliciosos debido al nivel de conocimiento que tiene dicha población sobre la temática de la ciberseguridad. Adicionalmente, se proponen criterios ponderados que dejarán en evidencia las practicas o métodos que los estudiantes aplican actualmente para contrarrestar las amenazas que representa los diversos tipos de malware comunes y potencialmente dañinos. De esta manera los resultados obtenidos facilitarán una posible solución a las fallas de ciberseguridad que atentan contra los dispositivos electrónicos más usados por la población objeto del estudio. La documentación propuesta también será de carácter público, por lo que todo usuario informático, si así lo desea, podrá estudiarla.

4.2 DISEÑO DE LA INVESTIGACIÓN

El diseño de este proyecto se basa en el tipo **no-experimental** ya que en su definición se dedican a investigar variables existentes y por ende no se tiene pensado manipularlas de ninguna manera (Coolican, 2024).

4.3 CRITERIOS IDENTIFICADOS QUE CONFORMAN EL NIVEL DE CONOCIMIENTO EN CIBERSEGURIDAD EN LOS ESTUDIANTES DEL FIEC-CRUV

Continuando con el planteamiento ubicado en el marco teórico, a partir de la sección 2.3, se establecen dos criterios destacados a nivel general que constituyen a la variable dependiente del problema: nivel de conocimiento en ciberseguridad:

- **Identificación de las amenazas de malware más comunes:** Los estudiantes de la facultad de informática deben conocer por lo menos

algunos de los nombres o significados de los programas maliciosos más comunes que atentan contra la seguridad de sus dispositivos personales.

- **Dominio de las técnicas y políticas en ciberseguridad:** Los estudiantes de la facultad de informática deben conocer por lo menos algunas estrategias fundamentales para mantener una buena ciberseguridad en temas como: navegación por Internet, instalación de software no seguro, gestión de contraseñas, identificar estafas, actualización de software etc.

4.4 HIPÓTESIS DE TRABAJO

Este anteproyecto de investigación se desarrollará con base en la hipótesis de trabajo que se plantea a continuación:

H_i: El nivel de conocimiento sobre ciberseguridad de los estudiantes de la FIEC-CRUV, **es al menos alto**, en función de los resultados de la encuesta aplicada y del modelo de evaluación utilizado.

H_0: El nivel de conocimiento sobre ciberseguridad de los estudiantes de la FIEC-CRUV, **no es alto**, en función de los resultados de la encuesta aplicada y del modelo de evaluación utilizado.

4.4.1 VARIABLES

Una variable es aquella la cual puede definirse como un carácter, condición o concepto que consigue tomar diferentes valores y, por lo tanto, ser mensurable. (Thomas, 2021).

Las variables que se definen dentro de esta investigación son:

- **Variable dependiente:** Se centra en el nivel de conocimiento en políticas de ciberseguridad que poseen los estudiantes del FIEC-CRUV al momento de ser encuestados. Destacando algunos indicadores como: gestión de contraseñas, uso adecuado de los respaldos en la nube, de correos electrónicos como también de aplicaciones, identificación de estafas virtuales etc.

- **Variable Independiente:** Se enfoca en los resultados obtenidos a través de la aplicación de encuesta a los estudiantes de la FIEC-CRUV.

4.4.2 DEFINICIÓN DE VARIABLES

En el siguiente cuadro se presenta la definición de variables, que incluye la variable, su definición conceptual y operacional, y el procedimiento de medición correspondiente.

Tabla 7: Definición De Variables

Variable	Definición Conceptual	Definición Operacional	Procedimiento De Medición
Resultados obtenidos a través de la aplicación de encuesta **(V. Independiente)**.	Datos recopilados y analizados sobre las respuestas ofrecidas por parte de la población encuestada, en cuanto a su nivel de aplicación de políticas de ciberseguridad orientadas a la protección de su información personal.	Cuantificar el nivel de conocimiento que tiene la población encuestada, en cuanto al nivel de aplicación de políticas de ciberseguridad orientadas a la protección de su información personal.	A través de una batería de preguntas preestablecidas que se le aplicará a la población objeto del estudio.

Variable	Definición Conceptual	Definición Operacional	Procedimiento De Medición
Nivel de conocimiento en ciberseguridad **(V. Dependiente)**.	Capacidad de los usuarios en cuanto a su manejo y aplicación de los conceptos y técnicas necesarias para proteger a sus los dispositivos tecnológicos ante los programas maliciosos que rondan en la Internet o periféricos, así como para desenvolverse en ciber-ambientes no confiables.	Establecer si el nivel de manejo y aplicación de los conceptos y técnicas relacionados a la ciberseguridad es mínimamente aceptable, a fin de permitirles un desenvolvimiento razonable en ciber-ambientes no confiables.	Los resultados obtenidos a nivel de la encuesta que se aplicará a la población objetivo se valorarán frente a un modelo de evaluación que será elaborado por el autor.

Fuente: El autor

4.5 DISEÑO DEL ESTUDIO

El diseño de estudio estará conformado por una sola encuesta dirigida a una población estudiantil universitaria como requisito único donde a través de ellos se aplique una prueba estadística de tal modo que contradiga o rectifique la hipótesis planteada de la investigación.

4.6 POBLACIÓN

La población específica a la cual se le realizó el estudio de la investigación en ciberseguridad fueron los estudiantes de todos los años de la Facultad de Informática, Electrónica y Comunicación del Centro Regional Universitario de Veraguas (FIEC-CRUV) en el periodo académico 2025. En el siguiente cuadro se presenta la población estimada a la cual se aplicó el estudio, tomada en función de la nota informativa que se presenta en la Figura 3.

Tabla 8: Población Estimada Objeto de Investigación

Tipo de población	Cantidad
Estudiantes de la Licenciatura en Informática para la Gestión Educativa y Empresarial en la FIEC-CRUV	103
Estudiantes de la Licenciatura en Ingeniería en Informática en la FIEC-CRUV	85
Total de Estudiantes en la FIEC-CRUV	**188**

Fuente: (Secretaría Académica, CRUV, 2025)

4.7 MUESTRA

La muestra es la representación de un grupo pequeño que se estudiará de la población debido a la gran cantidad de dificultades que se pueden presentar al hacer el sondeo en general (Coolican, 2024).

Contrario a una muestra se encuentra el censo, el cual básicamente se dedica a estudiar a toda la población de un área sin dejar excluido a ningún individuo evitando de esta manera a quienes creen que opinión no cuenta (Hernández-Sampieri & Mendoza Torres, 2018).

Debido a que la cantidad de la población objeto de estudio es de 188 (ver Tabla 8) y se encuentra concentrada en una localidad geográfica específica (CRUV), se considera que el investigador tiene la capacidad de realizar el estudio mediante un censo.

4.8 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Una vez definidas las variables de investigación sección 4.4.1 se procede con la elaboración de los instrumentos para la recolección de datos, que es un paso imprescindible en el proceso de investigación y consiste en aplicar uno, dos o la cantidad necesaria de herramientas para conseguir la información útil que

requiere el estudio (Hernández Sampieri, Mendoza Torres, Méndez Valencia, & Cuevas Romo, 2019).

4.8.1 ENCUESTA

Para este proyecto de investigación únicamente se realizó una sola encuesta dirigida a los estudiantes cursando en el FIEC-CRUV, aplicando diferentes tipos de preguntas en el ámbito de las políticas de ciberseguridad orientadas en establecer su nivel de conocimiento en aspectos tales como: identificar por lo menos un tipo de malware, conocimiento en gestión de contraseñas, reconocer las estafas virtuales, identificación de archivos de dudosa procedencia etc.

Las generalidades de la encuesta aplicada se detallan a continuación:

- **Identificación de la población de estudio**: La cantidad de estudiantes de la FIEC-CRUV en Santiago de Veraguas, que contestaron las interrogantes de políticas de ciberseguridad.

- **Ámbito geográfico**: Censo que se aplica a toda la población de estudiantes pertenecientes del FIEC-CRUV en la ciudad de Santiago de Veraguas.

- **Método de administración**: Mediante enlace o link directo a la plataforma FormsApp para que la población de estudio conteste las interrogantes.

- **Diseño de instrumento:** El instrumento que se aplicó a los estudiantes de la FIEC-CRUV se presenta en la sección 10.1.

Cabe destacar que la aplicación de la evaluación a los estudiantes de Informática pertenecientes al FIEC-CRUV se realizará de forma **autoadministrada**, es decir

que la encuesta o cuestionario se les enviará directamente a través de enlaces que conduzcan a un sitio web donde se implementarán las preguntas, de modo que dispongan de la oportunidad de contestar a las interrogantes en el tiempo que tengan libre (Hernández-Sampieri & Mendoza Torres, 2018).

4.8.2 OBSERVACIÓN

En el contexto de este proyecto de investigación la observación no es necesaria debido a que con ella se estudia el comportamiento y situaciones **observables** a través de diferentes categorías, contrario a lo que el autor requiere que es: conocer el nivel de conocimiento que tienen los estudiantes universitarios del FIEC-CRUV. Este conocimiento se adquiere directamente de la encuesta aplicada a la población vía censo (Hernández Sampieri, Mendoza Torres, Méndez Valencia, & Cuevas Romo, 2019).

4.9 ANÁLISIS DE DATOS

Reiterando que el estudio de esta investigación es de tipo no experimental, el análisis de datos sugiere que se recojan y analicen las estadísticas descriptivas a partir de los datos. No sin antes haber pasado por una etapa de predicción y análisis de todas las informaciones previstas (Cumming & Calin-Jagemen, 2024).

4.9.1 PRUEBA DE HIPÓTESIS EN FUNCIÓN A LA HIPÓTESIS DE TRABAJO

Habiendo formulado la prueba de hipótesis anteriormente en la sección 4.4, el proyecto de investigación plantea que:

Ecuación 1: Prueba De Hipótesis En Función De La Hipótesis De Trabajo

$$H_i : 60\% < NC$$

$$H_0 : 60\% \geq NC$$

Fuente: El autor

Donde:

- H_i representa a la hipótesis alterna.
- H_0 hace referencia a la hipótesis nula
- NC representa el nivel de conocimiento alcanzado por la población encuestada.

4.10 DISEÑO DEL MODELO DE EVALUACIÓN DE LOS CONOCIMIENTOS QUE TIENEN LOS ESTUDIANTES DEL FIEC-CRUV EN CUANTO A POLÍTICAS DE CIBERSEGURIDAD

Complementando lo descrito en los puntos anteriores, uno de los objetivos de esta investigación es diseñar un modelo de evaluación que cumpla con el principio fundamental el cual es: el establecimiento de políticas de ciberseguridad orientadas a los estudiantes de la FIEC-CRUV, para que de tal manera dichos estudiantes tengan la posibilidad de contrarrestar las amenazas de malware o programas maliciosos que se introducen en los dispositivos móviles y portátiles. Para ello resulta útil desarrollar este proyecto apoyándose en el **estudio basado en objetivos**, donde su manera de manejar el estudio de investigación trata sobre preguntas limitadas a la población objetivo, donde al final en la recolección del informe muestren como se lograron esos objetivos planteados y bajo que evidencias se justifican (Stufflebeam & Coryn, 2014).

4.10.1 FUNDAMENTOS DEL MODELO DE EVALUACIÓN

Para lograr el diseño del modelo de evaluación se necesita comprender los fundamentos teóricos como prácticos del tema de ciberseguridad a la población objetivo. De este modo el plan de diseño de evaluación es la de obtener información que responda y respalde de forma razonable el planteamiento del problema (Hernández-Sampieri & Mendoza Torres, 2018).

Del mismo modo la elaboración de un modelo de evaluación no debe carecer de sentido. Para (Brace & Bolton, 2022) resulta ser esencial evitar algunos errores en la aplicación de encuestas o cuestionarios, para que al recoger los datos de la población objetivo al momento de la evaluación estos no generen dudas o no puedan interpretar correctamente las interrogantes.

4.10.2 INDICADORES DEL MODELO

Como consecuencia para los indicadores de modelo se hace uso de diferentes puntos antes redactados en el apartado desde la sección 2 hacia adelante.

Tabla 9: Indicadores del Modelo de Evaluación

#	Indicadores	Peso	Abreviatura
1	Políticas de Seguridad Informática	6.66%	**PSI**
2	Exposición de información personal en Internet	6.66%	**EIPI**
3	Terminología básica de ciberseguridad	6.66%	**TBC**
4	Conocimientos formales de seguridad informática	6.66%	**CFSI**
5	Control de claves de acceso	6.66%	**CCA**
6	Métodos de recuperación efectivos	6.66%	**MRE**
7	Supervisión de información mediante aplicaciones	6.66%	**SIMA**
8	Ideas para salvaguardar datos personales	6.66%	**ISDP**
9	Software de apoyo contra webs maliciosas.	6.66%	**SAWM**
10	Identificación de malfuncionamiento en sistemas	6.66%	**IMS**
11	Actualización de software	6.66%	**AS**
12	Gestión de contraseñas	6.66%	**GC**
13	Razonamiento ante ataques potenciales.	6.66%	**RAP**
14	Comodidad ante software de dudosa procedencia	6.66%	**CSDP**
15	Responsable principal ante software malicioso.	6.66%	**RPSM**

Fuente: El Autor

4.10.3 INTERPRETACIÓN DE LOS PESOS QUE SE LE ASIGNÓ A CADA INDICADOR EN CUANTO A POLÍTICAS DE CIBERSEGURIDAD

El peso de cada uno de los indicadores que representan a las políticas de ciberseguridad posee porcentajes iguales, debido a que se considera a cada punto con igual nivel de importancia, al momento de considerar los niveles de conocimiento en ciberseguridad.

4.10.4 MATRIZ DE PONDERACIÓN DE MODELO

A continuación, se presenta la matriz de ponderación del modelo de evaluación que se utilizará para establecer la calificación que obtuvieron los estudiantes del FIEC-CRUV en cuanto a su nivel de conocimiento en ciberseguridad.

La escala de modelo de evaluación que se usará es el de **relación**, similar a otras escalas populares, pero con la diferencia de que la escala de relación añade el punto cero, lo que quiere decir “un conocimiento mínimo o nulo” en dado caso de que se llegue a encontrar un nivel bajo en políticas de ciberseguridad (Mbanaso, Abrahams, & Chinedu Okafor, 2023).

El siguiente cuadro muestra el modelo de la matriz de ponderación a usar durante la encuesta:

Tabla 10: Matriz de Ponderación del Nivel de Conocimiento que Tienen los Estudiantes del FIEC-CRUV en cuanto a ciberseguridad en dispositivos móviles y portátiles

Ponderación (P)	Nivel de conocimiento que tienen los estudiantes del FIEC-CRUV en cuanto a políticas de ciberseguridad en dispositivos móviles y portátiles
P < 20%	**Muy bajo**
20% < P < 40%	**Bajo**
40% < P < 60%	**Satisfactorio**
60% < P < 80%	**Alto**
80% < P	**Muy alto**

Fuente: El Autor & (Mbanaso, Abrahams, & Chinedu Okafor, 2023)

El cuadro anterior se debe interpretar de la siguiente forma:

- Si **P** es menor a 20%, se da por entendido como el nivel de conocimiento en ciberseguridad muy bajo.

- Si **P** resulta ser mayor o igual a 20% y menor que 40%, se da por hecho como el nivel de conocimiento en ciberseguridad bajo.

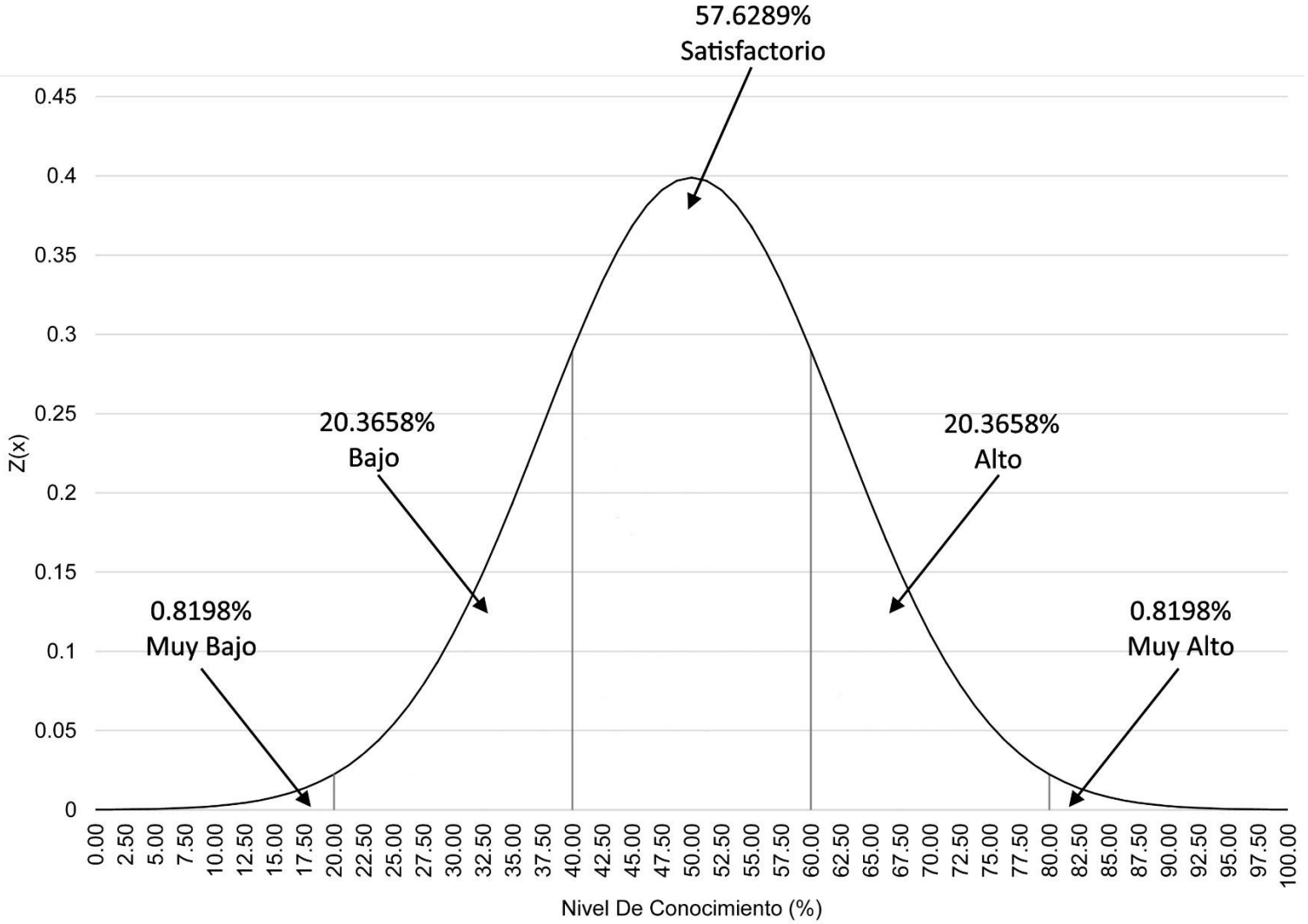
- Si **P** resulta ser mayor o igual a 40% y menor que 60%, se asimila como el nivel de conocimiento en ciberseguridad satisfactorio.

- Si **P** resulta ser mayor o igual a 60% y menor a 80% se deduce como el nivel de conocimiento en ciberseguridad alto.

- Por último, si **P** resulta ser mayor o igual a 80% se intuye como nivel de conocimiento en ciberseguridad muy alto.

Dado que la población estudiada supera ampliamente a los 30 individuos, se puede asumir que se ajusta a una distribución normal en cuanto al nivel de conocimiento que tienen en cuanto a políticas de ciberseguridad, de acuerdo con los rangos establecidos en la Tabla 10 y que se representa de forma gráfica en la Figura 2. Dicha distribución también es conocida como campana de Gauss y representa la probabilidad continua simétrica donde su punto más alto representa la media de los valores analizados, en tanto que sus costados simbolizan la desviación estándar de la muestra (Agresti, Franklin, & Klingenberg, 2023).

Figura 2: **Distribución Normal Para Los Rangos Del Modelo De Evaluación**



Fuente: El autor

5. PROCESAMIENTO, ANÁLISIS Y RESULTADOS DE LA INVESTIGACIÓN

En el siguiente capítulo se explicará de forma detallada: el procesamiento, análisis y resultados de la información adquirida al desarrollar este tema de investigación.

5.1 RESULTADOS DE LA INVESTIGACIÓN

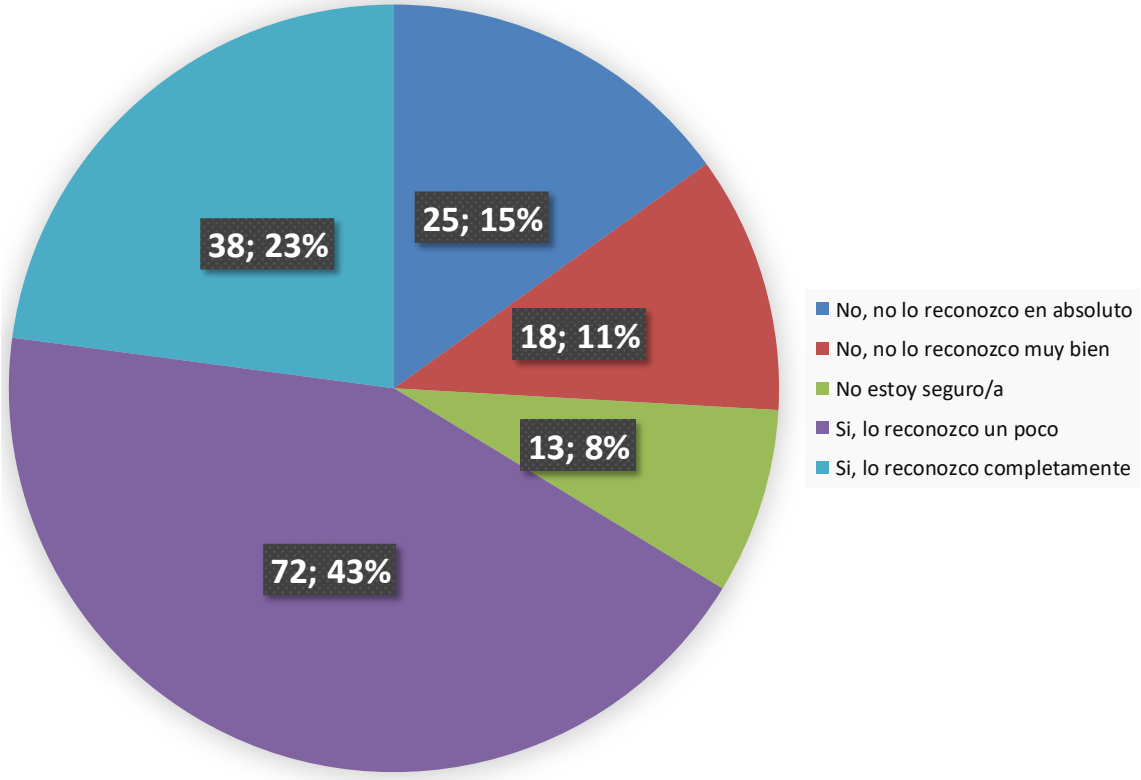
Los datos que se utilizaran en esta sección provienen originalmente de la participación de la encuesta aplicada a los estudiantes de la FIEC-CRUV en cuanto al nivel de conocimiento en políticas de ciberseguridad.

En consecuencia, se detallan las diferentes interrogantes planteadas por el investigador, con base en los indicadores del modelo de evaluación propuesto en la Tabla 9, en conjunto con sus debidos gráficos.

5.1.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

En el Gráfico 1, se presenta la opinión del grupo encuestado acerca de la pregunta sobre el nivel de identificación que tienen del concepto de políticas de seguridad informática.

Gráfico 1: ¿Reconoce el concepto de políticas de seguridad informática?



Fuente: El autor

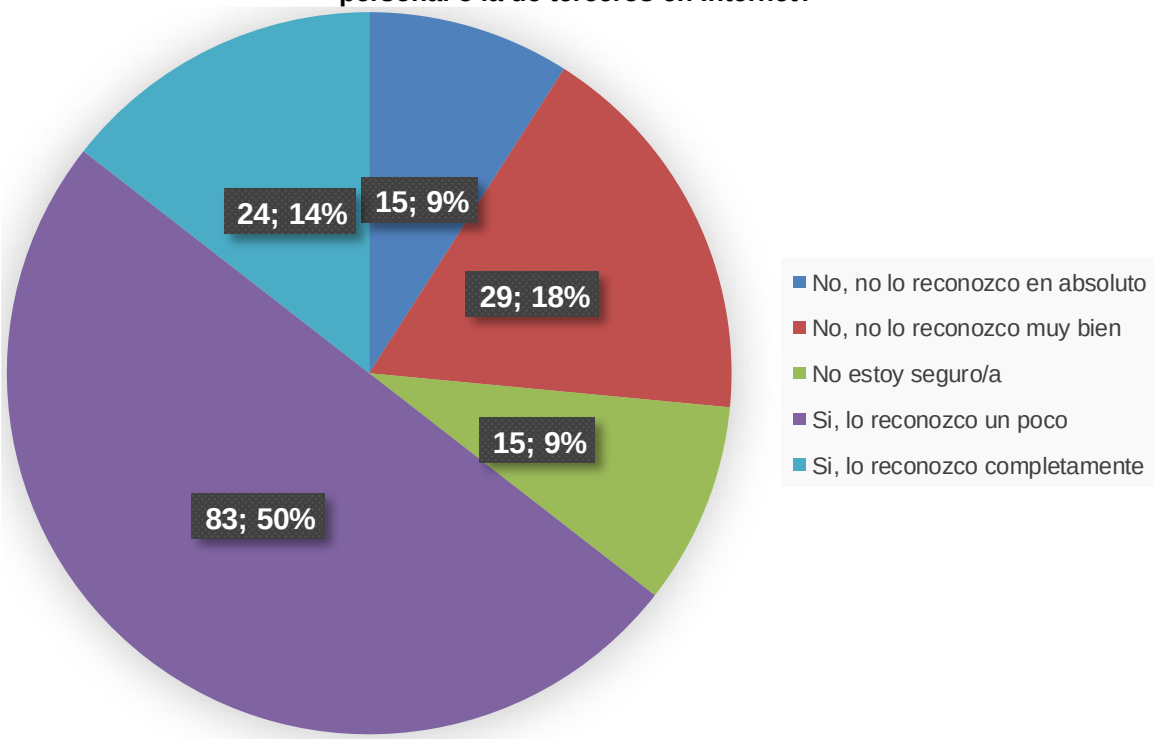
En dicho Gráfico, se evidencia que el 43% dijo que reconoce un poco el término de políticas de seguridad informática, el 23% lo reconoce completamente, 15% no lo reconoce en absoluto, el 11% no lo reconoce muy bien y el 8% no está seguro/a.

Se puede observar que la cantidad mayor de la población encuestada respondió en un 43% que solo reconoce un poco el concepto de las políticas de seguridad informática, dejando en evidencia que están un tanto familiarizados en el tema más sin embargo no manejan el tema a cabalidad.

5.1.2 EXPOSICIÓN DE INFORMACIÓN PERSONAL EN INTERNET

En el Gráfico 2, se presenta la opinión del grupo encuestado acerca de la pregunta de la capacidad para identificar riesgos de exposición de información en Internet.

Gráfico 2: ¿Identifica los riesgos asociados con la exposición de su información personal o la de terceros en Internet?



Fuente: El autor

En el Gráfico 2 se observa que el 50% de la población respondió que, si reconoce un poco los riesgos asociados con la exposición de su información personal o la de terceros en internet, mientras que el 18% dice no lo reconoce muy bien, el 14% dijo que lo reconoce completamente, el 9% no lo reconoce en absoluto y el otro 9% no está segura.

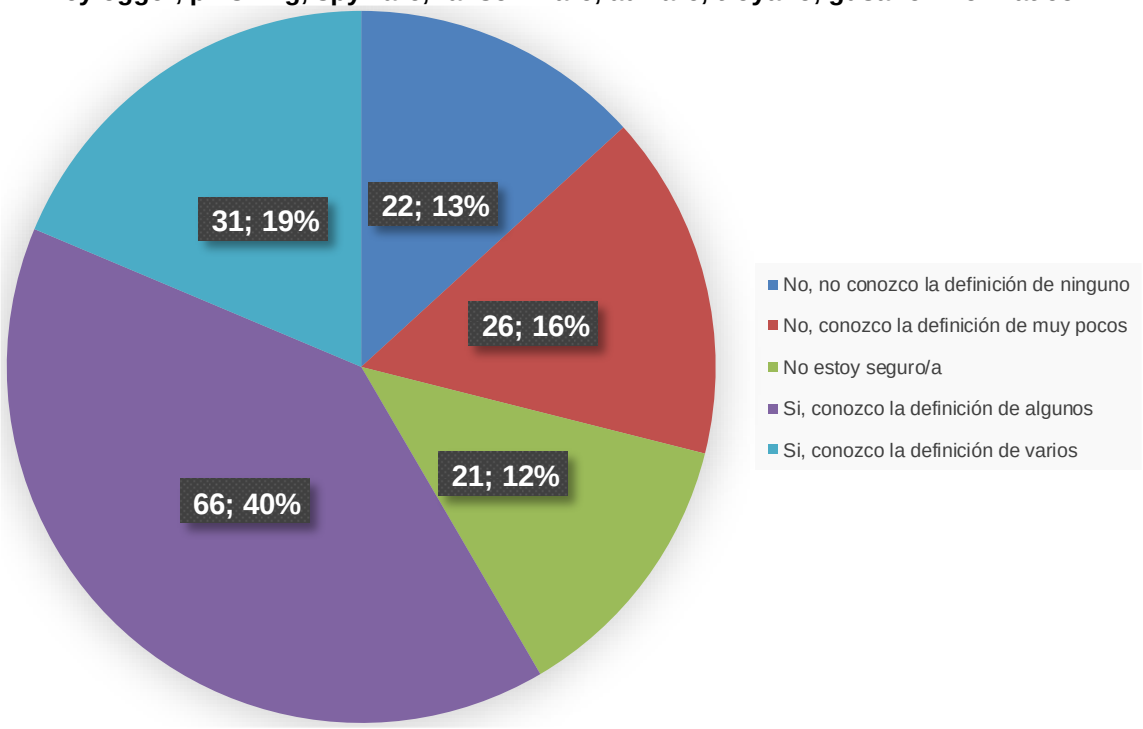
El 50% de los encuestados dice identificar en parte los riesgos de la exposición de su información personal o de terceros en internet, lo cual se puede interpretar

como un indicio positivo de su conciencia sobre las amenazas que pueden comprometer la integridad, disponibilidad o la confidencialidad de su información.

5.1.3 TERMINOLOGÍA BÁSICA DE CIBERSEGURIDAD

En el Gráfico 3, se presenta la opinión del grupo encuestado acerca de la pregunta para identificar la terminología básica de ciberseguridad.

Gráfico 3: ¿Conoce la definición de al menos uno de los siguientes términos keylogger, phishing, spyware, ransomware, adware, troyano, gusano informático?



Fuente: El autor

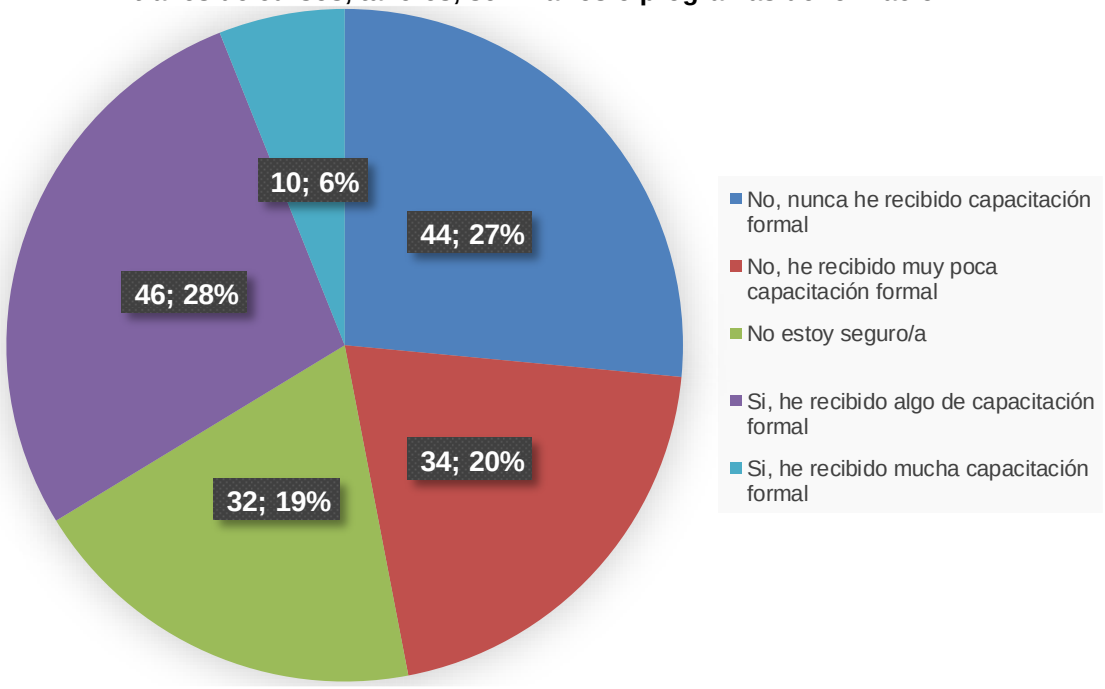
En el Gráfico 3 manifiesta que 40% de la población encuestada contestó que conoce la definición de algunos términos de malware como, por ejemplo: keylogger, phishing, spyware, ransomware, adware, troyano, gusano informático, el 19% dijo conocer la definición de varios, el 16% dijo conocer la definición de muy pocos y el 13% dijo no conocer la definición de ninguno, así como también no estar seguro/a.

Aunque el 40% de los encuestados dice dijo conocer la definición de algunos términos de malware, lo cual quiere decir bajo interpretación propia que están familiarizados con algunos tipos de malware, pero no con todos. Este aspecto es preocupante por cuanto que es importante poder reconocer a cada una de estas amenazas, puesto que individualmente tienen características únicas y distintivas entre sí.

5.1.4 CONOCIMIENTOS FORMALES DE SEGURIDAD INFORMÁTICA

En el Gráfico 4, se presenta la opinión del grupo encuestado acerca de la pregunta para identificar los conocimientos formales de seguridad informática.

Gráfico 4: ¿Ha recibido capacitación formal sobre seguridad informática, ya sea a través de cursos, talleres, seminarios o programas de formación?



Fuente: El autor

En el Gráfico 4 el encuestado respondió con un 28% haber recibido algo de capacitación formal, el 27% dijo nunca haber recibido capacitación formal, el 20%

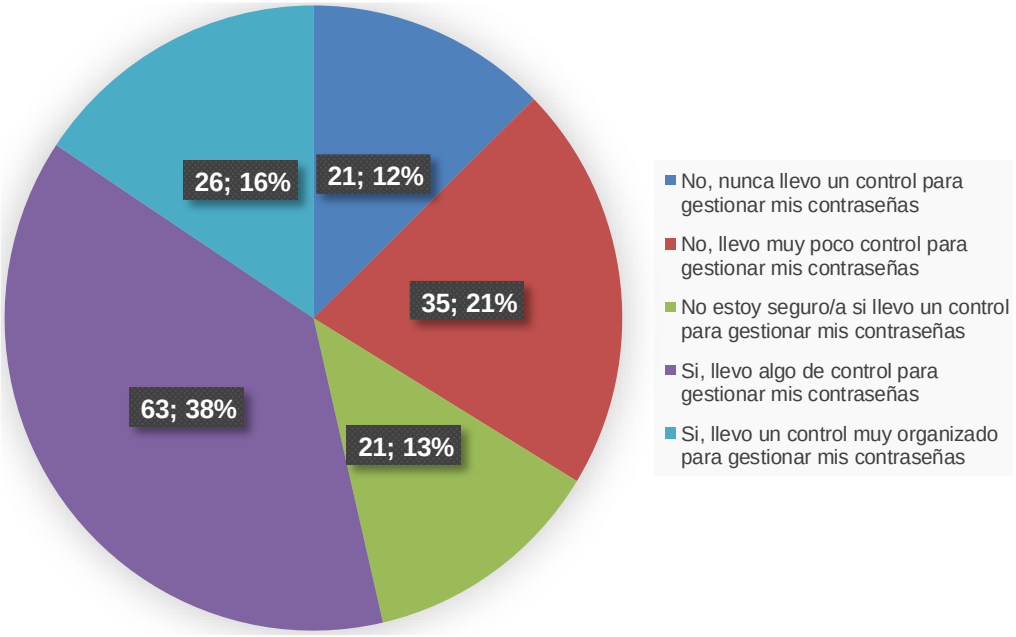
dijo haber recibido muy poca capacitación formal, el 19% no está seguro/a y el 6% si ha recibido mucha capacitación formal.

Lo anterior es una situación un poco llamativa y a la vez preocupante, que solamente el 28% de los encuestados hayan adquirido algo de capacitación en cuanto a seguridad informática se refiere. Puesto que es un tema que se expande comúnmente y requiere de conocimientos moderados para acatar cualquier eventualidad.

5.1.5 CONTROL DE CLAVES DE ACCESO

En el Gráfico 5, se presenta la opinión del grupo encuestado acerca de la pregunta sobre el control de claves de acceso.

Gráfico 5: ¿Mantiene o lleva algún tipo de control para gestionar todas sus contraseñas en caso de olvidarlas?



Fuente: El autor

En el Gráfico 5 se muestra que el 38% de los encuestados afirma que lleva algo de control para gestionar sus contraseñas en caso de olvidarlas, el 21% lleva muy

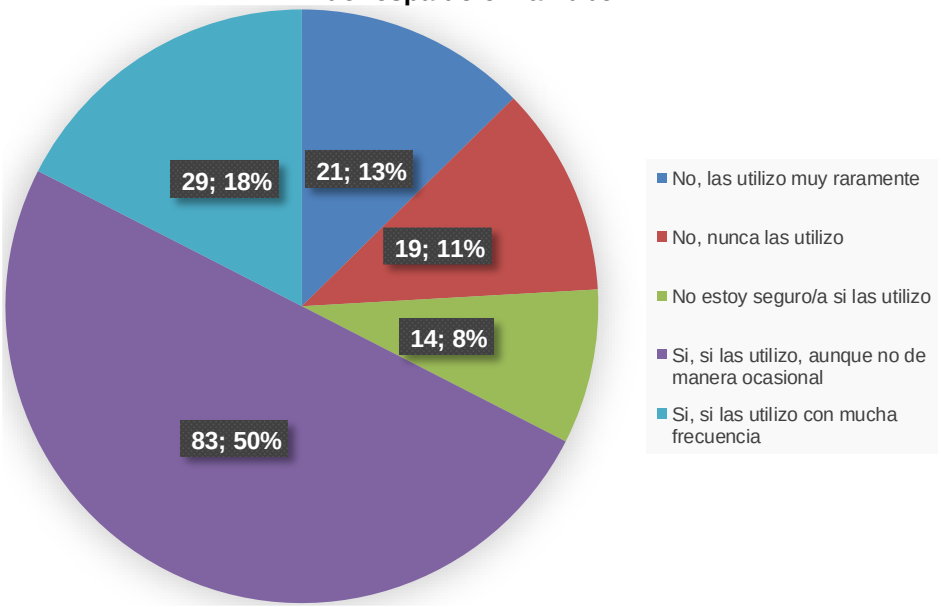
poco control para gestionarlas, el 16% nunca lleva un control para gestionarlas, el 13% no está segura si lleva un control para gestionarlas y el 12% si lleva un control muy organizado para gestionarlas.

Tanto el 38% como el 21% en el sector de los encuestados dicen llevar algo o muy poco control para gestionar sus contraseñas, lo cual se puede interpretar como un tema de poca importancia para los usuarios o porque utilizan una única clave o contraseña para la mayoría de los accesos.

5.1.6 MÉTODOS DE RECUPERACIÓN EFECTIVOS

En el Gráfico 6, se presenta la opinión del grupo encuestado acerca de la pregunta sobre los métodos de recuperación efectivos.

Gráfico 6: ¿Utiliza alguna de estas opciones como copia de seguridad en caso de perder su información personal o de tercero? Discos extraíbles, Memorias USB, sistema de respaldo en la nube



Fuente: El autor

En el Gráfico 6 el 50% de los estudiantes encuestados respondió que utiliza, aunque no de manera ocasional herramientas de respaldo de datos como Discos

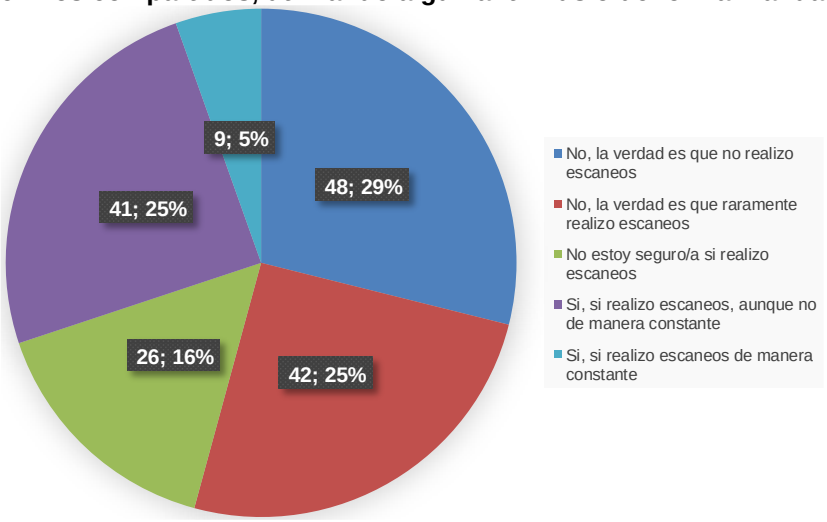
extraíbles, USB, sistemas en la nube, el 18% las utiliza con mucha frecuencia, el 13% las utiliza muy raramente, el 11% nunca las utiliza y el 8% no está seguro/a si las utiliza.

Utilizar herramientas de respaldo de datos debería ser una práctica diaria o por lo menos cuando se realicen modificaciones en los documentos personales o de terceros, ya que no se sabe con exactitud cuando se pueden dar por hecho hurtos digitales o perdidas de información, tal como se evidencia el 50% de los encuestados, el cual utiliza diferentes herramientas de respaldo.

5.1.7 SUPERVISIÓN DE INFORMACIÓN MEDIANTE APLICACIONES

En el Gráfico 7, se presenta la opinión del grupo encuestado acerca de la pregunta en cuanto a supervisión de información mediante aplicaciones.

Gráfico 7: ¿Realiza escaneos constantes de sus correos electrónicos, aplicaciones o archivos compartidos, utilizando algún antivirus o de forma manual?



Fuente: El autor

En el Gráfico 7 se observa que el 29% de la población estudiantes encuestada afirma no realizar escaneos de sus correos electrónicos, aplicaciones o archivos

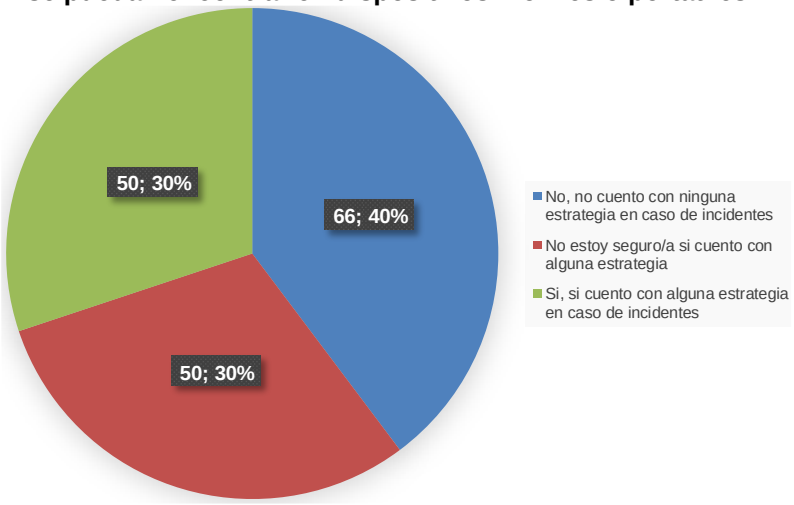
compartidos, utilizando algún antivirus o de forma manual, un 25% dice raramente realizar escaneos y el otro 25% los realizar, aunque no de manera constante, el 16% no está seguro/a si realizar escaneos y el 5% si realiza escaneos de forma constante.

Resulta crítico que la población encuestada no supervise sus correos electrónicos, archivos o aplicaciones compartidos. Ante esta situación es de carácter verídico que los escaneos deben ser en su total mayoría constantes ya que se pueden encontrar en cualquier momento en las bandejas de entradas o al realizar un mal procedimiento mientras se editan archivos personales o de terceros.

5.1.8 IDEAS PARA SALVAGUARDAR DATOS PERSONALES

En el Gráfico 8, se presenta la opinión del grupo encuestado acerca de la pregunta de ideas para salvaguardar datos personales.

Gráfico 8: ¿Cuenta usted con alguna estrategia para posibles incidentes que amenacen el estado de su privacidad o la seguridad de sus documentos personales que se puedan encontrar en dispositivos móviles o portátiles?



Fuente: El autor

En el Gráfico 8 la población presentó un 40% de estudiantes que afirmaron no contar con ninguna estrategia en caso de incidentes que amenacen el estado de

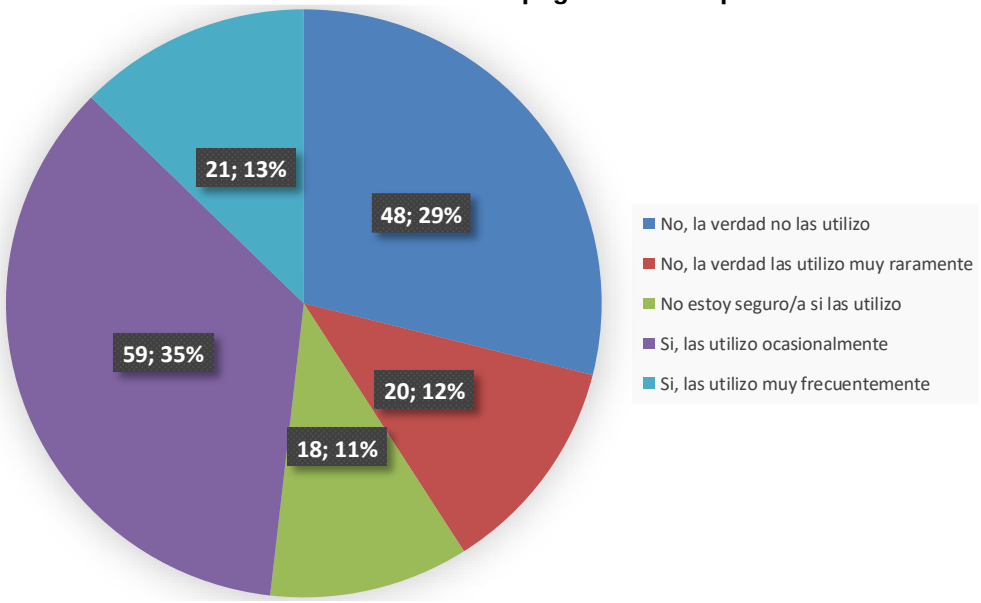
su privacidad o la seguridad de sus documentos personales, un 30% dijo no estar seguro/a si cuentan con alguna estrategia y el otro 30% dijo si contar con alguna estrategia.

Los porcentajes para esta pregunta están divididos en cantidades similares, exceptuando el 40% que contestó no tener ninguna estrategia, lo cual deja en claro que, ante cualquier tipo de amenaza, sea menor o mayor no están preparados categóricamente para afrontar perdidas de documentación, por ejemplo.

5.1.9 SOFTWARE DE APOYO CONTRA WEBS MALICIOSAS

En el Gráfico 9, se presenta la opinión del grupo encuestado acerca de la pregunta de software de apoyo contra webs maliciosas.

Gráfico 9: ¿Utiliza aplicaciones o extensiones en navegadores que le faciliten saber si está intentando acceder a una página web sospechosa?



Fuente: El autor

El Gráfico 9 evidencia que el 35% utiliza ocasionalmente aplicaciones o extensiones en navegadores que le faciliten saber si está intentando acceder a

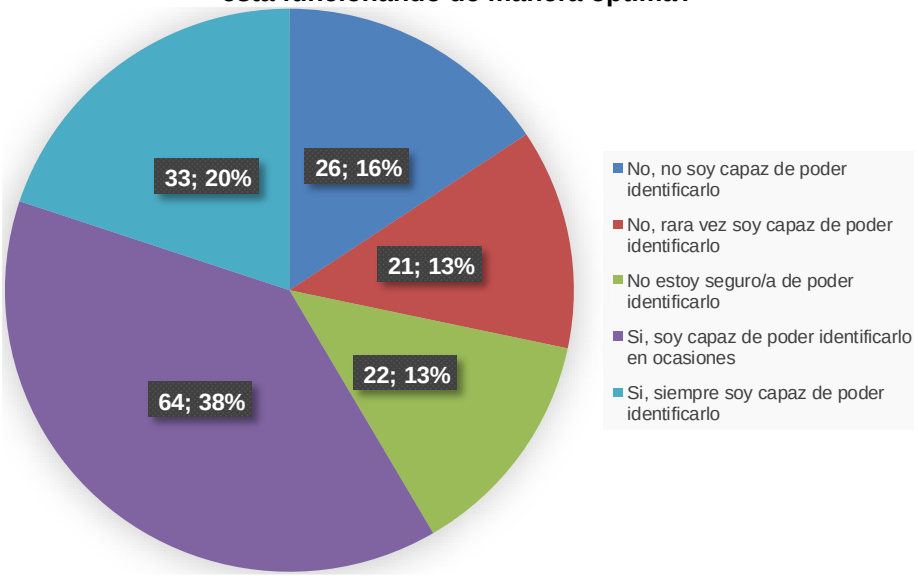
una página web sospechosa, el 29% no las utiliza, el 13% las utiliza muy frecuentemente, el 12% las utiliza muy raramente y el 11% no está seguro/a si las utiliza.

Aunque el 35% afirma utilizar herramientas ocasionalmente cuando se está accediendo a sitios webs sospechosos, el 29% dice que no las utiliza y resulta ser una problemática a tener en cuenta ya que acceder a una web bajo un posible software malicioso compromete al equipo informático a que resulte infectado.

5.1.10 IDENTIFICACIÓN DE MALFUNCIONAMIENTO EN SISTEMAS

En el Gráfico 10, se presenta la opinión del grupo encuestado acerca de la pregunta sobre la identificación de malfuncionamiento en sistemas.

Gráfico 10: ¿Es usted capaz de identificar cuando su dispositivo móvil o portátil no está funcionando de manera óptima?



Fuente: El autor

El Gráfico 10 muestra que el 38% de los encuestados dicen ser capaz de poder identificar en ocasiones cuando su dispositivo móvil o portátil no está funcionando

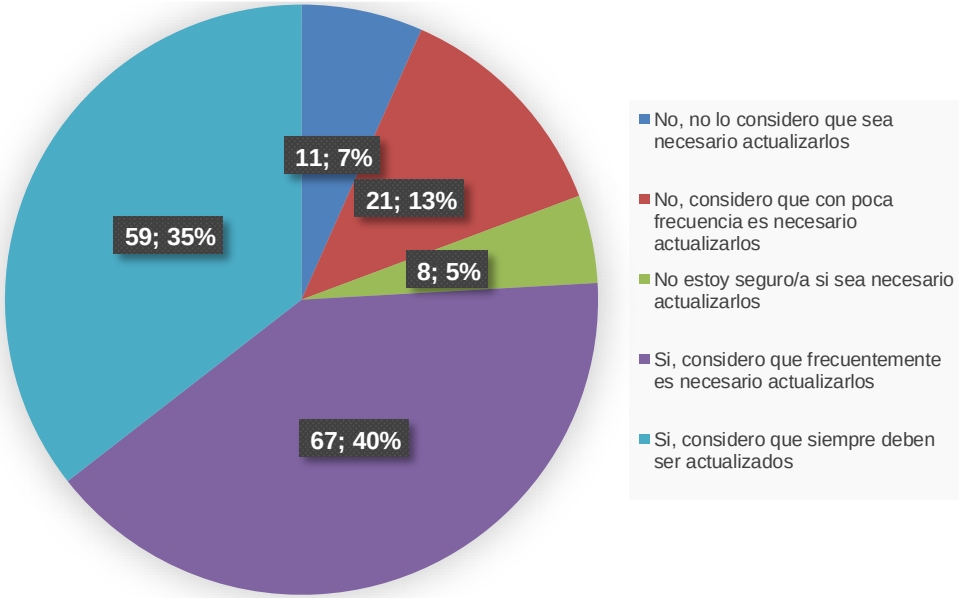
de manera óptima, el 20% siempre es capaz de poder identificarlo, el 16% no es capaz de poder identificarlo, el 13% rara vez es capaz de poder identificarlo y el otro 13% no está seguro/a de poder identificarlo.

Identificar una amenaza conlleva a una detección temprana de malware que además atente contra la seguridad de los dispositivos móviles y portátiles, aunque preferiblemente esta práctica deba hacerse más que de manera ocasional. Lo cierto es que el 38% de los encuestados están conscientes de cuando su dispositivo se comporta de manera sospechosa.

5.1.11 ACTUALIZACIÓN DE SOFTWARE

En el Gráfico 11, se presenta la opinión del grupo encuestado acerca de la pregunta de actualización de software.

Gráfico 11: ¿Considera usted que los sistemas operativos y aplicaciones necesariamente deben estar actualizados a su última versión?



Fuente: El autor

En el Gráfico 11 el 40% de los estudiantes encuestados contestó que frecuentemente es necesarios que los sistemas operativos y aplicaciones

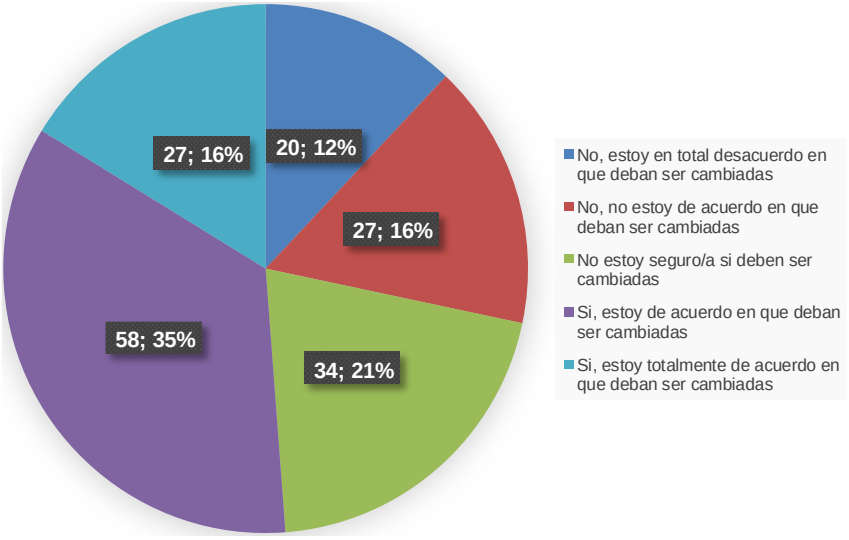
necesariamente deben estar actualizados a su última versión, el 35% considera que siempre de ser actualizados, el 13% considera que con poca frecuencia deben ser actualizados, el 7% no lo considera que deba ser necesario actualizarlos y el 5% no está seguro/a si deben ser actualizados.

El 40% y el 35% de los estudiantes que respondieron ante la necesidad de actualizar los sistemas operativos y aplicaciones, entienden que es importante reforzar la seguridad de la misma debido a que constantemente los delincuentes informáticos andan al asecho esperando alguna vulnerabilidad para de este acceder a la información que deseen.

5.1.12 GESTIÓN DE CONTRASEÑAS

En el Gráfico 12, se presenta la opinión del grupo encuestado acerca de la pregunta sobre gestión de contraseñas.

Gráfico 12: ¿Qué tan de acuerdo está usted en que las contraseñas deberían ser cambiadas cada 90 días?



Fuente: El autor

El Gráfico 12 muestra que el 35% de la población contestó estar de acuerdo con que las contraseñas deban ser cambiadas cada 90 días, el 21% no está seguro si

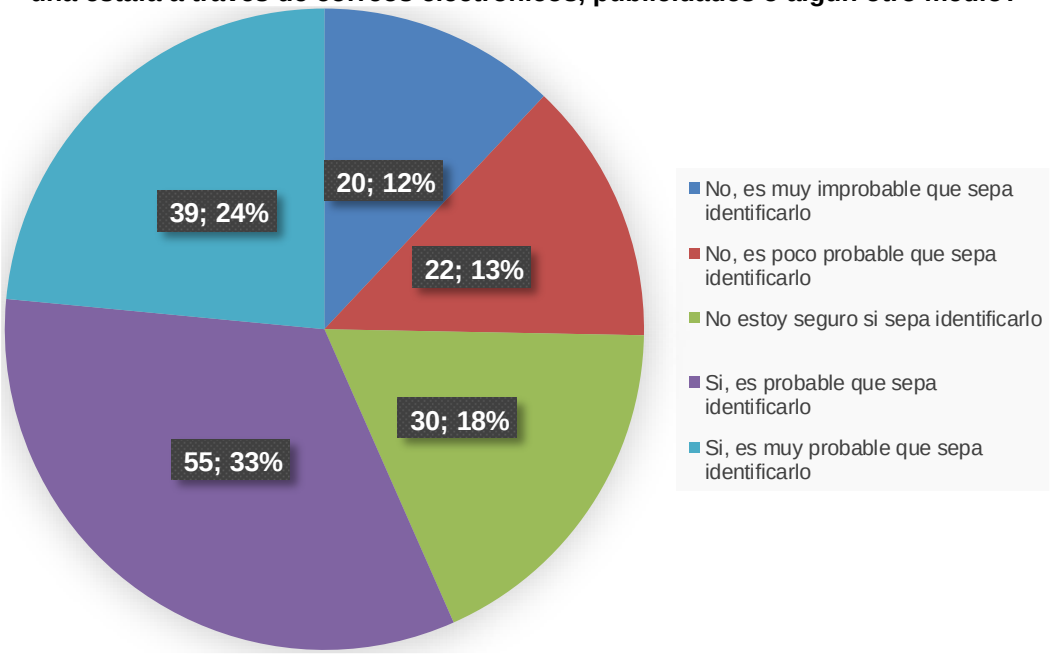
deban ser cambiadas, el 16% está totalmente de acuerdo que deban ser cambiadas, otro 16% no está de acuerdo que deban ser cambiadas y el 12% está en total desacuerdo que deban ser cambiadas.

Las contraseñas necesitan ser modificadas, ya que para los delincuentes informáticos resulta ser más sencillo hurtar datos si no se realizan dichos cambios. Y resulta totalmente entendible por parte de los encuestados.

5.1.13 RAZONAMIENTO ANTE ATAQUES POTENCIALES

En el Gráfico 13, se presenta la opinión del grupo encuestado acerca de la pregunta de razonamiento ante ataques potenciales.

Gráfico 13: ¿Qué tan probable es que sepa identificar cuando está siendo tentado a una estafa a través de correos electrónicos, publicidades o algún otro medio?



Fuente: El autor

El Gráfico 13 muestra que el 33% de los encuestados dijeron que es probable que sepan identificar cuando están siendo tentado a una estafa a través de correos electrónicos, publicidades o algún otro medio, el 24% dijo que es muy probable

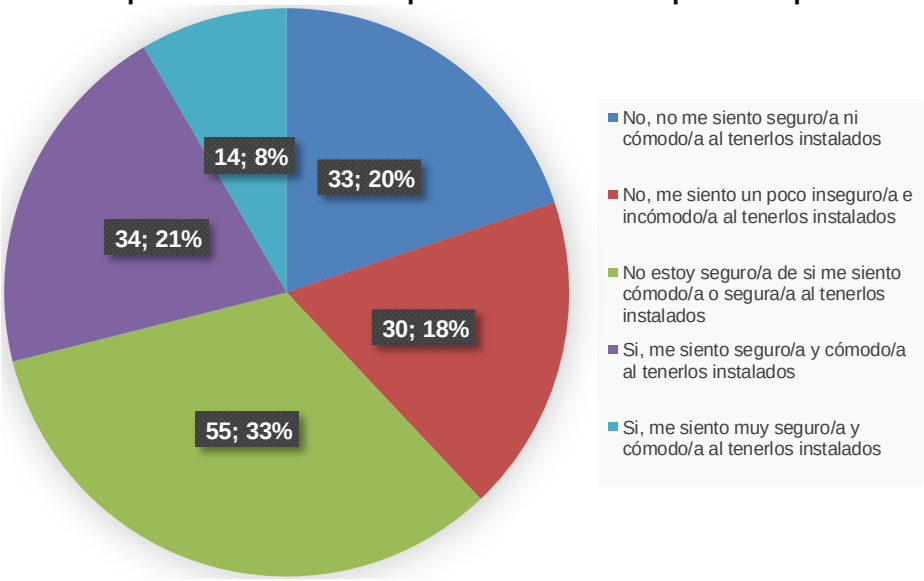
que sepan identificarlo, el 18% no está seguro/a, el 13% dijo que es poco probable que sepa identificarlo y el 12% dijo que es muy improbable que sepa identificarlo.

Las estafas son diariamente rondando internet y es esencial identificar una amenaza como las que fueron mencionadas, por lo tanto, resulta positivo que el 24% de los encuestados ya que en teoría están conscientes de cuando una actividad cibernética resulta ser sospechosa.

5.1.14 COMODIDAD ANTE SOFTWARE DE DUDOSA PROCEDENCIA

En el Gráfico 14, se presenta la opinión del grupo encuestado acerca de la pregunta sobre comodidad ante software sospechoso.

Gráfico 14: ¿Qué tan seguro y cómodo se siente al tener instalado aplicaciones de dudosa procedencia en su dispositivo móvil o computadora portátil?



Fuente: El autor

En el Gráfico 14, el 33% de la población encuestada respondió que no está seguro/a ni cómodo/a al tener instalado aplicaciones de dudosa procedencia en su dispositivo móvil o computadora portátil, el 21% se siente seguro/a y cómodo/a,

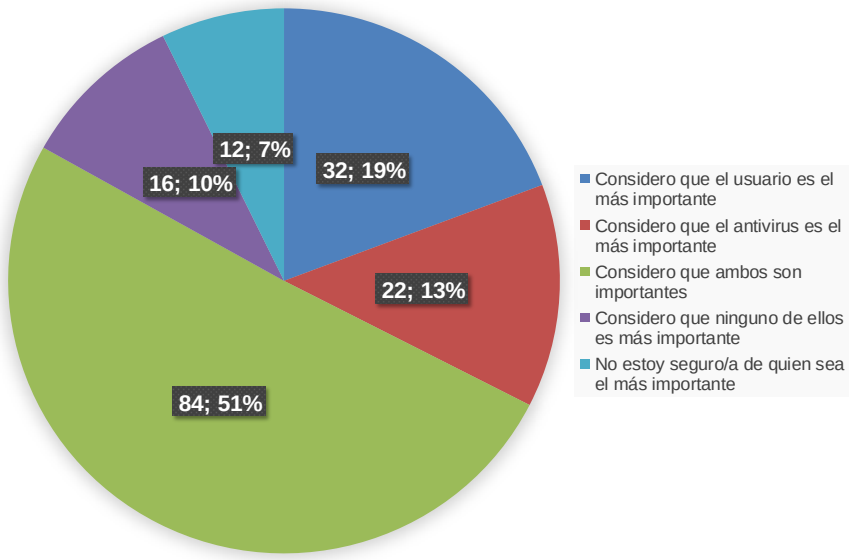
el 20% no se siente seguro/a ni cómodo/a, el 18% se siente un poco inseguro/a e incómodo/a y el 8% no se siente seguro/a ni cómodo/a.

Las aplicaciones de dudosa procedencia son una problemática para los dispositivos móviles y portátiles, no por el contenido que brindan sino por lo que esconden detrás de ellos, afectando el rendimiento de los dispositivos y a la vez hurtando datos de mayor importancia. Para el 33% de los encuestados es entendible el debate, sin embargo, existe un 21% que piensa lo contrario y resulta ser una situación preocupante.

5.1.15 RESPONSABLE PRINCIPAL ANTE SOFTWARE MALICIOSO

En el Gráfico 15, se presenta la opinión del grupo encuestado acerca de la pregunta sobre el responsable principal ante software malicioso.

Gráfico 15: ¿Quién considera que es más importante para mantener en buen estado la seguridad de los dispositivos móviles o computadoras portátiles, el usuario, antivirus o ambos?



Fuente: El autor

El Gráfico 15 se observa que la pregunta sobre quién considera que es más importante para mantener en buen estado la seguridad de los dispositivos móviles o computadoras portátiles, el usuario, antivirus o ambos, el 51% respondió que ambos son importantes, el 19% considera al usuario más importantes, el 13% considera al antivirus más importante, el 10% considera que ninguno de ellos es más importante y el 7% no está seguro/a de quien sea más importante.

Dejarle la total responsabilidad al antivirus para proteger los dispositivos móviles o portátiles no es una tarea que sea efectiva totalmente, ya que se encuentran malware que trabajan de manera silenciosa y desapercibidas, tanto que el antivirus no es capaz de detectarlo, por ende, entra la responsabilidad del usuario ya que conoce como funciona su dispositivo y las consecuencias de un mal funcionamiento. Es por eso que tanto el usuario como el antivirus realizan un trabajo en equipo para salvaguardar la información esencial, tal como lo señala el 51%. De los encuestados el cual es aceptable.

5.2 RESULTADOS GLOBALES

Al finalizar, de forma integral los resultados principales, bajo la perspectiva provenientes de los apartados 4.10.2 se construye la siguiente tabla, el cual refleja el promedio total del nivel de conocimientos en políticas que tienen los estudiantes del FIEC-CRUV en cuanto a ciberseguridad se refiere, en base a respuestas al menos satisfactorias.

Tabla 11: Resultados principales globales

#	Indicadores	Peso relativo	Respuestas al menos Satisfactorias	Porcentaje relativo	Nivel de conocimiento
1	Políticas de Seguridad Informática	6.66%	123	74.10%	Alto
2	Exposición de información personal en Internet	6.66%	122	73.49%	Alto
3	Terminología básica de ciberseguridad	6.66%	118	71.08%	Alto
4	Conocimientos formales de seguridad informática	6.66%	88	53.01%	Satisfactorio
5	Control de claves de acceso	6.66%	110	66.27%	Alto
6	Métodos de recuperación efectivos	6.66%	126	75.90%	Alto
7	Supervisión de información mediante aplicaciones	6.66%	76	45.78%	Satisfactorio
8	Ideas para salvaguardar datos personales	6.66%	100	60.24%	Alto
9	Software de apoyo contra webs maliciosas.	6.66%	98	59.04%	Satisfactorio
10	Identificación de malfuncionamiento en sistemas	6.66%	119	71.69%	Alto
11	Actualización de software	6.66%	134	80.72%	Muy Alto
12	Gestión de contraseñas	6.66%	119	71.69%	Alto
13	Razonamiento ante ataques potenciales	6.66%	124	74.70%	Alto
14	Comodidad ante software de dudosa procedencia	6.66%	103	62.05%	Alto
15	Responsable principal ante software malicioso	6.66%	112	67.47%	Alto
	Promedio			**67.15%**	**Alto**

Fuente: El Autor

En conclusión, se aprecia en cada grafico mostrado que para los estudiantes de la CRUV-FIEC, el nivel de conocimiento en cuanto a políticas de seguridad informática para contrarrestar el malware en los dispositivos móviles y portátiles, según la matriz de ponderación ubicada en la Tabla 12 es ***alto***, lo que implica que no tienen dificultades significativas al afrontar diferentes escenarios para contrarrestar amenazas informáticas. Esta afirmación **aclara** la pregunta de investigación anteriormente planteada en el apartado que desarrolla la definición del problema, sección 3.1.

Como resultado complementario del trabajo de investigación se confirma la veracidad de la hipótesis alterna H_i planteada en la sección 4.4, así como en la sección 4.9.1, ya que el nivel de conocimiento NC reflejado en los resultados obtenidos supera el nivel mínimo preestablecido del 60%.

Finalmente, en función al modelo de evaluación planteado en la sección 4.10, así como en los resultados obtenidos en la sección 5.2, se establece que la población objeto de estudio en esta investigación alcanzó un nivel **alto** en cuanto a su conocimiento en políticas de seguridad informática en dispositivos móviles y portátiles.

Por lo tanto, no se identifica un problema significativo de conocimiento en cuestiones de seguridad informática, que justifique algún tipo de propuesta de capacitación académica en la temática antes mencionada, tal como se tenía previsto en los objetivos específicos de esta investigación, sección 3.2.2.

6. CONTRIBUCIONES, LIMITACIONES Y PROYECCIONES FUTURAS

En el siguiente capítulo, se empezará por mostrar los resultados obtenidos durante la elaboración de la investigación, los temas que se puedan abordar o continuar de ello, así como también aquellas limitaciones que se encontraron conforme se avanzaba en la elaboración de este proyecto.

6.1 APORTES CONCRETADOS

En función de la elaboración del proyecto de investigación, se enlistan los aportes que se concretaron.

6.1.1 POLÍTICAS DE CIBERSEGURIDAD PERSONAL COMPENDIADAS

En función a los criterios planteados en la sección 2.3, se enuncian las políticas generales de ciberseguridad que se recomienda que sigan los usuarios personales de dispositivos móviles y portátiles.

- Administrar las contraseñas de usuario de acuerdo al **modelo de gestión de contraseñas**, planteado en la sección 2.3.1.1.

- Implementar hasta donde sea posible la autenticación multifactorial de los usuarios (sección 2.3.1.2).

- Administrar los respaldos en la nube de acuerdo a los criterios expuestos en la sección 2.3.1.3.

- Actuar con precaución al momento de abrir correos electrónicos, portales web, así como archivos descargados o adjuntos a correos electrónicos (sección 2.3.1.4).

- Únicamente mantener instaladas las aplicaciones que se utilizan regularmente. Aquellas que se emplean ocasionalmente, se instalarán, se utilizarán y se desinstalarán en el momento de su empleo (sección 2.3.1.5).

- Evadir el uso de aplicaciones de terceros que se dedican a recolectar datos personales a través de redes sociales (sección 2.3.1.6).

- Evitar ser víctima de tentativas de estafas económicas que se encuentran en las redes sociales, tales como compra de acciones o inversiones (sección 2.3.1.7).

- Actuar con cautela al momento de realizar compras virtuales con tarjetas bancarias o cualquier otro método de compra por medio de Internet, para minimizar el hurto de credenciales (sección 2.3.1.8).

- Desconfiar de solicitudes de información personal de forma remota. De ser posible, confirmar con las personas, instituciones u organizaciones las peticiones de datos personales sensibles (sección 2.3.1.9).

- Evitar el uso de software ilegal o de dudosa procedencia en los dispositivos móviles y portátiles (sección 2.3.1.10).

6.1.2 NIVEL DE CONOCIMIENTO EN POLÍTICAS DE CIBERSEGURIDAD PARA CONTRARRESTAR EL MALWARE

Tal como se describe en el apartado 3.1 el usuario promedio afronta una serie de obstáculos que le dificultan de cierta manera navegar de forma segura a través de la Internet.

No obstante, se identificó que la población objeto de estudio, presenta un nivel de conocimiento alto en cuanto a políticas de seguridad para contrarrestar el malware en dispositivos móviles y portátiles. Esta información se estableció mediante la interpretación de los datos recabados en la encuesta aplicada y que se aprecia en cada gráfico mostrado a partir de la sección 5.1. Es decir, que no muestran dificultades notorias al momento de localizar o confrontar cualquier tipo de amenaza informática.

6.2 LIMITANTES RELEVANTES DENTRO DEL ESTUDIO

La elaboración de la encuesta de la investigación contó con un total de 166 encuestados, resultando ser una cifra aproximada de la población Universitaria matriculada en la FIEC-CRUV (ver Figura 3). En consecuencia, se excluyeron 22 estudiantes (13.25%), por diferentes razones, entre las que resaltan:

- Algunos no quisieron ser encuestados,
- Otros se habían retirado de la Facultad o de la Universidad,
- Finalmente, ciertos individuos no estaban presentes en las aulas al momento de aplicar la encuesta

Por lo antes planteado, se tiene que aceptar que los resultados obtenidos involucran un nivel de error de al menos un 13%.

6.3 PROYECTOS DERIVADOS DE ESTA INVESTIGACIÓN

Al concluir esta investigación, se pueden inferir algunos proyectos derivados de la misma, entre los que se destacan:

- Establecer el nivel de conocimiento en políticas de seguridad informática entre estudiantes pertenecientes a otras facultades del CRUV, fuera de la FIEC.

- Establecer el nivel de conocimiento en políticas de seguridad informática entre estudiantes pertenecientes a otras universidades, dentro de la provincia de Veraguas, diferentes de la Universidad de Panamá.

- Elaborar con criterios más estrictos, políticas de seguridad especializadas para poblaciones de diversas formaciones profesionales tales como: diseñadores gráficos, educadores, abogados, especialistas en ciencias administrativas y profesionales de la ciencia de la salud, entre otros casos.

- Modelar un conjunto de políticas de seguridad básicas que deberían implementar los usuarios de sistemas operativos y aplicaciones no informáticos, a fin de minimizar los niveles de riesgo a los que se expone su información personal.

7. CONCLUSIONES

Al término de este proyecto de investigación, se plantean las conclusiones que se enuncian a continuación.

- El empleo de la tecnología se ha convertido en parte del diario vivir de las personas, involucrando el empleo sistemático de sus datos personales, académicos o laborales. Al mismo tiempo, la delincuencia informática se ha incrementado a tal grado de generar preocupación e inseguridad de los usuarios en los últimos años.

- La seguridad informática no afecta únicamente el ámbito empresarial, sino también los datos personales de los usuarios, con el fin de obtener y hurtar tanto dinero como credenciales digitales, a través de aplicaciones y técnicas como el ransomware y phishing, entre otros casos.

- La investigación dedujo estadísticamente que la población objeto de estudio no muestra debilidades significativas en cuanto a su conocimiento sobre seguridad informática. Disponen de conocimiento en temáticas como, por ejemplo: la terminología de nombres de los programas maliciosos más comunes, los métodos de recuperación de datos extraviados, control y gestión de contraseñas y razonamiento ante tentativas de ataques informáticos.

- Ante los resultados previamente obtenidos en la sección 5.2, no se identificaron dificultades relevantes en cuanto a seguridad informática que justifiquen la realización del objetivo específico propuesto en la sección 3.2.2, relacionado con el diseño de una propuesta didáctica como alternativa de solución ante los niveles bajos de conocimiento en ciberseguridad, orientado a los estudiantes de la FIEC-CRUV.

8. RECOMENDACIONES

- Pese a que se obtuvo un porcentaje positivo significativo en cuanto al nivel de conocimiento en seguridad informática; se aconseja a los estudiantes de la FIEC-CRUV que deben continuar reforzando su conocimiento en temas de ciberseguridad mediante el estudio de distintos medios digitales como lo son: investigaciones, publicaciones, libros o conferencias, entre otros casos, ya que las amenazas a la seguridad de la información evolucionan con el constante avance tecnológico.

- Se recomienda la ejecución de investigaciones complementarias a la previamente realizada, enfocadas en otras poblaciones, tales como:

  - ✓ Otras facultades de la Universidad de Panamá, así como en su personal docente y administrativo,

  - ✓ Otras universidades que se encuentran en la ciudad de Santiago, o a nivel nacional.

Las mismas permitirán ampliar el conocimiento de las distintas poblaciones investigadas y, de ser necesario, plantear programas de capacitaciones en ciberseguridad, en los casos que sea necesario.

9. REFERENCIAS BIBLIOGRÁFICAS

Agresti, A., Franklin, C., & Klingenberg, B. (2023). *Statistics: The Art and Science of Learning from Data* (Fifth ed.). Harlow, United Kingdom: Pearson Education.

Baiaragi, V., & Munot, M. (2019). *Research methodology: a practical and scientific approach* (First ed.). New York, United States of America: CRC Press.

Belous, A., & Saladukha, V. (2020). *Viruses, Hardware and Software Trojans: Attacks and Countermeasures (First Ed).* Cham, Switzerland: Springer.

Bhooshan Gupta, B. (2022). *Advances in Malware and Data-Driven Network Security* (First ed.). Hershey, United States of America: IGI Global.

Brace, I., & Bolton, K. (2022). *Questionnaire Design: How to plan, structure and write survey material for effective market research* (Fifth ed.). London: Kogan Page.

Cabrera, C. Y. (junio de 2015). Incidencia del uso del internet en los adolecentes de las instituciones de educación media. *8*(14), 57-66. Recuperado el 19 de octubre de 2022, de https://www.redalyc.org/pdf/5826/582663828008.pdf

Collier, N. (2021, febrary 12). *Barcode Scanner app on Google Play infects 10 million users with one update*. Retrieved 09 13, 2023, from Malwarebytes Labs: https://www.malwarebytes.com/blog/news/2021/02/barcode-scanner-app-on-google-play-infects-10-million-users-with-one-update

Coolican, H. (2024). *Research Methods and Statistics in* (Eighth ed.). New York: Routledge.

Cumming, G., & Calin-Jagemen, R. (2024). *Introduction to the new statistics: estimation, open science, and beyond* (Second ed.). New York: Routledge.

Dascalescu, A. (2020, december 2). *The 12+ Internet Crime Stories That Make Cybersecurity Measures Essential*. Retrieved october 1, 2022, from Heimdal Security: https://heimdalsecurity.com/blog/12-true-stories-that-will-make-you-care-about-cyber-security/

Eolas. (2021, august). *Garda National Cyber Crime Bureau: "Most crime has a digital footprint"*. Retrieved september 22, 2023, from https://www.eolasmagazine.ie: https://www.eolasmagazine.ie/garda-national-cyber-crime-bureau-most-crime-has-a-digital-footprint/

European Commission. (2021). *European Commission*. Retrieved 09 20, 2023, from https://home-affairs.ec.europa.eu: https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

Federal Trade Commission. (2022, september). *https://consumer.ftc.gov*. Retrieved from How to Recognize and Avoid Phishing Scams: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Goutam, R. K. (2021). *Cybersecurity Fundamentals, Understand the Role of Cybersecurity: Its Importance and Modern Techniques Used by Cybersecurity Professionals* (First ed.). Delhi, India: BPB Publications.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(01), 49-58. doi:https://doi.org/10.1093/cybsec/tyw018

Guapacha, J. (11 de agosto de 2017). *Diseño de diplomado virtual en principios de seguridad informática.* Universidad Libre, Maestría en Educación con énfasis en Informática Educativa, Bogotá. Recuperado el 29 de septiembre de 2022, de Universidad Libre: https://repository.unilibre.edu.co/handle/10901/10553

Hernández Sampieri, R., Mendoza Torres, P., Méndez Valencia, S., & Cuevas Romo, A. (2019). *Metodología de la investigación para bachillerato (Segunda Ed.)* (Segunda ed.). Ciudad de México: McGraw-Hill.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (Primera ed.). Ciudad de México: McGraw-Hill.

Interpol. (2024). *Piratería Digital*. Recuperado el 14 de enero de 2024, de https://www.interpol.int/es: https://www.interpol.int/es/Delitos/Productos-ilegales/Compre-de-forma-segura/Pirateria-digital#:~:text=La%20pirater%C3%ADa%20digital%20consiste%20en,la%20m%C3%BAsica%20y%20el%20juego.

ISO. (2022). *ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls.* Genova: ISO copyright office.

Kleymenov, A., & Thabet, A. (2022). *Mastering Malware Analysis: A malware analyst's practical guide to combating malicious software, APT, cybercrime, and IoT attacks (First Ed.)* (Second ed.). Birmingham, United Kingdom: Packt.

Krebs, B. (2023, august 4). *Teach a Man to Phish and He's Set for Life*. Retrieved september 25, 2023, from KrebsonSecurity: https://krebsonsecurity.com/2023/08/teach-a-man-to-phish-and-hes-set-for-life/

Kriscautzky, M., & Ferreiro, E. (2014). La Confiabilidad De La Información En Internet: Criterios Declarados Y Utilizados Por Jóvenes Estudiantes Mexicanos. *SciELO, 40*(4), 913-934. doi:https://doi.org/10.1590/s1517-97022014121511

Kumar, G., Saini, D., & Cuong, N. (2021). *Cyber Defense Mechanisms: Security, Privacy, and Challenges* (First ed.). Boca Raton, United States of America: CRC Press.

Lizano Mora, H. (5 de mayo de 2022). *Voz experta: Taxonomía del malware, el caso Ransomware Conti*. Recuperado el 1 de octubre de 2022, de Universidad de Costa Rica: https://www.ucr.ac.cr/noticias/2022/05/05/voz-experta-taxonomia-del-malware-el-caso-ransomware-conti.html

Lukings, M., & Habibi Lashkari, A. (2022). *Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective* (First ed.). Cham, Switzerland: Springer.

Malwarebytes. (2022). *Malwarebytes*. Recuperado el 1 de octubre de 2022, de https://es.malwarebytes.com/malware/

Markley, K. (2023, april 25). *Data Recovery Pitfalls to Avoid*. Retrieved september 25, 2023, from ISACA: https://www.isaca.org/resources/news-and-trends/industry-news/2023/data-recovery-pitfalls-to-avoid

Martin, A. (31 de marzo de 2015). *welivesecurity*. Recuperado el 1 de octubre de 2022, de https://www.welivesecurity.com/la-es/2015/03/31/6-formas-backup-informacion/

Martínez, N., & Martínez, R. (3 de diciembre de 2018). Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. *RECAI, 7*(20), 23. Recuperado el 4 de abril de 2023, de https://www.redalyc.org/journal/6379/637968308002/

Mbanaso, U. M., Abrahams, L., & Chinedu Okafor, K. (2023). *Research Techniques for Computer Science, Information Systems and Cybersecurity* (First ed.). Cham: Springer.

Méndez, M. (mayo-agosto de 2018). Enfrentando los ransomwares. *Telemática, 17*(2), 36-41. Recuperado el 24 de octubre de 2022, de https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/301/277

Merino, M. (7 de noviembre de 2023). *Instagram Wrapped 2023 promete revelar quién revisa tu perfil. Pero es una estafa que se inventa datos (mientras accede a los tuyos)*. Recuperado el 3 de enero de 2024, de www.genbeta.com: https://www.genbeta.com/actualidad/intagram-wrapped-2023-promete-revelar-quien-revisa-tu-perfil-estafa-que-se-inventa-datos-accede-a-tuyos

Montero Salinas, J. (2021). *Manejo virtual en tiempos de pandemia, relacionado a las competencias personales, estuiantes, Escuela Cerro Algodón.* Tesis, Universidad Especializada de,las Américas, Facultad de Educación Especial y Pedagogia, Santiago. Recuperado el 15 de junio de 2023, de http://repositorio2.udelas.ac.pa/bitstream/handle/123456789/1001/Montero_Salinas_Jos%c3%a9_Manuel.pdf?sequence=1&isAllowed=y

Muncaster, P. (15 de marzo de 2023). *5 razones para mantener tu software y dispositivos actualizados*. Obtenido de https://www.welivesecurity.com/: https://www.welivesecurity.com/la-es/2023/03/15/razones-mantener-software-dispositivos-actualizados/

National Cybersecurity Alliance. (2022, may 26). *https://staysafeonline.org/*. Retrieved from Passwords: https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/

Pizarro, H. (29 de abril de 2016). *Cylance realiza la primera presentación mundial de neutralización de ransomware en tiempo real*. Recuperado el 29 de septiembre de 2022, de Diario TI: https://diarioti.com/cylance-realiza-la-primera-presentacion-mundial-de-neutralizacion-de-ransomware-en-tiempo-real/97458

Rains, T. (2023). *Cybersecurity Threats, Malware Trends And Strategies. (Second Ed.)* (Second ed.). Birmingham, United Kingdom: Packt.

Ramos Gómez, J. S. (2019). *Ambiente simulado con malware para entrenamiento de usuarios regulares.* Tesis, Ingeniería de Sistemas y Computación, Bogotá.

Redacción de TVN Noticias. (18 de Octubre de 2023). *Desmantelan red de estafadores, vendían paquetes vacacionales*. Recuperado el 27 de Diciembre de 2023, de https://www.tvn-2.com: https://www.tvn-2.com/nacionales/desmantelan-red-estafadores-vendian-paquetes_1_2085750.html

Roa Buendía, J. (2013). *Seguridad Informática* (Primera ed.). Madrid, España: McGraw-Hill.

Rodríguez C, O., Dutari D, R., Rodríguez F, D., Fernández G, L., Díaz R, K., Quintero P, J., & Chang M, H. (mayo de 2022). Percepción de la ciberseguridad: ciberlitos, normas legales y políticas de seguridad. *6*(2), 20. Recuperado el 29 de abril de 2023, de https://matriculapre.up.ac.pa/index.php/antataura/article/view/3387

Roman, V. (3 de mayo de 2024). *Estafadores ya están usando deepfakes en tiempo real*. Recuperado el 9 de mayo de 2024, de https://www.robotitus.com: https://www.robotitus.com/estafadores-ya-estan-usando-deepfakes-en-tiempo-real#:~:text=Un%20reciente%20informe%20de%20WIRED,para%20ejecutar%20estafas%20de%20romance.

Saeed, S., Almuhaideb, A., & Others. (2023). *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (First ed.). Hershey: IGI Global.

Sanchez, J., & Montoya, L. (2017). La confianza como elemento fundamental en las compras a través de canales de comercio electrónico. Caso de los consumidores en Antioquia (Colombia). *Innovar, 27*(64), 11-22. doi:https://doi.org/10.15446/innovar.v27n64.62365

Santos, O. (2019). *Developing Cybersecurity Programs and Policies* (First ed.). London, United Kingdom: Pearson Education.

Secretaría Académica, CRUV. (2025). *Población estudiantil de la Facultad de Informática, Electrónica y Comunicación del CRUV.* Nota Informátiva, Universidad de Panamá, Centro Regional Universitario de Veraguas.

Shishkova, T. (18 de agosto de 2022). *Evolución de las ciberamenazas en el segundo trimestre de 2022*. Recuperado el 3 de noviembre de 2022, de Securelist by Kaspersky: https://securelist.lat/it-threat-evolution-in-q2-2022-mobile-statistics/96970/

Smith, L. (2022). *Cyber Security For Beginners: a comprehensive and essential guide for every novice to understand and master cybersecurity* (First ed.). Seattle, United States of America: CreateSpace Independent Publishing Platform.

Sophos Ltd. (27 de abril de 2021). *El estado del ransomware 2021.* SOPHOS Cybersecurity evolved. Recuperado el 1 de octubre de 2022, de https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

Stallings, W., & Browm, L. (2018). *Computer security: principles and practice* (Fourth ed.). New York, United States of America: Pearson Education.

Stefanko, L. (06 de abril de 2022). *Falsas tiendas online roban credenciales bancarias utilizando malware para Android*. Recuperado el 3 de enero de 2024, de welivesecurity by ESET: https://www.welivesecurity.com/la-es/2022/04/06/falsas-tiendas-online-roban-credenciales-bancarias-malware-android/

Stufflebeam, D. L., & Coryn, L. S. (2014). *Evaluation theory, models, and applications* (Second ed.). San Francisco, United States of America: Jossey-Bass.

Thomas, G. (2021). *Research Methodology and Scientific Writing* (Second ed.). Thrissur, Kerala, India: Springer.

Toth, P. (2019, december 17). *How Vulnerable Are You To a Cyber Attack? A Self-Assessment Tool for Manufacturers*. Retrieved september 26, 2023, from https://www.nist.gov: https://www.nist.gov/blogs/how-vulnerable-are-you-cyber-attack-self-assessment-tool-manufacturers

TVN Noticias. (22 de septiembre de 2023). *tvn*. Recuperado el 2 de septiembre de 2023, de https://www.tvn-2.com: https://www.tvn-2.com/nacionales/no-caiga-phishing-emiten-alerta_1_2080430.html

TVN Noticias. (21 de abril de 2024). *Miviot advierte sobre suplantación de identidad del ministro Rogelio Paredes*. Recuperado el 9 de mayo de 2024, de https://www.tvn-2.com/: https://www.tvn-2.com/nacionales/miviot-advierte-suplantacion-identidad-ministro_1_2130365.html

Umawing, J. (2022, august 8). *KMSpico explained: No, KMS is not "kill Microsoft"*. Retrieved january 2024, 16, from Malwarebytes Labs: https://www.malwarebytes.com/blog/news/2022/08/kmspico-explained-no-kms-is-not-kill-microsoft

Vizuete Salazar, J. (2020). *Implementación de políticas de seguridad en dispositivos móviles para el manejo de la información en Pymes.* Tesis, ESPOCH, Seguridad Telemática, Riobamba. Recuperado el 5 de mayo de 2022

Volynkin, A., Horneman, A., & Morales, J. (2017, may 31). *Ransomware: Best Practices for Prevention and Response*. Retrieved september 24, 2023, from Carnegie Mellon University: https://insights.sei.cmu.edu/blog/ransomware-best-practices-for-prevention-and-response/

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime* (First ed.). New York, United States of America: Apress.

World Economic Forum. (2022). *The Global Risks Report 2022.* Geneva: World Economic Forum. Retrieved from https://www.weforum.org/reports/global-risks-report-2022/

Zigel, H., & Kupreev, O. (2023, june 5). *AO Kaspersky Lab*. Retrieved june 28, 2023, from securelist.com: https://securelist.com/satacom-delivers-cryptocurrency-stealing-browser-extension/109807/

10. APÉNDICES

Seguidamente, se desarrollan los apéndices que se han confeccionado para complementar este proyecto de investigación.

10.1 ENCUESTA APLICADA A LOS ESTUDIANTES DE LA FIEC-CRUV

UNIVERSIDAD DE PANAMÁ
CENTRO REGIONAL UNIVERSITARIO DE VERAGUAS
FACULTAD DE INFORMÁTICA, ELECTRÓNICA Y COMUNICACIÓN
ESCUELA DE INFORMÁTICA PARA LA GESTIÓN EDUCATIVA Y EMPRESARIAL

ENCUESTA:

NIVEL DE CONOCIMIENTOS EN POLÍTICAS DE SEGURIDAD INFORMÁTICA QUE TIENEN LOS ESTUDIANTES DE LA CRUV-FIEC.

Estimado/a Participante:

Este formulario tiene como propósito establecer el nivel de conocimiento en la población estudiantil de la FIEC-CRUV en materia de políticas de seguridad en el contexto informático y tecnológico. Los datos obtenidos serán empleados exclusivamente con fines de investigación académico, respetando los más altos estándares de confidencialidad, privacidad y ética en el manejo de la información, conforme a las normas bioéticas vigentes. Toda la información proporcionada será tratada de manera anónima y utilizada únicamente en el contexto de este estudio, sin posibilidad de identificación individual de los encuestados.

Agradecemos profundamente su tiempo y disposición para responder a este cuestionario; ya que su colaboración es invaluable para el desarrollo de iniciativas que contribuyan a la seguridad y privacidad de la información en la comunidad universitaria. Muchas Gracias por su participación.

1. **¿Reconoce el concepto de Políticas de Seguridad informática?**
   No, no lo reconozco en absoluto
   No, no lo reconozco muy bien
   No estoy seguro/a
   Si, lo reconozco un poco
   Si, lo reconozco completamente

2. **¿Identifica los riesgos asociados con la exposición de su información personal o la de terceros en Internet?**
   No, no lo reconozco en absoluto
   No, no lo reconozco muy bien
   No estoy seguro/a
   Si, lo reconozco un poco
   Si, lo reconozco completamente

3. **¿Conoce la definición de al menos uno de los siguientes términos keylogger, phishing, spyware, ransomware, adware, troyano, gusano informático**

   No, no conozco la definición de ninguno

   No, conozco la definición de muy pocos

   No estoy seguro/a

   Si, conozco la definición de algunos

   Si, conozco la definición de varios

4. **¿Ha recibido capacitación formal sobre seguridad informática, ya sea a través de cursos, talleres, seminarios o programas de formación?**

   No, nunca he recibido capacitación formal

   No, he recibido muy poca capacitación formal

   No estoy seguro/a

   Si, he recibido algo de capacitación formal

   Si, he recibido mucha capacitación formal

5. **¿Mantiene o lleva algún tipo de control para gestionar todas sus contraseñas en caso de olvidarlas?**

   No, nunca llevo un control para gestionar mis contraseñas

   No, llevo muy poco control para gestionar mis contraseñas

   No estoy seguro/a si llevo un control para gestionar mis contraseñas

   Si, llevo algo de control para gestionar mis contraseñas

   Si, llevo un control muy organizado para gestionar mis contraseñas

6. **¿Utiliza alguna de estas opciones como copia de seguridad en caso de perder su información personal o de tercero? Discos extraíbles, Memorias USB, sistema de respaldo en la nube**

   No, las utilizo muy raramente

No, nunca las utilizo

No estoy seguro/a si las utilizo

Si, si las utilizo, aunque no de manera ocasional

Si, si las utilizo con mucha frecuencia

7. **¿Realiza escaneos constantes de sus correos electrónicos, aplicaciones o archivos compartidos, utilizando algún antivirus o de forma manual?**

   No, la verdad es que no realizo escaneos

   No, la verdad es que raramente realizo escaneos

   No estoy seguro/a si realizo escaneos

   Si, si realizo escaneos, aunque no de manera constante

   Si, si realizo escaneos de manera constante

8. **¿Cuenta usted con alguna estrategia para posibles incidentes que amenacen el estado de su privacidad o la seguridad de sus documentos personales que se puedan encontrar en dispositivos móviles o portátiles?**

   No, no cuento con ninguna estrategia en caso de incidentes

   No estoy seguro/a si cuento con alguna estrategia

   Si, si cuento con alguna estrategia en caso de incidentes

9. **¿Utiliza aplicaciones o extensiones en navegadores que le faciliten saber si está intentando acceder a una página web sospechosa?**

   No, la verdad no las utilizo

   No, la verdad las utilizo muy raramente

   No estoy seguro/a si las utilizo

   Si, las utilizo ocasionalmente

   Si, las utilizo muy frecuentemente

10. **¿Es usted capaz de identificar cuando su dispositivo móvil o portátil no está funcionando de manera óptima?**
    - No, no soy capaz de poder identificarlo
    - No, rara vez soy capaz de poder identificarlo
    - No estoy seguro/a de poder identificarlo
    - Si, soy capaz de poder identificarlo en ocasiones
    - Si, siempre soy capaz de poder identificarlo

11. **¿Considera usted que los sistemas operativos y aplicaciones necesariamente deben estar actualizados a su última versión?**
    - No, no lo considero que sea necesario actualizarlos
    - No, considero que con poca frecuencia es necesario actualizarlos
    - No estoy seguro/a si sea necesario actualizarlos
    - Si, considero que frecuentemente es necesario actualizarlos
    - Si, considero que siempre deben ser actualizados

12. **¿Qué tan de acuerdo está usted en que las contraseñas deberían ser cambiadas cada 90 días?**
    - No, estoy en total desacuerdo en que deban ser cambiadas
    - No, no estoy de acuerdo en que deban ser cambiadas
    - No estoy seguro/a si deben ser cambiadas
    - Si, estoy de acuerdo en que deban ser cambiadas
    - Si, estoy totalmente de acuerdo en que deban ser cambiadas

13. **¿Qué tan probable es que sepa identificar cuando está siendo tentado a una estafa a través de correos electrónicos, publicidades o algún otro medio?**
    - No, es muy improbable que sepa identificarlo
    - No, es poco probable que sepa identificarlo

No estoy seguro si sepa identificarlo

Si, es probable que sepa identificarlo

Si, es muy probable que sepa identificarlo

14. **¿Qué tan seguro y cómodo se siente al tener instalado aplicaciones de dudosa procedencia en su dispositivo móvil o computadora portátil?**

No, no me siento seguro/a ni cómodo/a al tenerlos instalados

No, me siento un poco inseguro/a e incómodo/a al tenerlos instalados

No estoy seguro/a de si me siento cómodo/a o segura/a al tenerlos instalados

Si, me siento seguro/a y cómodo/a al tenerlos instalados

Si, me siento muy seguro/a y cómodo/a al tenerlos instalados

15. **¿Quién considera que es más importante para mantener en buen estado la seguridad de los dispositivos móviles o computadoras portátiles, el usuario, antivirus o ambos?**

Considero que el usuario es el más importante

Considero que el antivirus es el más importante

Considero que ambos son importantes

Considero que ninguno de ellos es más importante

No estoy seguro/a de quien sea el más importante

10.2 RESULTADOS ACERCA DE LA ENCUESTA QUE SE APLICÓ A LOS ESTUDIANTES DE LA CRUV-FIEC CON RELACIÓN AL TEMA SOBRE EL NIVEL DE CONOCIMIENTO EN CIBERSEGURIDAD PARA

CONTRARRESTAR EL MALWARE EN DISPOSITIVOS MÓVILES Y PORTÁTILES

Tabla 12: Pregunta1: ¿Reconoce el concepto de Políticas de Seguridad Informática?

¿Reconoce el concepto de Políticas de Seguridad informática?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no lo reconozco en absoluto	Muy Bajo	25	15.06%
No, no lo reconozco muy bien	Bajo	18	10.84%
No estoy seguro/a	Satisfactorio	13	7.83%
Si, lo reconozco un poco	Alto	72	43.37%
Si, lo reconozco completamente	Muy Alto	38	22.89%
Total		166	100.00%
Respuestas al menos Satisfactorias		123	74.10%

Fuente: El autor

Tabla 13: Pregunta 2: ¿Identifica los riesgos asociados con la exposición de su información personal o la de terceros en Internet?

¿Identifica los riesgos asociados con la exposición de su información personal o la de terceros en Internet?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no lo reconozco en absoluto	Muy Bajo	15	9.04%
No, no lo reconozco muy bien	Bajo	29	17.47%
No estoy seguro/a	Satisfactorio	15	9.04%
Si, lo reconozco un poco	Alto	83	50.00%
Si, lo reconozco completamente	Muy Alto	24	14.46%
Total		166	100.00%
Respuestas al menos Satisfactorias		122	73.49%

Fuente: El autor

Tabla 14: Pregunta 3: ¿Conoce la definición de al menos uno de los siguientes términos keylogger, phishing, spyware, ransomware, adware, troyano, gusano informático?

¿Conoce la definición de al menos uno de los siguientes términos keylogger, phishing, spyware, ransomware, adware, troyano, gusano informático?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no conozco la definición de ninguno	Muy Bajo	22	13%
No, conozco la definición de muy pocos	Bajo	26	16%
No estoy seguro/a	Satisfactorio	21	13%
Si, conozco la definición de algunos	Alto	66	40%
Si, conozco la definición de varios	Muy Alto	31	19%
Total		166	100.00%
Respuestas al menos Satisfactorias		118	71.08%

Fuente: El autor

Tabla 15: Pregunta 4: ¿Ha recibido capacitación formal sobre seguridad informática, ya sea a través de cursos, talleres, seminarios o programas de formación?

¿Ha recibido capacitación formal sobre seguridad informática, ya sea a través de cursos, talleres, seminarios o programas de formación?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, nunca he recibido capacitación formal	Muy Bajo	44	27%
No, he recibido muy poca capacitación formal	Bajo	34	20%
No estoy seguro/a	Satisfactorio	32	19%
Si, he recibido algo de capacitación formal	Alto	46	28%
Si, he recibido mucha capacitación formal	Muy Alto	10	6%
Total		166	100.00%
Respuestas al menos Satisfactorias		88	53.01%

Fuente: El autor

Tabla 16: Pregunta 5: ¿Mantiene o lleva algún tipo de control para gestionar todas sus contraseñas en caso de olvidarlas?

¿Mantiene o lleva algún tipo de control para gestionar todas sus contraseñas en caso de olvidarlas?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, nunca llevo un control para gestionar mis contraseñas	Muy Bajo	21	13%
No, llevo muy poco control para gestionar mis contraseñas	Bajo	35	21%
No estoy seguro/a si llevo un control para gestionar mis contraseñas	Satisfactorio	21	13%
Si, llevo algo de control para gestionar mis contraseñas	Alto	63	38%
Si, llevo un control muy organizado para gestionar mis contraseñas	Muy Alto	26	16%
Total		166	100.00%
Respuestas al menos Satisfactorias		110	66.27%

Fuente: El autor

Tabla 17: Pregunta 6: ¿Utiliza alguna de estas opciones como copia de seguridad en caso de perder su información personal o de tercero? Discos extraíbles, Memorias USB, sistema de respaldo en la nube

¿Utiliza alguna de estas opciones como copia de seguridad en caso de perder su información personal o de tercero? Discos extraíbles, Memorias USB, sistema de respaldo en la nube			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, las utilizo muy raramente	Muy Bajo	21	13%
No, nunca las utilizo	Bajo	19	11%
No estoy seguro/a si las utilizo	Satisfactorio	14	8%
Si, si las utilizo, aunque no de manera ocasional	Alto	83	50%
Si, si las utilizo con mucha frecuencia	Muy Alto	29	17%
Total		166	100.00%
Respuestas al menos Satisfactorias		126	75.90%

Fuente: El autor

Tabla 18: Pregunta 7: ¿Realiza escaneos constantes de sus correos electrónicos, aplicaciones o archivos compartidos, utilizando algún antivirus o de forma manual?

¿Realiza escaneos constantes de sus correos electrónicos, aplicaciones o archivos compartidos, utilizando algún antivirus o de forma manual?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, la verdad es que no realizo escaneos	Muy Bajo	48	29%
No, la verdad es que raramente realizo escaneos	Bajo	42	25%
No estoy seguro/a si realizo escaneos	Satisfactorio	26	16%
Si, si realizo escaneos, aunque no de manera constante	Alto	41	25%
Si, si realizo escaneos de manera constante	Muy Alto	9	5%
Total		166	100.00%
Respuestas al menos Satisfactorias		76	45.78%

Fuente: El autor

Tabla 19: Pregunta 8: ¿Cuenta usted con alguna estrategia para posibles incidentes que amenacen el estado de su privacidad o la seguridad de sus documentos personales que se puedan encontrar en dispositivos móviles o portátiles?

¿Cuenta usted con alguna estrategia para posibles incidentes que amenacen el estado de su privacidad o la seguridad de sus documentos personales que se puedan encontrar en dispositivos móviles o portátiles?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no cuento con ninguna estrategia en caso de incidentes	Bajo	66	40%
No estoy seguro/a si cuento con alguna estrategia	Satisfactorio	50	30%
Si, si cuento con alguna estrategia en caso de incidentes	Alto	50	30%
Total		166	100.00%
Respuestas al menos Satisfactorias		100	60.24%

Fuente: El autor

Tabla 20: Pregunta 9: ¿Utiliza aplicaciones o extensiones en navegadores que le faciliten saber si está intentando acceder a una página web sospechosa?

¿Utiliza aplicaciones o extensiones en navegadores que le faciliten saber si está intentando acceder a una página web sospechosa?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, la verdad no las utilizo	Muy Bajo	48	29%
No, la verdad las utilizo muy raramente	Bajo	20	12%
No estoy seguro/a si las utilizo	Satisfactorio	18	11%
Si, las utilizo ocasionalmente	Alto	59	36%
Si, las utilizo muy frecuentemente	Muy Alto	21	13%
Total		166	100.00%
Respuestas al menos Satisfactorias		98	59.04%

Fuente: El autor

Tabla 21: Pregunta 10: ¿Es usted capaz de identificar cuando su dispositivo móvil o portátil no está funcionando de manera óptima?

¿Es usted capaz de identificar cuando su dispositivo móvil o portátil no está funcionando de manera óptima?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no soy capaz de poder identificarlo	Muy Bajo	26	16%
No, rara vez soy capaz de poder identificarlo	Bajo	21	13%
No estoy seguro/a de poder identificarlo	Satisfactorio	22	13%
Si, soy capaz de poder identificarlo en ocasiones	Alto	64	39%
Si, siempre soy capaz de poder identificarlo	Muy Alto	33	20%
Total		166	100.00%
Respuestas al menos Satisfactorias		119	71.69%

Fuente: El autor

Tabla 22: Pregunta 11: ¿Considera usted que los sistemas operativos y aplicaciones necesariamente deben estar actualizados a su última versión?

¿Considera usted que los sistemas operativos y aplicaciones necesariamente deben estar actualizados a su última versión?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no lo considero que sea necesario actualizarlos	Muy Bajo	11	7%
No, considero que con poca frecuencia es necesario actualizarlos	Bajo	21	13%
No estoy seguro/a si sea necesario actualizarlos	Satisfactorio	8	5%
Si, considero que frecuentemente es necesario actualizarlos	Alto	67	40%
Si, considero que siempre deben ser actualizados	Muy Alto	59	36%
Total		166	100.00%
Respuestas al menos Satisfactorias		134	80.72%

Fuente: El autor

Tabla 23: Pregunta 12: ¿Qué tan de acuerdo está usted en que las contraseñas deberían ser cambiadas cada 90 días?

¿Qué tan de acuerdo está usted en que las contraseñas deberían ser cambiadas cada 90 días?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, estoy en total desacuerdo en que deban ser cambiadas	Muy Bajo	20	12%
No, no estoy de acuerdo en que deban ser cambiadas	Bajo	27	16%
No estoy seguro/a si deben ser cambiadas	Satisfactorio	34	20%
Si, estoy de acuerdo en que deban ser cambiadas	Alto	58	35%
Si, estoy totalmente de acuerdo en que deban ser cambiadas	Muy Alto	27	16%
Total		166	100.00%
Respuestas al menos Satisfactorias		119	71.69%

Fuente: El autor

Tabla 24: Pregunta 13: ¿Qué tan probable es que sepa identificar cuando está siendo tentado a una estafa a través de correos electrónicos, publicidades o algún otro medio?

¿Qué tan probable es que sepa identificar cuando está siendo tentado a una estafa a través de correos electrónicos, publicidades o algún otro medio?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, es muy improbable que sepa identificarlo	Muy Bajo	20	12%
No, es poco probable que sepa identificarlo	Bajo	22	13%
No estoy seguro si sepa identificarlo	Satisfactorio	30	18%
Si, es probable que sepa identificarlo	Alto	55	33%
Si, es muy probable que sepa identificarlo	Muy Alto	39	23%
Total		166	100.00%
Respuestas al menos Satisfactorias		124	74.70%

Fuente: El autor

Tabla 25: Pregunta 14: ¿Qué tan seguro y cómodo se siente al tener instalado aplicaciones de dudosa procedencia en su dispositivo móvil o computadora portátil?

¿Qué tan seguro y cómodo se siente al tener instalado aplicaciones de dudosa procedencia en su dispositivo móvil o computadora portátil?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
No, no me siento seguro/a ni cómodo/a al tenerlos instalados	Muy Bajo	33	20%
No, me siento un poco inseguro/a e incómodo/a al tenerlos instalados	Bajo	30	18%
No estoy seguro/a de si me siento cómodo/a o segura/a al tenerlos instalados	Satisfactorio	55	33%
Si, me siento seguro/a y cómodo/a al tenerlos instalados	Alto	34	20%
Si, me siento muy seguro/a y cómodo/a al tenerlos instalados	Muy Alto	14	8%
Total		166	100.00%
Respuestas al menos Satisfactorias		103	62.05%

Fuente: El autor

Tabla 26: Pregunta 15: ¿Quién considera que es más importante para mantener en buen estado la seguridad de los dispositivos móviles o computadoras portátiles, el usuario, antivirus o ambos?

¿Quién considera que es más importante para mantener en buen estado la seguridad de los dispositivos móviles o computadoras portátiles, el usuario, antivirus o ambos?			
Respuestas Posibles	**Valor en el Modelo de Evaluación**	**Conteo**	**Porcentaje**
Considero que el usuario es el más importante	Muy Bajo	32	19.28%
Considero que el antivirus es el más importante	Bajo	22	13.25%
Considero que ambos son importantes	Satisfactorio	84	50.60%
Considero que ninguno de ellos es más importante	Alto	16	9.64%
No estoy seguro/a de quien sea el más importante	Muy Alto	12	7.23%
Total		166	100.00%
Respuestas al menos Satisfactorias		112	67.47%

Fuente: El autor

10.3 SOLICITUD DE INFORMACIÓN ESTADÍSTICA DE LA POBLACIÓN DE LA FIEC-CRUV, A LA SECRETARÍA ACADÉMICA DEL CRUV

Figura 3: Nota de respuesta de la Secretaría Académica del CRUV

Universidad de Panamá
Centro Regional Universitario de Veraguas
Secretaría Académica

Santiago, 29 de abril de 2025.
CRUV/SA/92/2025

Profesor
Raúl Dutari
Facultad de Informática, Electrónica y Comunicación
Centro Regional Universitario de Veraguas

Respetado profesor:

Ante su solicitud, le indicamos a continuación, la información estadística de la población estudiantil de la Facultad de Informática, Electrónica y Comunicación, correspondiente al primer semestre 2025.

- Licenciatura en Informática para la Gestión Educativa y Empresarial
  - 103 estudiantes
- Licenciatura en ingeniería en informática
  - 85 estudiantes

Atentamente,

Dra. Giannina Núñez Marín
Secretaria Académica

2025: "Conmemorando el XX Aniversario de la Universidad de Panamá"
Teléfono (507) 528-3502, 523-3503, 935-1755 ext 128
E-mail: cruv.academica@up.ac.pa

Fuente: (Secretaría Académica, CRUV, 2025)