UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD DE INGENIERÍAS, ARQUITECTURA Y CIENCIAS DE LA NATURALEZA

TÍTULO DEL TRABAJO:

DESARROLLO DE UNA APLICACIÓN PARA GENERAR Y ESCANEAR CÓDIGOS BIDIRECCIONALES QR CON SEGURIDAD INTEGRADA EN ANDROID

LÍNEA DE INVESTIGACIÓN:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

MODALIDAD DE TITULACIÓN:

TRABAJO DE INTEGRACIÓN CURRICULAR

CARRERA:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO A OBTENER:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:

DANIEL ANDRÉ PEÑAHERRERA BARRIGA

TUTOR:

ING. MARCOS ANTONIO ESPINOZA MINA, PHD.

SAMBORONDÓN – ECUADOR

AÑO 2024

ANEXO No. 9

PROCESO DE TITULACIÓN

CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, ……. de …….. de 2024

Magíster

Erika Ascencio

Facultad de Ingenierías, Arquitectura y Ciencias de la Naturaleza

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: DESARROLLO DE UNA APLICACIÓN PARA GENERAR Y ESCANEAR CÓDIGOS BIDIRECCIONALES QR CON SEGURIDAD INTEGRADA EN ANDROID, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: PEÑAHERRERA BARRIGA DANIEL ANDRÉ**,** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

ING. MARCOS ANTONIO ESPINOZA MINA, PHD

Tutor(a)

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: DESARROLLO DE UNA APLICACIÓN PARA GENERAR Y ESCANEAR CÓDIGOS BIDIRECCIONALES QR CON SEGURIDAD INTEGRADA EN ANDROID elaborado por DANIEL ANDRÉ PEÑAHERRERA BARRIGA fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del (%)__ mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.

ATENTAMENTE,

ING. MARCOS ANTONIO MENDOZA MINA, PDF
Tutor(a)

DEDICATORIA

La realización del presente trabajo investigativo no sería posible sin el soporte

de mi familia; especialmente el de mi madre,

cuyo apoyo incondicional me sigue impulsando a ser la mejor versión posible de mí.

Y a mi futura esposa, Valeria, cuya (aún persistente) indiferencia por el manejo de su información personal sirvió como motivación (por segunda vez) para llevar a cabo este trabajo investigativo.

AGRADECIMIENTOS

Deseo agradecer a mis colegas por el apoyo brindado durante este trayecto laboral.

De la misma manera, agradezco a mis docentes, cuya pasión por impartir su conocimiento ha inspirado la realización de este trabajo.

Resumen

El presente trabajo investigativo está enfocado en el desarrollo de una aplicación para dispositivos móviles Android que permita generar y leer códigos de barras de dos dimensiones QR (Quick Response), cuyo contenido se encuentre cifrado de tal manera que sólo el receptor del mensaje logre recibir el mensaje y acceder a la información.

Se plantea que el prototipo resultante de la presente propuesta tecnológica esté calificado para la generación y escaneo de códigos QR. Adicionalmente, el sistema podrá también cifrar el mensaje que se desee enviar. Durante el proceso de cifrado, se hará uso del algoritmo de cifrado por bloques AES (Advanced Encryption Standard) en modo de Encadenamiento de Bloques de Cifrado (CBC), añadiendo un Vector de Iniciación (VI).

El desarrollo de este sistema podría representar un avance en el uso de los códigos QR convencionales; a pesar de ser ampliamente utilizados, integrar mecanismos de protección en ellos podría suponer una mejora en la seguridad de estos códigos.

Dentro de las metodologías de investigación, se hará uso de la metodología aplicada, debido a la implementación de conocimientos técnicos y teóricos como enfoque principal en la resolución de problemas. El alcance aplicado fue de carácter mixto; exploratorio durante la etapa inicial para la compresión del estado del arte de los códigos QR, y descriptivo para detallar las características del prototipo desarrollado y sus funcionalidades.

El prototipo será sometido a diferentes pruebas, esto con la finalidad de validar, estimar y evaluar la efectividad del sistema.

Palabras clave: Seguridad de la Información, Códigos QR, Códigos bidireccionales, Cifrado.

Abstract

This research work focuses on the development of an application for Android mobile devices that allows for generating and reading two-dimensional QR (Quick Response) barcodes, with their content encrypted in such a way that only the intended recipient can receive the message and access the information.

It is proposed that the prototype resulting from this technological proposal be qualified for generating and scanning QR codes. Additionally, the system will also be able to encrypt the message intended for sending. During the encryption process, the AES (Advanced Encryption Standard) block cipher algorithm will be used in Cipher Block Chaining (CBC) mode, adding an Initiation Vector (VI).

The development of this system could represent an advancement in the use of static QR codes; despite their widespread use, integrating protection mechanisms could enhance the security of these codes.

Among the research methodologies, the applied methodology will be used due to its focus on implementing technical and theoretical knowledge as the main approach to problem-solving. The applied scope was of a mixed nature: exploratory during the initial stage to understand the state of the art of QR codes, and descriptive to detail the characteristics and functionalities of the developed prototype.

The prototype will undergo various tests to validate, estimate, and evaluate its effectiveness.

Keywords: Information Security, QR Codes, Two-dimensional Codes, Cipher.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Introducción

(Peralta & Porfirio, 2003) señalan que “Los seres humanos somos gregarios. Esto quiere decir que nacemos y vivimos como miembros de una agrupación de personas llamada sociedad; sin la cual no podríamos existir, porque individualmente, solos y aislados somos los seres más incapaces e indefensos.” (p. 1). Los seres humanos, como criaturas sociales, poseen la necesidad de guardar y compartir información. El desarrollo de nuevas tecnologías ha provocado, poco a poco, una adopción digital global. Debido a esto, muchos usuarios utilizan (y toman provecho) de estas nuevas tecnologías para poder almacenar y transferir grandes volúmenes de información.

Para la Southern New Hampshire University (2023),

> En la era digital, la comunicación cumple con un papel fundamental. En primer lugar, porque permite seguir estableciendo relaciones sociales entre diferentes individuos, y en segundo lugar, porque se trata de la herramienta que facilita la difusión de la información, que puede compartirse fácilmente. Por estos motivos, es imposible contemplar un mundo sin comunicación. (Southern New Hampshire University, 2023)

Dentro de la era digital contemporánea, la presencia de los códigos QR, que son códigos de barras de dos dimensiones (también denominados “bidireccionales” o “2D”) desarrollados por Denso Wave en 1994 (Denso Wave, 1994), ha logrado transformar la manera en la que interactuamos con la información en nuestra vida cotidiana. Desde facilitar transacciones comerciales (Guo, Gao, Yang, & Jia, 2018) hasta proveer enlaces rápidos para recursos en línea (Chandra & Kumar, 2019), los códigos QR han emergido como una herramienta eficiente. Sin embargo, esta misma proliferación ha provocado

grandes desafíos en términos de seguridad informática. La vulnerabilidad de estos códigos QR ha logrado plantear varias interrogantes decisivas sobre su uso.

Como respuesta a esta preocupación creciente, el presente texto investigativo propone el desarrollo de una aplicación para dispositivos móviles Android, que sea capaz de cifrar y descifrar códigos QR mediante el uso del algoritmo de cifrado AES. La elección de este tema investigativo está fundamentada por la urgencia de robustecer la seguridad de un componente utilizado globalmente, dado que pueden ser manipulados por *scammers,* debido que todos estos parecen ser similares (Malwarebytes, 2023). La importancia de abordar este tema en la era actual radica en la necesidad de lograr salvaguardar la información transmitida a través de los códigos QR.

Planteamiento del Problema

La problemática que motiva el desarrollo de este trabajo investigativo está centrada en las vulnerabilidades presentes en los códigos QR convencionales, y su necesidad de fortalecer la seguridad de los mismos. A pesar de que los códigos QR han demostrado ser una herramienta digital valiosa bajo distintos contextos, (Focardi, Luccio, & Wahsheh, 2019) señalan que “las personas tienden a escanear códigos QR y confiar en su contenido, pero no existe ningún mecanismo estándar para proporcionar autenticidad y confidencialidad del contenido del código”.

Para poder llegar a una situación óptima, debemos alcanzar un punto intermedio en el cual los códigos QR garantizan niveles elevados de seguridad manteniendo su eficiencia, practicidad y facilidad de uso actual.

Las principales causas para la proliferación del malware (por medio de códigos QR), y el uso de este por actores malintencionados son: la facilidad de lectura de los códigos QR y el uso de dispositivos móviles para escanear estos códigos, cuando una

persona escanea un código QR, no tiene forma de saber de antemano si el código es legítimo (Kaspersky, 2023), y la facilidad que tienen los ciberdelincuentes para tanto códigos QR digitales como físicos para reemplazar códigos legítimos por códigos maliciosos (Posey, 2022).

Sobre los posibles riesgos de la seguridad durante el uso de códigos QR, (Focardi, Luccio y Wahsheh, 2019) comentan que “los posibles riesgos de seguridad se refieren a la codificación de URL maliciosas que parecen similares a las honestas y a la codificación de datos que desencadenan vulnerabilidades en las aplicaciones de back-end” (Focardi, Luccio, & Wahsheh, 2019). Si bien es cierto que se han planteado algunas soluciones, aún no se cuenta con un estándar generalizado y eficaz desde la perspectiva de la seguridad de la información.

Como consecuencia, Internet Crime Complaint Center (2023) expone que

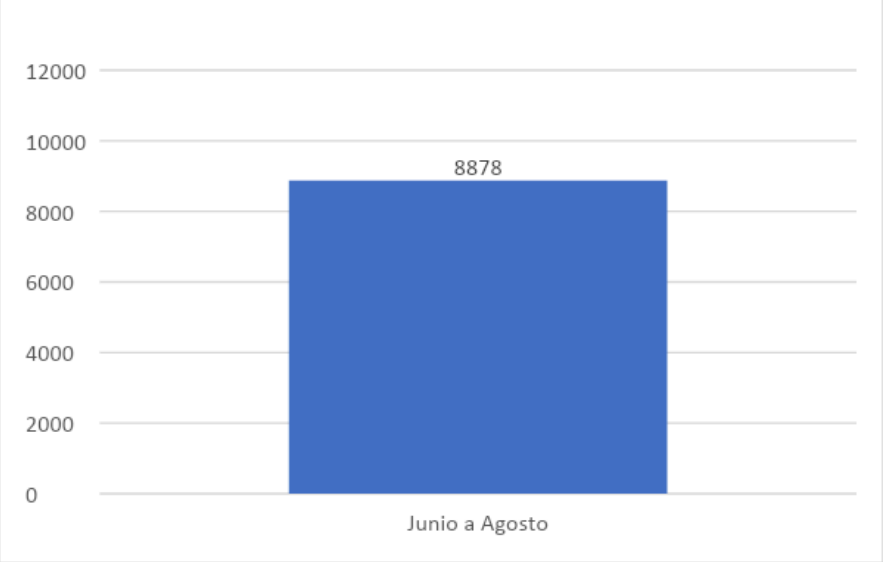
> “Los códigos QR maliciosos también pueden contener malware incrustado, lo que permite a un criminal acceder al dispositivo móvil de la víctima e identificar su ubicación, así como información personal y financiera. El ciberdelincuente puede aprovechar la información financiera robada para retirar fondos de las cuentas de la víctima”. (Internet Crime Complaint Center (IC3), 2023)

Estadísticas de ataques utilizando códigos QR

Durante el año 2024, el proveedor de soluciones de ciberseguridad, Keepnet Labs, publicó un análisis detallado de las estadísticas en aumento del Quishing. Este estudio recolectó información, desde 2023 a 2024, sobre reportes realizados a diferentes sistemas de seguridad. (Keepnet Labs, 2024)

Ilustración 1.

Incidentes relacionados con Quishing reportados por sistemas de seguridad durante el 2023

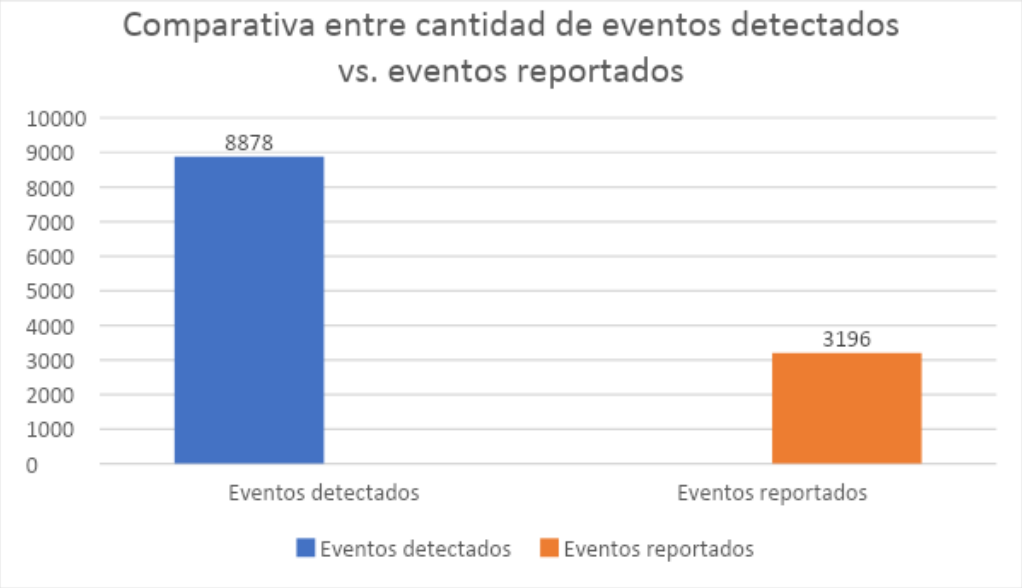


Nota. La ilustración muestra los eventos de seguridad reportados por sistemas durante los meses de junio a agosto de 2023. Fuente: (Keepnet Labs, 2024). Elaborado por: Autor.

De los 8878 eventos que fueron detectados por los sistemas, únicamente el 36% de estos (3196 eventos) fueron identificados y reportados por los destinatarios. Estas estadísticas sobre el phishing con códigos QR muestran que la baja tasa de detección y reporte es un aspecto alarmante de estos ataques. Esta falta de conciencia y preparación en seguridad deja a muchos expuestos a los peligros del Quishing.

Ilustración 2.

Tasa comparativa entre Detección y Reporte de los Ataques de Phishing utilizando Códigos QR



Nota. Ilustración comparativa entre la cantidad de eventos detectados y los eventos reportados. Fuente: (Keepnet Labs, 2024). Elaborado por: Autor.

Las estadísticas sobre el phishing con códigos QR, demostradas en la ilustración 2, detallan que la baja tasa de detección y reporte es un aspecto alarmante de estos ataques. Apenas el 36% de los incidentes fueron correctamente identificados y reportados por los destinatarios. Esta falta de conciencia y preparación en seguridad deja a muchos expuestos a los riesgos del phishing engañoso con códigos QR.

Por su parte, la firma de soluciones de seguridad McAfee publicó, en el año 2023, un reporte de seguridad denominado *Safer Summer Holidays.* Este estudio, que contó con la participación de 7000 personas alrededor de siete países, brinda una perspectiva sobre qué tan cuidadosas son las personas cuando interactúan con herramientas digitales mientras viajan al exterior.

El estudio asegura que una de cada tres personas han sido víctimas de estafas al momento de reservar vuelos o lugares de hospedaje más económicos en línea. También se prevé que 1 de cada 4 estadounidenses serán víctimas de estafas mediante el uso de códigos QR fraudulentos. (McAfee, 2023)

Con base en lo anteriormente descrito, se demuestra cómo los QR han cambiado la manera con la que interactuamos con nuestro medio, dado que son capaces de almacenar determinados tipos de información. Actualmente, son utilizados en diferentes sectores, tales como: salud, Instituciones educativas, Marketing y publicidad, Hotelería y Turismo, Retail, Finanzas, entre otros. Debido a esto, podemos concluir que la utilización de los códigos QR supone una gran manera de acceder a información de una manera muy rápida y eficaz.

Sin embargo, también se ha demostrado que los códigos QR contienen varias vulnerabilidades que serán explicadas a detalle durante el desarrollo de este trabajo investigativo. El uso de códigos QR sin ninguna medida de seguridad representa un riesgo que debe ser mitigado.

Mediante el desarrollo del aplicativo, se espera que los resultados demuestren una mejora significativa en la seguridad de los códigos QR, sin sacrificar la facilidad de uso y la practicidad de estos. Finalmente, se espera que el desarrollo de la aplicación sirva como referencia para futuros trabajos investigación (que podrían tener o no aplicación práctica) enfocados en la protección de la información, transmitida mediante los códigos QR, para así contribuir con un entorno digital más seguro dentro de la era digital actual.

Pregunta Global

¿Sería posible generar un código QR con un mensaje cifrado cuya información sólo pueda ser leída por los destinatarios?

Preguntas Específicas

- ¿Cuáles son las vulnerabilidades en la seguridad de los códigos QR convencionales que necesitan ser abordadas?
- ¿De qué manera se podría implementar medidas de seguridad para los códigos QR sin sacrificar la facilidad de uso?
- ¿Qué medidas de seguridad adicionales son necesarias para asegurar la protección de la información contenida en el código QR para poder prevenir las posibles amenazas?

Objetivos del trabajo de Integración Curricular

Objetivo General

Desarrollar una aplicación para dispositivos Android que integre componentes de seguridad para su incorporación en el código QR, con la finalidad de asegurar la integridad de la información transmitida a través de estos códigos.

Objetivos Específicos

- Identificar las vulnerabilidades presentes en los códigos QR convencionales.
- Establecer un algoritmo de cifrado.
- Demostrar la viabilidad práctica del nuevo código QR propuesto mediante la ejecución de pruebas controladas y desarrollo del prototipo.

Justificación

Tradicionalmente, los códigos unidireccionales (códigos de barras) han tenido sus orígenes en las bodegas, en donde eran los métodos más populares para identificar y hacer seguimiento del inventario. La siguiente generación de códigos, llamados

códigos bidireccionales, lograban almacenar información de manera vertical y horizontal, lo que permitía almacenar mucha mayor información que su contraparte. El código de Respuesta Rápida ("QR – Quick Response", por sus siglas en inglés) nació en el año 1994, de la mano de la empresa Japonesa Denso Wave (Denso Wave, 1994). Estos códigos nacieron como una opción revolucionaria al código de barras tradicional, brindando una solución más eficiente.

Los códigos de respuesta rápida (QR) se han tornado en un fenómeno mundial, siendo adoptado como medio de pago electrónico en varias localidades del mundo. Un reporte publicado por la consultora de negocios Grand View Research, reveló que la tasa de mercado global del uso de códigos QR como método de pago, durante el 2022, fue de 9.98 miles de millones de dólares (Grand View Research, 2023). Este mismo reporte pronostica un incremento de esta tasa en 16.2% para el año 2030. Por su lado, la empresa Insider Intelligence, empresa dedicada a realizar investigaciones de mercado y tendencias de marketing digital reveló, mediante un estudio publicado en el año 2021, que el número de usuarios de teléfonos inteligentes, mayores de 18 años, quienes escanearon (al menos) un código QR durante el año del estudio, pasó de ser 52.6 millones de usuarios, en el 2019 a 75.8 usuarios durante el 2021 (Insider Intelligence, 2022). Este estudio muestra un claro incremento de usuarios durante el año 2020, a causa de la pandemia de COVID-19.

La popularidad y aceptación global del uso de los códigos QR es inmensa, cualquier persona puede crear y difundir un código QR con la finalidad de que este sea escaneado. Curiosamente, tal facilidad de creación y difusión es lo que ha generado una creciente preocupación dentro del ámbito de la seguridad de la información. La firma de seguridad Kaspersky (2023) comenta que, como los humanos no pueden leer

códigos QR, es fácil para los atacantes alterar un código QR para que apunte a un recurso alternativo sin ser detectados. (Kaspersky, 2023)

En el año 2022, la plataforma de seguridad basada en nube (Lookout, 2022) publicó un estudio denominado “Global State of Mobile Phishing Report” en donde se muestra que el año 2022 tuvo el porcentaje más alto de tasas de encuentros con phishing móvil jamás registrado: más del 30 % de los usuarios personales y empresariales estuvieron expuestos a estos ataques cada trimestre del año.

Durante el inicio del año 2023, Cofense (2023), una empresa que brinda soluciones de seguridad -especializada en phishing-, observó una gran cantidad de campañas de phishing con códigos QR (conocida como “Quishing”) dirigidas a las credenciales de Microsoft de usuarios de una amplia gama de industrias. El objetivo más notable, una importante empresa de energía con sede en EE. UU., vio alrededor del 29% de los más de 1.000 correos electrónicos que contenían códigos QR maliciosos. Otras cuatro industrias objetivo principales incluyen manufactura, seguros, tecnología y servicios financieros, que representan el 15%, 9%, 7% y 6% del tráfico de la campaña, respectivamente. La mayoría de los enlaces de phishing estaban compuestos por URL de redireccionamiento de Bing, pero otros dominios notables incluyen krxd.com (asociado con la aplicación Salesforce) y cf-ipfs.com (servicios Web3 de Cloudflare). (Cofense, 2023)

La revista digital Security Magazine publicó los resultados del estudio realizado por la firma de ciberseguridad Reliaquest, aquel estudio subraya las crecientes tendencias en ciberataques dirigidos a usuarios de códigos QR. Un informe de análisis de los incidentes de sus clientes muestra un aumento del 51 % en este tipo específico de tendencia de phishing cibernético durante septiembre de 2023, lo que contrasta

marcadamente con las cifras acumuladas de los meses anteriores, de enero a agosto. (Security Magazine, 2023).

Empleando un enfoque en el contexto nacional, el proveedor de servicios de seguridad informática, ESET, publicó, en el año 2023, un reporte anual denominado "*ESET: Security Report Latam 2023*". Dentro de estos hallazgos, se releva que, a nivel global, los países de la región con mayor porcentaje de detecciones de códigos maliciosos en campañas de Phishing son Ecuador 8%, siendo este el país con mayores detecciones por phishing en la región Latinoamericana. Para establecer una comparación, el estudio también revela los porcentajes de diferentes países pertenecientes a la misma región, estos fueron: Costa Rica 7,2%, Colombia 5,7%, Guatemala 5,2% y El Salvador 5,1%. (ESET, 2023)

Uno de los vectores de propagación más utilizados y que es el punto de partida de muchos de los ataques que afectan a las organizaciones es el phishing. Según los datos de la telemetría de ESET en Latinoamérica, los países con mayores niveles de detección de este tipo de amenaza son Ecuador, Costa Rica, Colombia, Guatemala y El Salvador. (ESET, 2023)

Esto podría desencadenarse en un problema para los usuarios de estos códigos (tomando en consideración que esto no se limita a individuos, sino que también a PyMES e industrias) que utilicen esta tecnología para la transferencia de información, dado que su seguridad será vulnerada y dará lugar a, irremediablemente, una pérdida de información y monetaria considerable. Debido a aquello, resulta imprescindible el desarrollar medidas informáticas de seguridad para asegurar la integridad de los datos durante el proceso de escaneo y transferencia de información, utilizando códigos QR; todo esto, sin perder la facilidad y practicidad que caracteriza a estos últimos. Por lo

tanto, el desarrollo de este aplicativo representaría un progreso significativo en el campo de la seguridad de la información.

Capítulo 1: Marco Teórico

1. Marco Teórico

1.1. Marco Fundamental

1.1.1. Importancia de la Seguridad Informática

La creciente interconexión global de sistemas informáticos, redes, y aplicaciones, así como de las empresas, ha elevado la importancia de la seguridad de la información a un nivel central en el contexto del desarrollo social. Las herramientas, anteriormente utilizadas para proteger y salvaguardar datos clasificados dentro de contextos diplomáticos o militares, ahora abarca un espectro mucho más amplio, en donde se incluyen transacciones comerciales y financieras, contratos, datos personales, registros médicos, comercio electrónico, entre otros. Esta expansión de la seguridad abarca dimensiones cada vez mayores y diversas dentro de nuestra vida cotidiana.

Por lo antes expuesto es que la seguridad informática toma tanta importancia, no solo desde el punto de vista de resguardo de información, sino también económico, la inversión de tiempo para el adiestramiento y programas de protección son la única manera de hacerle frente a los cibercriminales y evitar mayores pérdidas monetarias en el futuro (Gamboa, 2020).

1.1.2. Concepto y definición de los códigos QR

La firma de seguridad Kaspersky define a los códigos QR como “Un tipo de código de barras que puede ser fácilmente leído por un dispositivo digital y que almacena información como una serie de píxeles en una cuadrícula en forma de cuadro.” (Kaspersky, 2023)

Sobre su funcionamiento, la empresa de soluciones de seguridad, Fortinet, comenta:

Cuando un usuario escanea con un lector de códigos QR, obtienen acceso inmediato al contenido que un código QR codifica, lo que luego desencadena una acción. Estas incluyen abrir una URL específica en el navegador web del usuario, registrarse automáticamente en una ubicación o conectarse a una red inalámbrica. Los códigos QR suelen usarse para almacenar texto en código ASCII (American Standard Code for Information Interchange), pero también pueden almacenar código binario. (Fortinet, s.f.)

Basado en el texto anterior, podemos concluir que los códigos QR funcionan como versiones digitales de los códigos de barras; fáciles de leer para dispositivos digitales y que almacenan información en una cuadrícula de píxeles. Cuando estos códigos son escaneados, proporcionan acceso instantáneo al contenido integrado, lo que desencadena diversas acciones, tales como: abrir enlaces web, realizar registros automáticos o conectarse a redes inalámbricas. Aunque comúnmente almacenan texto, también es posible que contengan código binario.

1.1.2.1. Breve historia y desarrollo de los códigos bidireccionales

Debido a las limitaciones de espacio de almacenamiento en los códigos de barras, Denso Wave, una compañía japonesa (subsidiaria de *Toyota Motor Corporation*) que fabrica componentes automotrices, tuvo que aplicar múltiples códigos en un solo producto para poder rastrear y transmitir la información correctamente. (Denso Wave, 1994). Además, debido a que los códigos de barras solo pueden ser escaneados desde una dirección, la empresa experimentó retrasos en la producción cuando los escáneres no podían leer los códigos adjuntos en las diversas formas y tamaños de las piezas automotrices. Esto resultó en dificultades para cumplir con los plazos de entrega debido a la ralentización de la producción causada por los códigos de barras.

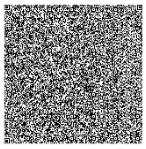
En 1994, Masahiro Hara, un empleado de Denso Wave, ideó los códigos QR mientras jugaba al juego “Go”. “Go”, es un juego de tablero con una matriz de 19x19, y piedras de colores colocadas sobre ella. Al observar el tablero de “Go”, Masahiro percibió la posibilidad de que un sistema de cuadrícula pudiera contener mucha más información en un solo código y ser leído desde diversas direcciones, distancias y ángulos, resultando en un menor tiempo de escaneo, agilizando así los procesos de producción (Denso Wave, s.f.). Hara y el equipo de Denso Wave llevaron esta idea a la realidad y desarrollaron el Código QR (Quick Response Code).

Existen varios tipos y modelos de códigos QR diseñados para múltiples propósitos y aplicaciones. Estos códigos pueden diferir en términos de tamaño, complejidad y capacidad de almacenamiento de datos. Además, pueden presentar variaciones en su diseño y estructura visual, adaptándose a las necesidades específicas de diferentes industrias y usuarios. (Keyence, s.f.). Las diferencias entre los modelos se detallan a continuación:

1.1.2.2. Modelos de códigos QR

Tabla 1.

Clasificación de modelos de código QR

Modelo	Máxima capacidad de caracteres	Número de versión máxima	Imagen referencial
QR Modelo 1	● Números: 1197 caracteres ● Alfanumérico: 707 caracteres ● Binario: 468 bytes ● Kanji: 299 caracteres	El modelo 1 puede ser aplicado hasta la versión 14 (módulos de 73x73)	
QR Modelo 2	● Números: 7089 caracteres ● Alfanumérico: 4296 caracteres ● Binario: 2953 bytes ● Kanji: 1817 caracteres	El modelo 2 puede ser aplicado hasta la versión 40 (módulos 177 x 177)	

Nota. Clasificación simplificada de los distintos modelos de QR. Fuente: Keyence.eu

En resumen, se han creado varios tipos y modelos de códigos QR, esto con la finalidad de cubrir las distintas necesidades para almacenar y transferir información, y cuya exigencia se eleva con el paso del tiempo.

1.1.3. La Integridad de los datos durante la transferencia de información

Se entiende como integridad de los datos a la garantía de la exactitud, fiabilidad y consistencia de la información, ya sea que se encuentre siendo procesada, transmitida o almacenada en cualquier dispositivo.

Sobre este tema, la firma IBM comenta lo siguiente:

> La integridad de los datos es la garantía de que los datos de una organización son precisos, completos y consistentes en cualquier punto de su ciclo de vida. Mantener la integridad de los datos implica proteger los datos de una organización contra pérdidas, filtraciones e influencias corruptoras**.** (IBM, 2024)

Es importante destacar que alcanzar la integridad de los datos no es una tarea únicamente reservada para un único sistema, plataforma o herramienta; se necesita el esfuerzo colectivo de la organización para poderla alcanzar, dicho esfuerzo será proveniente del conjunto de la infraestructura, las políticas de seguridad que se hayan establecido, y sobre todo el compromiso de los individuos que tienen acceso a los sistemas de datos.

1.1.3.1. Principios ALCOA++

Estos principios se crean para enfrentar los desafíos asociados con la preservación de la integridad de los datos, especialmente en registros electrónicos.

Sobre su origen, Mettler-Toledo International Inc afirma que “los principios ALCOA++ de integridad de datos provienen de las directrices de la Administración de Alimentos y Medicamentos (FDA) de los Estados Unidos, la Agencia Europea de Medicamentos (EMA) y otras autoridades reguladoras.” (Mettler-Toledo International Inc, 2024). Para poder comprender estos principios, (Willis, s.f.) lista cada uno de ellos con su explicación, como se puede ver en la siguiente tabla:

Tabla 2.

Principios del modelo ALCOA++

Nombre del Principio	**Explicación**
Attributable (Atribuible)	¿Quién generó la información o realizó una acción?
Legible	¿Puede leerse la información de los registros de las bitácoras de laboratorio?

Contemporaneous (Contemporáneo)	¿La información se documentó en el momento en que se realizó la actividad?
Original	¿Es la información un registro u observación original, o una copia certificada del mismo?
Accurate (Exacto)	¿Hay errores o ediciones sin enmiendas documentadas?
Complete (Completo)	Toda la información, incluyendo cualquier repetición o reanálisis se encuentra registrada.
Consistent (Consistente)	Todos los elementos se encuentran fechados o cuentan con registro de hora en la secuencia esperada.
Enduring (Duradero)	La información se registra en bitácoras de laboratorio oficiales y/o en registros electrónicos.
Available (Disponible)	Los reportes de datos se encuentran disponibles para ser revisados, auditados, o inspeccionados, durante todo su ciclo de vida.
Traceable (Trazable)	La información debe ser trazable durante todo su ciclo de vida, y los cambios que se realicen deben ser registrados como parte de los metadatos.

Nota. Esta tabla muestra los principios del modelo ALCOA++. Fuente: Global Life Science Services Group, Adaptado de ALCOA++ por T. Willis.

1.2. Marco Conceptual

1.2.1. Conceptos Clave en la Seguridad de Códigos Bidireccionales

1.2.1.1. Tríada CID de la Seguridad de la Información

La tríada CID (o CIA, por sus siglas en inglés) es un modelo común dentro de la seguridad de la información. Este modelo funciona como base fundamental para el desarrollo de sistemas de seguridad.

1.2.1.1.1. Confidencialidad

La Confidencialidad hace referencia a la protección de la información contra el acceso no autorizado, es decir, se asegura que los datos sean accesibles únicamente para los usuarios autorizados y mantener la privacidad de la información.

La multinacional Fortinet, dedicada al comercio y desarrollo de software de seguridad comenta:

> La confidencialidad implica los esfuerzos de una organización para garantizar que los datos se mantengan en secreto o privados. Para lograr esto, el acceso a la información debe controlarse para evitar el intercambio no autorizado de datos, ya sea intencional o accidental y asegurar la integridad de la información. (Fortinet, s.f.)

1.2.1.1.2. Integridad

La Integridad consiste en garantizar que los datos sean fiables y no hayan sido sometidos a ningún proceso que haya podido alterarlos. La integridad, como tal, sólo será preservada si los datos son precisos, confiables y auténticos.

Sobre este aspecto, la Washington University in St. Louis afirma:

> Es importante destacar que la integridad de los datos puede ser comprometida por autores sin mala intención, tales como: fallos en los sistemas informáticos, errores de usuario, entre otros. Por otro lado, los autores malintencionados (como ciberdelincuentes) pueden alterar la integridad de los datos. (Washington University in St. Louis, s.f.)

1.2.1.1.3. Disponibilidad

La Disponibilidad asegura que los datos y sistemas sean accesibles y operativos cuando se los necesite. La disponibilidad de la información se garantiza si y sólo si los usuarios autorizados pueden acceder a los datos y recursos sin interrupciones.

La firma de seguridad informática CheckPoint Software Technologies (2024) comenta:

> Las organizaciones se enfrentan a una variedad de amenazas naturales e impulsadas por humanos a la disponibilidad de los datos y del sistema. Los cortes de energía e Internet o los desastres naturales podrían dejar los sistemas fuera de línea. La denegación de

servicio distribuido (DDoS), el ransomware y otros ataques podrían hacer que los sistemas y los datos sean inaccesibles. (CheckPoint, 2024)

1.2.1.2. Criptografía

La criptografía es la práctica de desarrollar y utilizar algoritmos codificados para proteger y ocultar la información transmitida para que solo puedan ser leídas por aquellos con permiso y capacidad de descifrarla. (IBM, 2024)

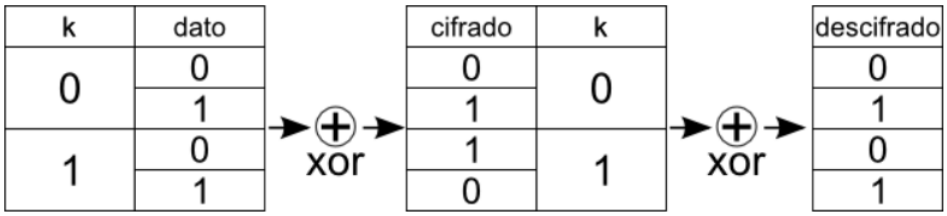
Dicho esto, se puede acotar que la criptografía se ocupa de proteger la información mediante la transformación de datos en un formato seguro, de tal manera que sólo los usuarios autorizados puedan acceder a ella.

1.2.1.2.1. Cifrado

El cifrado es un método de codificación de datos, de modo que nadie pueda leerlos, salvo las partes autorizadas. El proceso de cifrado, o encriptado, convierte los textos normales en codificados utilizando una clave criptográfica. Una clave criptográfica es un conjunto de valores matemáticos conocidos y convenidos por y entre el remitente y el destinatario. (Kingston, 2023).

Ilustración 3.

Funcionamiento del cifrado RC4-ARC4



Nota. Funcionamiento del cifrado, se puede apreciar como un bit se cifra haciendo *XOR* con el valor de la función de flujo de cifrado en ese bit. Fuente: (García, s.f.)

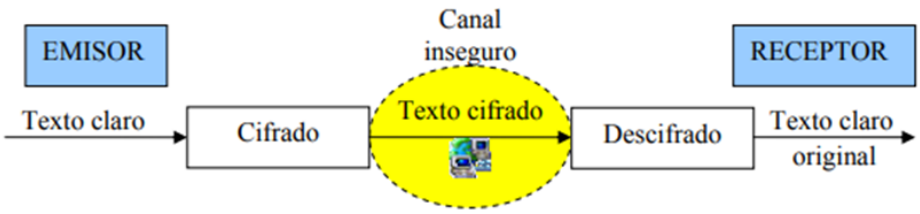
1.2.1.2.2. Descifrado

Si el descifrado es la contraparte del cifrado, entonces este buscará, mediante el uso de algoritmos, la conversión de un texto previamente cifrado, en texto plano.

El descifrado es una primitiva criptográfica: transforma un mensaje de texto cifrado en texto simple utilizando un algoritmo criptográfico llamado cifrado. Al igual que el cifrado, el descifrado en cifrados modernos se realiza mediante un algoritmo específico y una clave. Dado que el algoritmo suele ser público, la clave debe permanecer secreta si el cifrado se mantiene seguro. (MDN Web Docs, 2023).

Ilustración 4.

Aplicación del descifrado sobre un texto cifrado



Nota. La ilustración muestra la finalidad, a nivel general, del descifrado. Esto puede lograrse mediante la aplicación de varios algoritmos de descifrado. Fuente: (Instituto Nacional de Ciberseguridad, 2019)

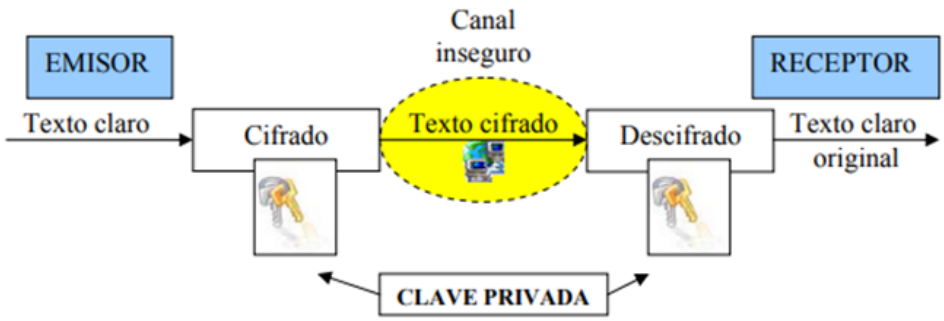
1.2.1.2.3. Algoritmos de Cifrado

Los algoritmos de cifrado son procesos matemáticos utilizados para convertir información legible (texto plano) en un formato ininteligible (texto cifrado) y viceversa. Estos algoritmos se dividen en dos categorías principales: cifrado simétrico y cifrado asimétrico.

- Cifrado Simétrico: Llamados así porque utilizan la misma clave (clave simétrica) para el cifrado y descifrado de la información.

Ilustración 5.

Funcionamiento general del cifrado simétrico



Nota. Explicación general del proceso de cifrado simétrico. Fuente: (Instituto Nacional de Ciberseguridad, 2019)

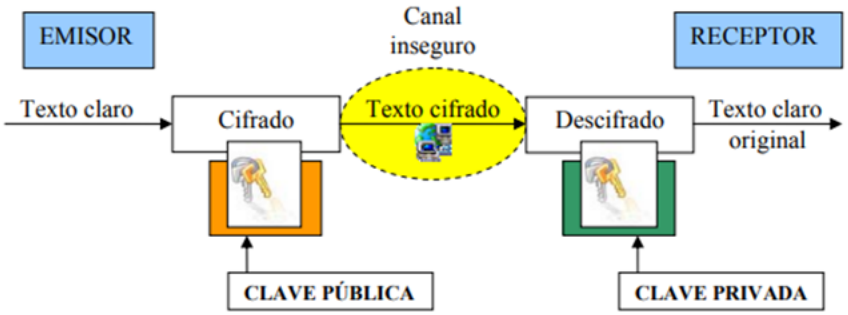
- Cifrado Asimétrico: Denominado así debido al uso de dos llaves (claves), una pública y otra privada; estas llaves forman una dupla y se encuentran matemáticamente relacionadas.

  Sobre el proceso del cifrado asimétrico, ISO (2023) aporta:

  Para aplicar la criptografía de clave pública, el remitente utiliza la clave pública del destinatario previsto para codificar el mensaje y luego lo envía. Cuando el mensaje llega a su destino, solo se puede utilizar la clave privada del destinatario para descodificarlo, lo que significa que un eventual mensaje robado no sirve de nada al ladrón sin la clave privada correspondiente. (ISO, 2023)

Ilustración 6.

Funcionamiento general del cifrado asimétrico

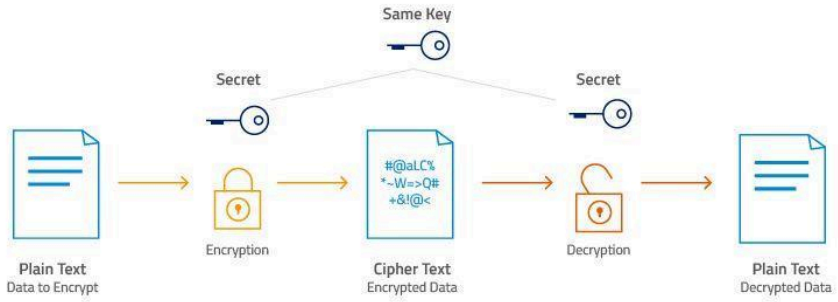


Nota. La siguiente imagen ilustra (en un plano general) el funcionamiento del cifrado asimétrico. Fuente: (Instituto Nacional de Ciberseguridad, 2019)

1.2.1.2.4. Cifrado AES

El Advanced Encryption Standard, abreviado AES, se usa con el fin de cifrar datos y de protegerlos contra cualquier acceso ilícito. El método criptográfico emplea para este objetivo una clave de longitud variada y se denomina según la longitud de clave usada AES-128, AES-192 o AES-256. (NFON)

Ilustración 7.
Funcionamiento del Cifrado AES



Nota. Utilización de cifrado AES en texto plano. Fuente: (Comillas Universidad Pontificia, 2022)

1.2.1.2.5. Vector de inicialización

El vector de utilización no es más que un bloque de bits arreglados de manera aleatoria, esto permite generar resultados que distan del cifrado si se usase el mismo texto y la misma clave.

1.2.1.2.6. Codificación en Base64

La utilización del algoritmo Base64 permite la representación de los datos en formato ASCII (binarios). Para lograr aquello, hace uso del alfabeto Base64, el cual contiene 65 caracteres.

1.2.1.2.7. Cadena de Cifrado en Bloques

El CBC (cipher-block chaining) es un sistema en el que se realiza una operación XOR entre el bloque de texto plano y el bloque de texto cifrado anterior. Para dar inicio a esta operación, entonces, se utiliza un valor conocido como vector de inicialización (IV, por sus letras iniciales en inglés). (KeepCoding, 2024)

1.2.2. Definiciones de amenazas, ataques y vulnerabilidades comunes en códigos QR

1.2.2.1. Quishing

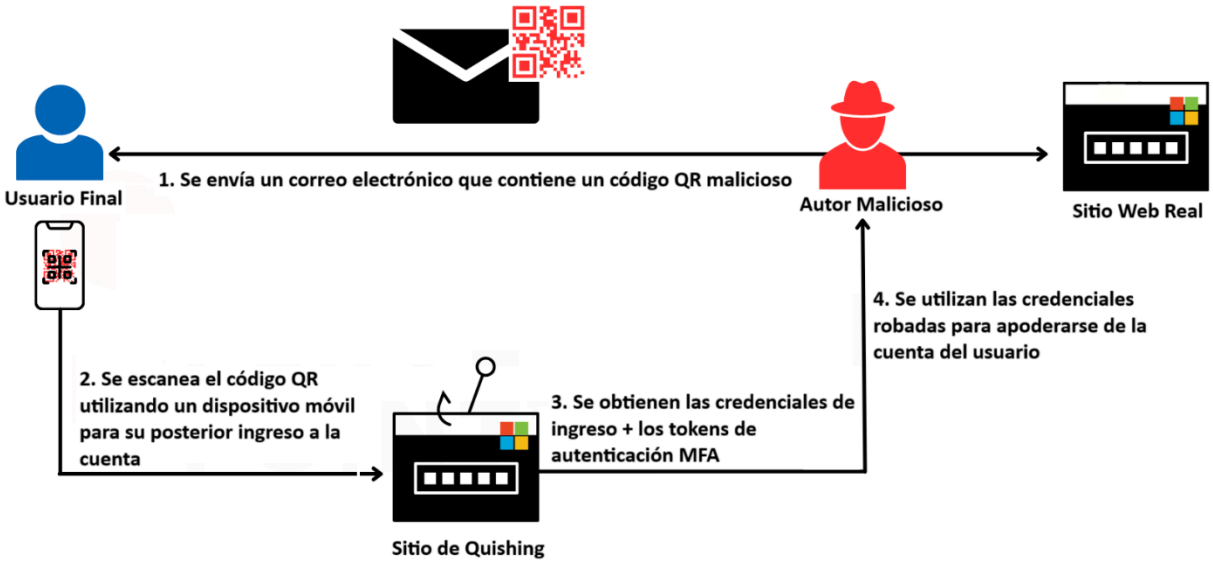
El *quishing* (también llamado “QR phishing”) es la implementación de códigos QR fraudulentos, por parte de autores malintencionados, para que sean posteriormente escaneados por las víctimas. Tiene como finalidad la sustracción de información sensible para su posterior uso en actividades ilícitas como robo de identidad, despliegue de ransomware o fraude financiero.

El proveedor de servicios de seguridad en la nube, Cloudfare, comenta lo siguiente:

En un ataque de quishing, los atacantes crean un código QR y lo enlazan a un sitio web malicioso. Normalmente, el atacante incrustará el código QR en correos electrónicos de phishing, redes sociales, folletos impresos u objetos físicos, y utilizará técnicas de ingeniería social para atraer a las víctimas…al utilizar sus teléfonos para escanear el código QR, las víctimas son dirigidas al sitio malicioso. (CloudFlare, s.f.)

Ilustración 8.

Funcionamiento del Quishing enfocado en la sustracción de credenciales



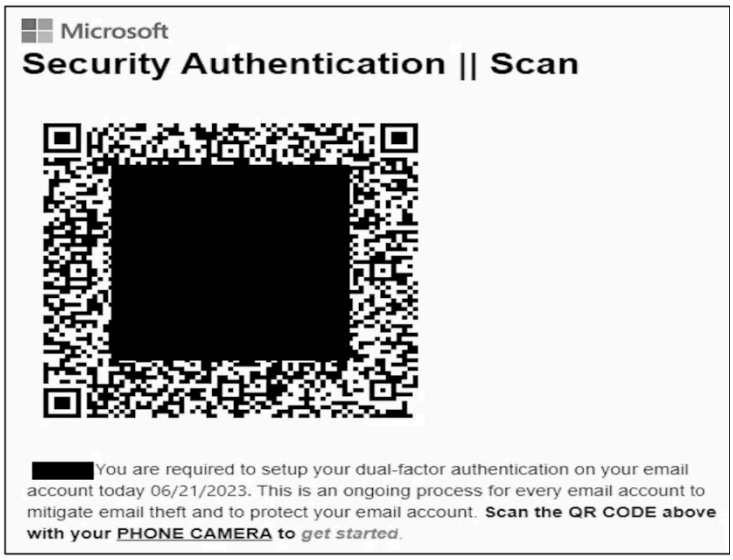
Nota. Explicación del funcionamiento del Quishing para el robo de credenciales mediante el correo electrónico. Fuente: PerceptionPoint

En septiembre de 2023, la firma de seguridad Hoxhunt realizó una prueba de referencia de quishing, que examinó a casi 600,000 empleados de 38 organizaciones en 9 industrias y 125 países. Los resultados revelaron que poco más de un tercio (36%) de los destinatarios identificaron y reportaron con éxito un ataque de phishing simulado a través de un código QR. Más de la mitad no lo reconoció como una amenaza, mientras que el 5% no superó la simulación. En términos prácticos, esto significaría que la

mayoría de las organizaciones quedarían vulnerables, si no completamente comprometidas, ante un ataque de phishing similar. (Hoxhunt, 2023).

Ilustración 9.

Captura de un email phishing conteniendo un código QR malicioso



Nota. Captura de un correo enviado mediante una campaña de phishing, el correo muestra a Microsoft como el emisor del mismo. Este correo contiene un QR que redirige a un sitio malicioso. Fuente: (Hoxhunt, 2023)

1.2.2.2. QRLJacking: Ataques de sesión

QRLJacking, o secuestro de inicio de sesión con código QR, es un método de ingeniería social que explota la función de iniciar sesión (mediante la utilización de códigos QR) utilizada por muchas aplicaciones y sitios web. Esta técnica puede llevar a la sustracción completa de una cuenta. Un ataque típico de QRLJacking se desarrolla de la siguiente manera:

- El atacante crea un sitio de phishing que imita la página de inicio de sesión de la aplicación o sitio objetivo, incluyendo un código QR falso que controla.

- El atacante envía el enlace de phishing a las víctimas a través de correo electrónico, SMS, aplicaciones de mensajería, etc.
- La víctima abre el enlace en su dispositivo móvil y escanea el código QR falso, creyendo que es legítimo.
- Al escanear el código, la víctima inicia sesión en la sesión falsa del atacante en lugar de la aplicación real.
- La aplicación asocia la cuenta de la víctima con la sesión del atacante y envía datos sensibles (como tokens de acceso).
- El atacante obtiene el control total de la cuenta de la víctima.

En agosto de 2023, el investigador de ciberseguridad Cristian Giustini reveló una instancia de un ataque QRLJacking utilizado sobre la plataforma de juegos Steam. El atacante creó un sitio de phishing, simulando ser el portar de inicio de sesión de Steam, que incluía un código QR como método de autenticación; una vez escaneado por la víctima, el atacante podría robar sus credenciales y obtener control total sobre la cuenta. (Giustini, 2023).

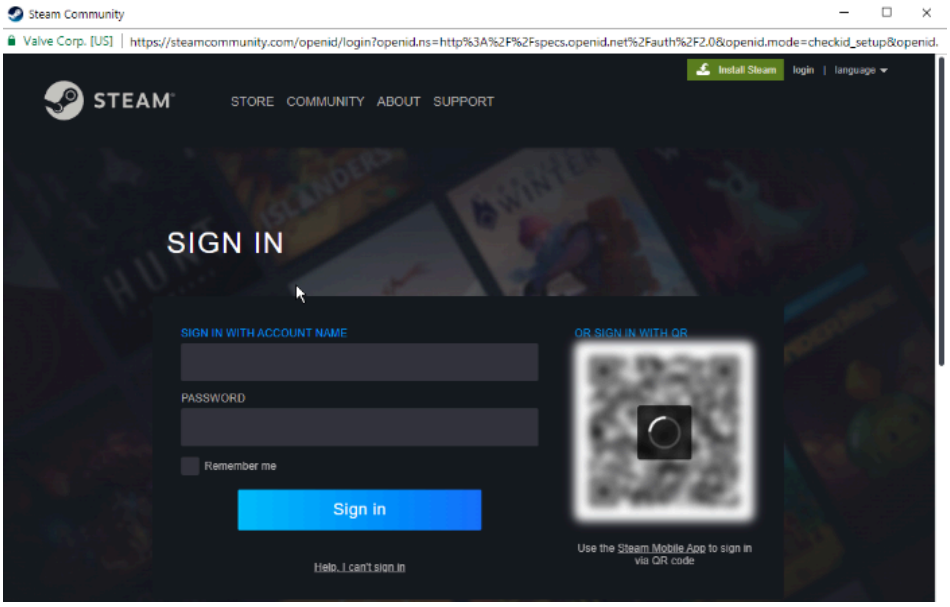
El portal de Steam mencionado anteriormente parecía ser legítimo a simple vista, dado que este contaba con:

- Certificado SSL verificado
- Dominio correcto
- Página de inicio de sesión correcta
- Las URLs del portal falso eran válidas
- No tenía errores gramaticales, *glitches* o relacionados.

Sin embargo, al ingresar las credenciales, el portal regresaba un mensaje de error, asegurando que las credenciales eran incorrectas. Esto debido a que el portal falso no tiene la capacidad de verificar credenciales, sólo de sustraerlas.

Ilustración 10.

Portal falso de inicio de sesión en la plataforma Steam



Nota. Se puede apreciar la el certificado SSL verificado, el dominio y la URL son correctos.

1.2.2.3. Sustitución física de códigos QR legítimos

Al encontrarse físicamente plasmados dentro de un punto de fácil acceso para la población (por ejemplo, un menú QR en un restaurante), los actores maliciosos pueden fácilmente reemplazar un código QR legítimo por uno malicioso. La firma de ciberseguridad, Techguard Security afirma que “los ciberdelincuentes pueden utilizar herramientas de codificación gratuitas disponibles en internet para crear códigos QR. Imprimen el código QR en papel adhesivo y lo colocan sobre un código QR legítimo.” (Techguard Security, 2023)(pf. 11).

1.2.2.4. Publicidad Malintencionada (Malvertising)

Algunas páginas web, así como también revistas (físicas o digitales) suelen brindar espacios para que personas puedan colocar sus anuncios para poder promocionar sus productos y servicios. Sin embargo, las entidades que alquilan estos espacios no suelen verificar la legitimidad de estos. Sobre esto, el portal de seguridad informática Tarlogic comenta:

> “Por ejemplo, a finales de 2023, BlackCat, uno de los grupos de ciberdelincuentes más célebres a nivel global puso en marcha una campaña de malvertising a través de Google Ads. Para ello, diseñó unos anuncios falsos que ofrecían software de índole profesional y empresarial." (Tarlogic, 2024)

1.3. Marco Situacional

1.3.1. Análisis de casos de uso de códigos QR con seguridad integrada

En la presente era digital, los códigos QR han emergido como una herramienta versátil ante diversas situaciones en las que se requiere un método de transferencia rápida de información. Como se mencionó anteriormente, el estado actual de estos códigos bidireccionales es globalizado, llegando a tener cierta omnipresencia dentro de nuestra interacción tecnológica diaria.

Sin embargo, a medida que se ha popularizado (globalizado) el uso de este tipo de código, también se han realizado múltiples estudios para la integración de medidas de seguridad avanzadas, de esta manera se podría prevenir amenazas, tales como: Qhishing, acceso no autorizado y manipulación de datos. Esta sección del presente trabajo investigativo pretende analizar diferentes casos de uso en los que los códigos QR, en conjunto con medidas de seguridad integrada en ellos, juegan un papel vital para salvaguardar y garantizar la protección de los datos de los usuarios.

Un estudio realizado en el 2020 denominado *Beautified QR Code with Security Based on Data Hiding* (Cai, Liu, & Yan, 2019) propone un algoritmo que genera códigos QR embellecidos utilizando un mecanismo de corrección de errores, lo que permite modificar los módulos del código sin comprometer su funcionalidad. A través de esta técnica, se logra mejorar la estética del código QR. Para añadir una capa adicional de seguridad, el código QR verificado se integra en el código embellecido, previniendo así su manipulación.

El método de ocultamiento de datos por el LSB (Least Significant Bit) se emplea para incrustar la imagen original y el código QR verificado en el código embellecido. Los resultados experimentales del estudio muestran que el código QR embellecido, generado mediante el algoritmo propuesto, supera a los métodos de referencia en términos de calidad visual y seguridad.

Este estudio ofrece una solución innovadora que combina la estética y la seguridad en los códigos QR. A través del uso de algoritmos de corrección de errores y técnicas de ocultamiento de datos, se logra mejorar tanto la apariencia visual como la integridad de los datos, lo que es crucial para diversas aplicaciones en sectores críticos.

A pesar de la extensa aceptación global de los códigos QR, estos carecen de mecanismos estándar para garantizar la autenticidad y la confidencialidad del contenido que almacenan. Esta ausencia de estándares de seguridad expone a los usuarios a varios ataques, como la redirección a sitios web maliciosos o la infección de sus dispositivos móviles con malware.

En el comercio y el marketing, los códigos QR con seguridad criptográfica pueden mejorar la confianza del consumidor, garantizando que las promociones y ofertas sean auténticas y protegiendo contra intentos de fraude.

Dentro de este contexto, el estudio titulado *Usable Security for QR Code* (Focardi, Luccio, & Wahsheh, 2019) realiza un análisis sistemático de las primitivas criptográficas modernas dentro de los códigos QR. Este estudio selecciona y compara esquemas criptográficos estándar y populares basándose en su rendimiento, tamaño y seguridad, evaluando cómo diferentes factores de usabilidad afectan el rendimiento de escaneo de los códigos QR y el equilibrio entre la usabilidad y la seguridad de los esquemas criptográficos considerados.

El estudio revela que, aunque los códigos QR pueden ser vulnerables a diversos ataques, la criptografía ofrece primitivas estándar que proporcionan confidencialidad, integridad y autenticidad de los datos. Estos mecanismos criptográficos pueden prevenir la mayoría de los ataques, especialmente en entornos cerrados donde las claves públicas de entidades confiables están claramente establecidas y las claves simétricas pueden intercambiarse de manera segura. Sin embargo, la adopción de criptografía en códigos QR es limitada debido a las restricciones de espacio y al rendimiento de los dispositivos móviles en comparación con los ordenadores personales.

Resultados del estudio

Rendimiento de smartphones

Los smartphones modernos no presentan problemas de rendimiento al realizar operaciones criptográficas típicas, como las firmas digitales, lo cual era una limitación hace algunos años.

Tamaño de los códigos QR

Los códigos QR pueden incrustar hasta aproximadamente 3 KB de datos, permitiendo la inclusión de firmas digitales y certificados. Sin embargo, se identificaron

problemas de usabilidad con códigos QR de gran tamaño en términos de tiempo de escaneo, rango de distancia y la posibilidad de escanear códigos erróneos.

Algoritmos Criptográficos Utilizables

- **ECDSA y RSA:** Utilizando claves pequeñas son usables en códigos QR, incluso cuando se imprimen en tamaños pequeños, como en productos de supermercado.
- **Certificados online:** La inclusión de certificados dentro del código QR genera problemas de usabilidad. Una alternativa viable es descargar certificados en línea a través de HTTPS, almacenándolos en caché para minimizar la necesidad de conectividad.

HMACs y cifrado simétrico (AES)

Ambos métodos son altamente seguros y pueden ser incluidos como cifrados utilizables en códigos QR.

Transmitir información confidencial a través de códigos QR se ha convertido en un tema significativo. Muchos dispositivos móviles utilizan códigos QR para pagos móviles, boletos electrónicos, bonos electrónicos y firmas digitales. Como resultado, la información privada necesita estar protegida contra el escaneo casual. El proceso de ocultación diseñado se basa en la capacidad de corrección de errores de los códigos QR, lo que puede preservar la legibilidad del código QR generado. Los usuarios generales pueden escanear para obtener el contenido de los datos del QR sin ser sospechosos ni atacados maliciosamente por otros.

Debido a esto, en el 2022 se publicó un artículo científico en Entropy, denominado *A Confidential QR Code Approach with Higher Information Privacy* (Lin, Lan, Chen, & Wu, 2022).

Los siguientes resultados se obtuvieron luego de concluir con el estudio:

Ocultación eficiente de información

El enfoque de agrupamiento de triple módulo oculta dos bits confidenciales cambiando solo un módulo del QR. Esto reduce la alteración de los módulos del QR y mejora la capacidad de información confidencial insertada.

Capacidad de información confidencial

La carga útil confidencial del nuevo sistema es el doble de la capacidad de corrección de errores de un código QR, resolviendo el problema de la insuficiencia de la carga útil privada. El rendimiento es superior a los esquemas relacionados.

Legibilidad y seguridad

Los dispositivos de escaneo comunes pueden leer directamente los módulos del QR (incluido el contenido de datos del QR y el secreto cifrado S) del código QR generado. La extracción de S es igual a la operación original del QR, pero el nuevo esquema necesita descifrar S. La encriptación y el descifrado pueden determinarse según los requisitos del sistema, utilizando una función hash unidireccional para reducir la complejidad temporal.

Aplicabilidad

El algoritmo es práctico para varios códigos de barras bidimensionales con capacidades de corrección de errores y puede aplicarse ampliamente en aplicaciones móviles o dispositivos de escaneo debido a su baja complejidad computacional.

1.4. Marco Legal

1.4.1. Ley Orgánica de Telecomunicaciones

La ley Orgánica de Telecomunicaciones de la República del Ecuador tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro

radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2015).

El artículo 77 de esta ley, el cual hace referencia a las Interceptaciones dice:

Únicamente se podrán realizar interceptaciones cuando exista orden expresa de la o el Juez competente, en el marco de una investigación de un delito o por razones de seguridad pública y del Estado, de conformidad con lo que establece la ley y siguiendo el debido proceso. En caso de interceptación legal, las y los prestadores de servicios deberán proveer toda la información requerida en la orden de interceptación, incluso los datos de carácter personal de los involucrados en la comunicación, así como la información técnica necesaria y los procedimientos para la descomprensión, descifrado o decodificación en caso de que las comunicaciones objeto de la interceptación legal hayan estado sujetas a tales medidas de seguridad.

Los contenidos de las comunicaciones y los datos personales que se obtengan como resultado de una orden de interceptación legal estarán sujetos a los protocolos y reglas de confidencialidad que establezca el ordenamiento jurídico vigente. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2015).

1.4.2. Ley Orgánica de Protección de Datos Personales

El objetivo de esta ley es garantizar el derecho que tienen todos los ciudadanos ecuatorianos a que se resguarden sus datos personales, a poder acceder libremente a dicha información y a decidir sobre ella. Para esto, la Ley “regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela”. (Banco Pichincha, 2022).

Dentro de esta ley, el capítulo V, artículo 33, toma en consideración el tratamiento de los datos personales de los usuarios:

Art. 33: Transferencia o comunicación de datos personales.- Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia. (Asamblea Nacional de la República del Ecuador, 2021)

Dentro del capítulo VI, se discute la seguridad de los datos personales. Los artículos aplicables para este trabajo investigativo son:

Art. 37: Seguridad de datos personales. El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos. (Asamblea Nacional de la República del Ecuador, 2021)

Art. 39: Protección de datos personales desde el diseño y por defecto. Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento. (Asamblea Nacional de la República del Ecuador, 2021)

Art. 43: Notificación de vulneración de seguridad. El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella. (Asamblea Nacional de la República del Ecuador, 2021)

Capítulo 2: Metodología del Proceso de Investigación

2. Metodología del Proceso de Investigación

2.1. Enfoque de la investigación

Se ha optado por la utilización de un enfoque de investigación aplicada tecnológica, dado que se encuentra enfocada a encontrar diversas estrategias para poder lograr un objetivo propuesto y ponerlo en marcha. En síntesis, resolver un problema aplicando recursos tecnológicos.

Sobre este enfoque, Lozada (2014) agrega que:

> "La investigación aplicada busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto." (Lozada, 2014)

2.2. Alcance de investigación

2.2.1. Alcance exploratorio

El presente trabajo investigativo tiene como objetivo el desarrollar un enfoque que pueda mejorar la seguridad y la integridad de los datos al examinar los impactos potenciales de este código, lo que dará como resultado una transferencia de información más segura. El objetivo principal de este estudio exploratorio es identificar y abordar estos problemas mediante la utilización de un código QR que incorpore sólidas medidas de seguridad.

La aplicación del alcance exploratorio es fundamental en este caso, dado que facilita la compresión de la naturaleza de esta problemática debido a la falta de trabajos investigativos de la misma (o similar) índole, bajo el contexto nacional. Este enfoque permite descubrir nuevas perspectivas, identificar variables clave y desarrollar un

prototipo que, se espera, servirá como base para proyectos, investigaciones, y desarrollos posteriores en este campo.

2.2.2. Alcance descriptivo

De la misma manera, este trabajo investigativo adopta un alcance descriptivo con el objetivo de identificar la postura de los encuestados sobre la información que escanean mediante códigos QR. Así mismo, se busca conocer más sobre su frecuencia de uso (frecuencia de escaneos de códigos QR), si poseen o no conocimiento acerca del *Quishing*, si los usuarios poseen alguna herramienta para el escaneo de códigos QR, y los requisitos y expectativas de los usuarios potenciales sobre la aplicación. La información recopilada a través de la encuesta servirá para moldear el prototipo del aplicativo; no sólo enfocándose en el apartado del diseño, sino también en las funcionalidades técnicas de este.

2.3. Delimitación de la investigación

2.3.1. Alcance del prototipo

El prototipo de desarrollo, producto de este trabajo de investigación, permitirá que los usuarios de dispositivos móviles Android generen y escaneen códigos QR cifrados o no cifrados.

La aplicación móvil resultante deberá poder generar y escanear códigos QR (cifrados o no). Adicionalmente, tendrá que cifrar el mensaje de forma rápida y eficaz, sin sacrificar la robustez de las medidas de seguridad integradas. A posteriori, el mensaje resultante de los procesos de cifrado será transcrito a un código QR.

Para efectuar aquello, se han implementado medidas de seguridad, siendo el principal aspecto a destacar la utilización del cifrado AES (Advanced Encryption Standard), adicionando un vector de iniciación aleatorio (*IV*, por sus siglas en inglés) y la

implementación del cifrado AES en modo CBC (*Cipher-Block Chaining* o Cadena de Cifrado en Bloques).

Como último punto, el prototipo deberá ser capaz de escanear el código QR (cifrado o no), y, de ser el caso, descifrarlo.

2.3.2. Restricción del sistema

El desarrollo del prototipo presenta ciertas restricciones, siendo algunas impuestas por el Marco Legal. Se han identificado las siguientes restricciones:

- La aplicación debe poder generar y escanear códigos QR rápida y eficazmente.
- La aplicación debe contar con una interfaz gráfica sencilla y de fácil uso.
- Las medidas de seguridad implementadas durante el desarrollo del prototipo deben ser seguras y robustas.
- El prototipo no enviará datos de usuarios de ninguna índole. Los datos que se generen mediante el uso de aplicativo son de uso y responsabilidad exclusiva usuario.

2.3.3. Población y muestra de la investigación

Se ha optado por limitar la población a los estudiantes de la Universidad Tecnológica Ecotec, campus Samborondón.

La muestra se centrará en los estudiantes que se encuentren cursando las carreras de: Ingeniería en Software, Ingeniería en Tecnologías de la información e Ingeniería en Sistemas.

El estudio se llevó a cabo durante un periodo de 6 meses, desde diciembre hasta junio del presente año. Los primeros cuatro meses fueron utilizados para recolectar información de los estudiantes mediante encuestas, en donde se llega a conocer más sobre la frecuencia de uso de códigos QR, y demás; esto con la finalidad

de: 1. Evaluar la fiabilidad del presente trabajo investigativo, y 2. Desarrollar un aplicativo que cumpla con las expectativas de los estudiantes, basado en sus necesidades. Dentro de este mismo periodo se realizó el análisis de la retroalimentación proporcionada por los estudiantes, lo cual dio marcha al diseño de la interfaz gráfica, análisis y desarrollo del aplicativo, así como también a las pruebas prácticas. La cantidad de estudiantes pertenecientes a las carreras previamente mencionadas se muestran en la siguiente tabla:

Tabla 3.

Cantidad de estudiantes pertenecientes a las carreras de Ing. en Software, Tecnologías de la información, y Sistemas de la Universidad Tecnológica Ecotec.

Carrera	Cantidad de estudiantes por carrera
Ingeniería en Software	121
Tecnologías de la Información	43
Ingeniería en Sistemas	39
Total de estudiantes por carrera	203

Nota. Número de estudiantes aproximados basado en la Rendición de Cuentas 2023 de la (Universidad Tecnológica Ecotec, 2024).

Para determinar el tamaño de la muestra, se utilizó la siguiente fórmula:

Ecuación 1.

Fórmula para determinar la muestra, basada en una población finita

$$\mathbf{n} = \frac{Z^2 . p . q . N}{NE^2 + Z^2 \; p . q .}$$

Nota. Se muestra la fórmula para determinar la muestra de una población finita. En este caso, se definen las variables como: **n** (Tamaño de la muestra), Z (Nivel de confianza, 95%), p (Probabilidad a favor), q (Probabilidad en contra), N (Población), E (Error de estimación)

2.3.3.1. Cálculo de la muestra

Nivel de confianza: Z=1.96

Probabilidad a favor: p=0.5p = 0.5p=0.5

Probabilidad en contra: q=1−p=0.5q = 1 - p = 0.5q=1−p=0.5

Tamaño de la población: N=203N = 203N=203

Error de estimación: E=0.05E = 0.05E=0.05

Lo cual resultaría en un tamaño de muestra de 134 personas.

2.3.4. Métodos empleados

2.3.4.1. Cuestionario

Se diseñó un cuestionario con preguntas cerradas para recopilar información cuantitativa sobre las percepciones de los estudiantes pertenecientes a la Universidad Tecnológica Ecotec (campus Samborondón) que se encuentren cursando las carreras de: Ingeniería en Software, Ingeniería en Tecnologías de la información e Ingeniería en Sistemas, utilizando escalas de Likert para medir la intensidad de acuerdo o desacuerdo con afirmaciones específicas relacionadas con la seguridad y la efectividad percibida de un código bidireccional con seguridad integrada para asegurar la protección de los datos durante el proceso de escaneo y transferencia de información. Adicionalmente, ciertas preguntas están orientadas a identificar lo que los usuarios potenciales valorarían más del aplicativo, pudiendo enforcase en aspectos tales como: rendimiento

del aplicativo, su diseño, su facilidad de uso, entre otros. El cuestionario completo se encuentra adjunto en el capítulo 7.1 perteneciente a Anexos.

2.4. Procesamiento y análisis de la información

2.4.1. Metodología aplicada

El presente trabajo investigativo aplicó la metodología Kanban, combinada con Personal Scrum.

Adicionalmente, el trabajo de investigación presenta cuatro fases para el desarrollo del aplicativo del escaneo y generación de código QR con seguridad integrada, las cuales se encuentran detalladas a continuación.

2.4.2. Fase I: Planificación

Durante esta fase inicial, se evalúa la viabilidad del sistema con base en los objetivos planteados anteriormente.

2.4.2.1. Entorno de desarrollo

Se define “Entorno de desarrollo” a toda información relacionada a los requisitos de software y hardware que conforman el ambiente donde se procederá con el desarrollo del prototipo.

2.4.2.2. Análisis de hardware

Evaluación de los recursos disponibles, estos recursos pueden ser de carácter tecnológico, como el análisis de las herramientas de desarrollo, así como también financiero (para la compra de los equipos necesarios).

Los recursos físicos destinados para este proyecto de investigación fueron:

- Laptop:
    - Modelo: Lenovo IdeaPad 3

- Sistema Operativo: Windows 11 Home Edition
- CPU: Ryzen 5 6600H
- GPU: NVDIA 3050 4GBs
- RAM: 16GBs DDR4 SODIMM
- Almacenamiento: 2 discos NvME de 1 TB cada uno.

- Teléfono Móvil 1:
  - Modelo: Samsung Galaxy Flip 4
  - Versión de Android: 14 (API 34)
  - CPU: Snapdragon 8+ Gen 1, 3.18 GHz
  - GPU: Adreno 730
  - RAM: 8 GBs
  - Kernel: 5.10.168
- Teléfono Móvil 2:
  - Modelo: Redmi Note 12
  - Versión de Android: 13 (API 33)
  - CPU: Snapdragon 685
  - GPU: Adreno 619
  - RAM: 4GBs
  - Kernel: 5.15.78

2.4.2.3. Análisis de software

El entorno de desarrollo empleado durante el desarrollo de este aplicativo será Android Studio. Esta IDE fue seleccionada por la gran cantidad de documentación disponible en línea, además de contar con un emulador de dispositivos móviles Android, lo cual simplificaría las pruebas y correcciones de errores.

Las versiones de Android Studio y complementos se detallan a continuación:

- Android Studio versión 2024.1
- Android SDK: 31 (Android 12)

El lenguaje de desarrollo utilizado para este trabajo investigativo fue Java. La elección de este lenguaje se debe a las extensas librerías existentes, así como también una amplia documentación.

2.4.2.4. Asesoramiento con expertos

Se realizaron consultas breves con expertos en ciberseguridad y desarrollo de software para obtener recomendaciones sobre cómo satisfacer las necesidades de seguridad en la aplicación propuesta, para de esta manera poder mitigar las vulnerabilidades existentes sin sacrificar la rapidez del proceso de escaneo característico de los códigos QR.

De esta manera se pudieron emplear mejores prácticas al momento de diseñar el aplicativo y trabajar en su codificación. De la misma forma, se obtuvo constante retroalimentación sobre el trabajo propuesto.

Finalmente, el prototipo fue sujeto de diversas pruebas con el fin de garantizar la efectividad de la seguridad integrada en el código, y la robustez del sistema prototipo en general.

2.4.3. Fase II: Análisis y desarrollo

La segunda fase de la investigación se centra en la metodología de desarrollo de software y el análisis detallado de los componentes necesarios para el desarrollo del prototipo.

El presente trabajo investigativo implementa la metodología Kanban, dado que la visualización de las fases del trabajo ayudará a conocer el estado en el que se encuentra; se busca organizar el tablero de tareas por columnas, las cuales sirven para

representar cada etapa del trabajo. De la misma manera, esta metodología también permite la organización de la carga del trabajo, asignando prioridades a las diferentes tareas a conveniencia.

2.4.3.1. Metodología Kanban

Se crea un tablero Kanban para visualizar el flujo de trabajo y gestionar las tareas de manera efectiva. El tablero tendrá columnas que representen las diferentes etapas del desarrollo (por ejemplo: "Por hacer", "En progreso", "En revisión", "Completado").

Adicionalmente, se implementarán límites de trabajo en progreso (WIP) para asegurar un flujo constante y evitar la sobrecarga.

Paso 1: Creación de un tablero Kanban.

Se establece un tablero Kanban virtual para visualizar de manera clara, precisa, y organizada las tareas relacionadas con el desarrollo del código bidireccional con seguridad integrada.

Paso 2: Definición de las etapas del flujo de trabajo.

Las etapas del flujo de trabajo incluyen: "Por Hacer", "En Progreso" y "Completado". Dado que el proyecto implica tareas en secuencia, se utilizan porcentajes para indicar el avance de cada sprint específico.

Paso 3: Priorizar y asignar Tareas.

Las tareas se organizarán basadas en su importancia dentro del contexto del proyecto. Esto garantiza que las actividades críticas tengan mayor prioridad y se completen en los tiempos previstos.

Paso 4: Visualización de etiquetas de progreso.

El tablero Kanban permitirá visualizar el progreso de las tareas a medida que se mueven por medio de etiquetas, como, por ejemplo: "Por Hacer" a "En Progreso" y finalmente a "Completado". Esta visualización será crítica para mantener el seguimiento de cada actividad, de esta manera se asegura que los objetivos establecidos sean cumplidos.

Paso 5: Establecer límites para tareas en progreso.

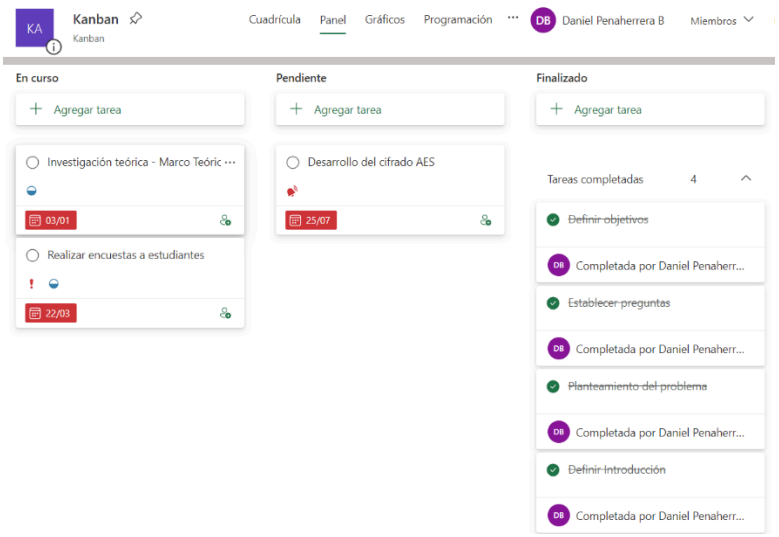
Se establecerán límites claros en la columna "En Progreso" para evitar la sobrecarga de trabajo. Esto asegurará que el proyecto avance paulatinamente, asignando un número manejable de tareas a la vez.

Paso 6: Revisión y mejora continua.

Regularmente, se revisará el tablero Kanban para identificar posibles cuellos de botella o áreas donde se pueda mejorar la eficiencia del desarrollo. Estas revisiones continuas permitirán ajustar y optimizar el proceso de trabajo conforme avance el proyecto.

Ilustración 11.

Tablero Kanban con tareas añadidas



Nota. Elaborado por: Autor.

2.4.3.2. Android Studio

Android Studio es el entorno de desarrollo integrado (IDE) oficial que se usa en el desarrollo de apps para Android. *(Android Developers, s.f.)*

2.4.3.3. **Desarrollo del prototipo**

El código importa ciertas librerías y componentes ya conocidos. Sin embargo, se destaca la utilización de zebra crossing, una librería utilizada para el manejo y creación de códigos de barras y QR.

Ilustración 12.

Importación de librerías y componentes

```
import com.google.android.material.textfield.TextInputEditText;
import com.google.android.material.textfield.TextInputLayout;
import com.google.zxing.BarcodeFormat;
import com.google.zxing.MultiFormatWriter;
import com.google.zxing.WriterException;
import com.google.zxing.common.BitMatrix;
import com.journeyapps.barcodescanner.BarcodeEncoder;
```

Nota. Elaborado por: Autor.

2.4.3.3.1. Disposición de los botones

Tal como se mostró en el diseño original, la disposición de mantiene un diseño botones básico e intuitivo, lo cual asegura la rápida respuesta por parte del aplicativo al momento de usarlo.

Ilustración 13.

Extracto de código en donde se disponen los botones

```
<TextView
    android:id="@+id/button_create"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:layout_below="@id/encrypt"
    android:layout_alignParentRight="true"
    android:layout_marginTop="10dp"
    android:background="@drawable/button_state"
    android:drawableLeft="@drawable/ic_qr_code_app"
    android:gravity="center"
    android:padding="10dp"
    android:text="Generar QR antes de cifrado" />
```

Nota. La disposición de los botones mantiene un diseño simple para no afectar el rendimiento del aplicativo.

2.4.3.3.2. Extracto de dependencias y compatibilidad

El proyecto está compilado por medio de una API nivel 31 (Android 12), el sistema operativo mínimo aceptado es Android 5.0 (Lollipop), siendo la aplicación diseñada para Android 12. Actualmente, el proyecto se encuentra en su primera versión.

Ilustración 14.

Dependencias y compatibilidad del proyecto

```
android {
    compileSdk 31

    defaultConfig {
        applicationId "com.example.scannerqrfinal"
        minSdk 21
        targetSdk 31
        versionCode 1
        versionName "1.0"

        testInstrumentationRunner "androidx.test.runner.AndroidJUnitRunner"
    }
```

Nota. Elaborado por: Autor.

2.4.3.3.3. Extracto de conversión de texto plano a código QR no encriptado

El siguiente extracto muestra cómo se convierte el texto añadido por el usuario en un código QR, mostrado en '*imageview*'

Ilustración 15.

Conversión de texto a código QR

```
buttonCreateQR.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View view) {
        if (!inQRCode.getText().toString().isEmpty()) {
            try {
                MultiFormatWriter multiFormatWriter = new MultiFormatWriter();
                BitMatrix bitMatrix = multiFormatWriter.encode(inQRCode.getText()
                BarcodeEncoder barcodeEncoder = new BarcodeEncoder();
                Bitmap bitmap = barcodeEncoder.createBitmap(bitMatrix);
                imageQR.setImageBitmap(bitmap);
```

Nota. Elaborado por: Autor.

2.4.3.3.4. Extracto de encriptado de texto

El siguiente extracto muestra cómo el texto añadido por el usuario se encripta utilizando el método '*crypto.encrypt()'.*

Ilustración 16.

Cifrado del texto plano

```
button_encrypt.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View view) {
        if (!inQRCode.getText().toString().isEmpty()) {
            try {
                String encryptedText = Crypto.encrypt(inQRCode.getText().toString());
                in_encrypt.setText(encryptedText);
```

Nota. Elaborado por: Autor.

2.4.3.3.5. Extracto de generación de texto plano a código QR cifrado

En esta opción, el usuario puede transformar su texto plano a código QR cifrado luego de presionar el botón '*Encrypt'*. Después de presionar ese botón, el texto se encontrará cifrado utilizando el método '*crypto.encrypt*'

Ilustración 17.

Generación de texto plano a código QR con mensaje cifrado

```
button_create_encrypt_qr.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View view) {
        if (!in_encrypt.getText().toString().isEmpty()) {
            try {
                MultiFormatWriter multiFormatWriter = new MultiFormatWriter();
                BitMatrix bitMatrix = multiFormatWriter.encode(in_encrypt.getText()
                BarcodeEncoder barcodeEncoder = new BarcodeEncoder();
                Bitmap bitmap = barcodeEncoder.createBitmap(bitMatrix);
```

Nota. Elaborado por: Autor.

2.4.3.3.6. Extracto de implementación de cifrado AES

El cifrado implementado en el desarrollo del aplicativo es AES 128-bits, esto con la finalidad de mantener la fluidez del código QR con mensaje cifrado, sin comprometer la seguridad de la información que contiene.

Dentro del siguiente extracto del código se puede apreciar la lógica general de la encriptación.

Ilustración 18.

Cifrado AES 128-bits

```
private static byte[] encrypt(byte[] raw, byte[] clear) throws Exception {
    SecretKey skeySpec = new SecretKeySpec(raw, "AES");
    Cipher cipher = Cipher.getInstance("AES");
    cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
    return cipher.doFinal(clear);
}
```

Nota. Elaborado por: Autor.

De la misma manera, el aplicativo es capaz de descifrar los códigos QR (cifrados) que se han generado con esta misma aplicación.

Ilustración 19.

Lógica del descifrado AES 128-bits

```
private static byte[] decrypt(byte[] encrypted) throws Exception {
    SecretKey skeySpec = new SecretKeySpec(keyValue, "AES");
    Cipher cipher = Cipher.getInstance("AES");
    cipher.init(Cipher.DECRYPT_MODE, skeySpec);
    return cipher.doFinal(encrypted);
}
```

Nota. Elaborado por: Autor.

2.4.4. Fase III: Diseño

2.4.4.1. Requisitos del diseño

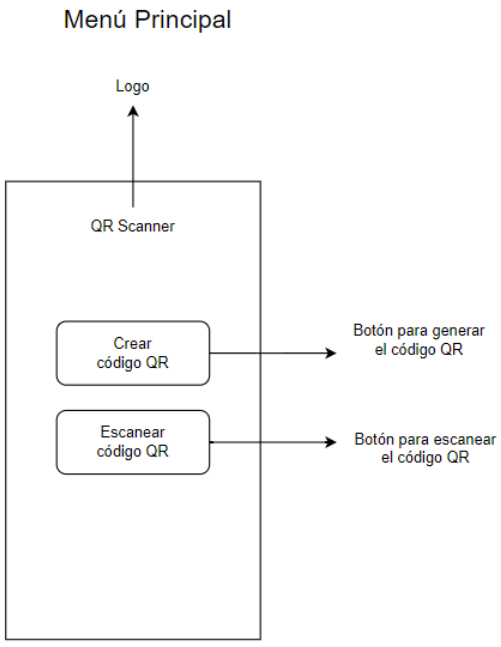
Gracias a las encuestas realizadas, se descubrió una tendencia en la muestra referente a la preferencia en la interfaz de usuario. La encuesta reveló que los usuarios gustan de una aplicación sencilla y que sea fácil de usar.

Los primeros bocetos del diseño del aplicativo fueron realizados en la plataforma de diseño gratuita denominada Draw.io.

Esta herramienta gratuita es utilizada para crear diagramas (de procesos, flujos, entre otros) de manera online (web) u offline (aplicación de escritorio). Algunas de sus funcionalidades incluyen la creación de bibliotecas personalizadas, inclusión de metadatos en diagramas, entre otras.

Ilustración 20.

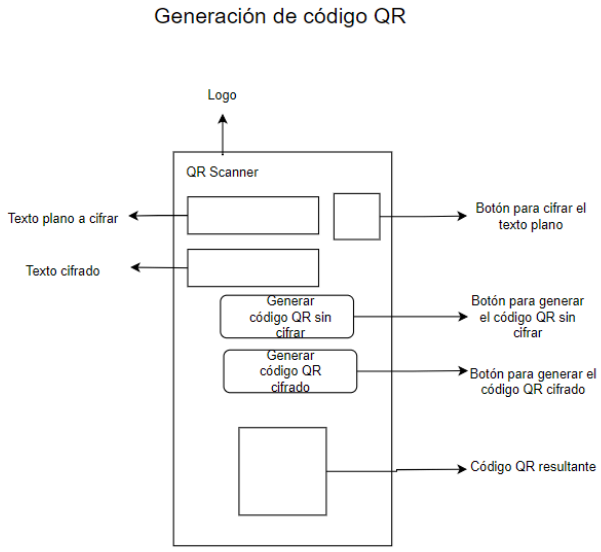
Diseño inicial del menú principal



Nota. Elaborado por: Autor.

Ilustración 21.

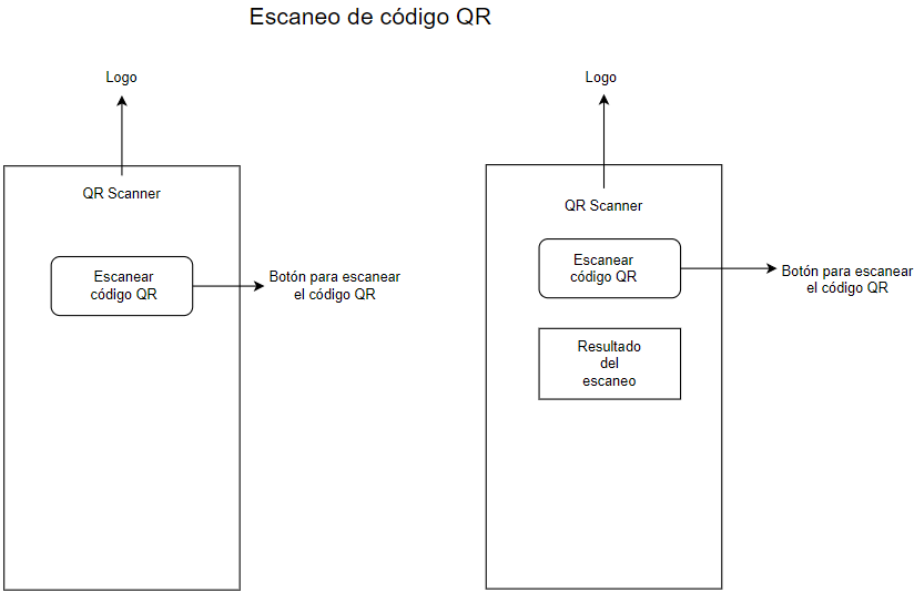
Diseño inicial de la pantalla de generación de códigos QR



Nota. Elaborado por: Autor.

Ilustración 22.

Diseño inicial de la función “Escanear código QR”



Nota. La ilustración de la izquierda muestra el proceso inicial del escaneo, el texto escaneado resultante se muestra en la ilustración derecha. Elaborado por: Autor.

2.4.4.2. Diseño de la interfaz gráfica

El prototipo presenta una interfaz gráfica muy sencilla e intuitiva. Esto asegura la fluidez de ejecución de los componentes de la aplicación dado que no deberá ejecutar ningún otro complemento que requiera de gran cantidad de recursos.

Tomando en consideración lo anteriormente expuesto, se ha llevado a cabo la creación de tres pantallas distintas para este prototipo, estas son:

1. Menú principal
2. Generar código QR Cifrado - Generación
3. Escanear código QR Cifrado - Lectura

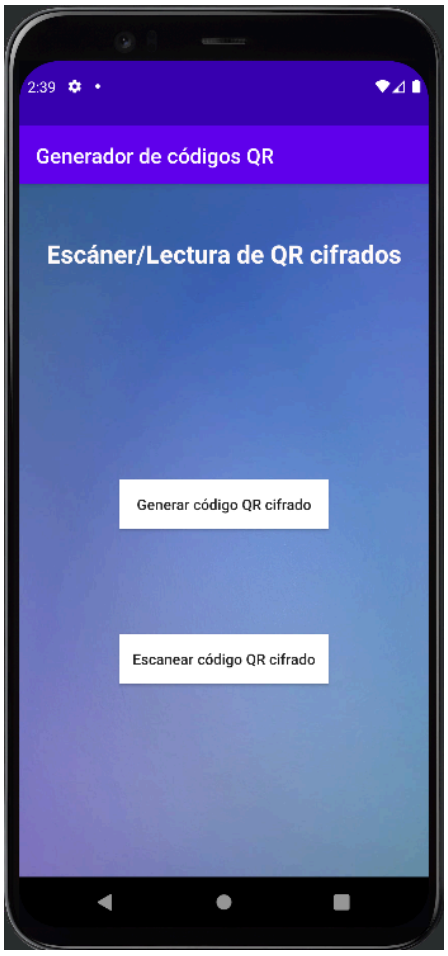
2.4.4.2.1. Menú Principal

El menú principal presenta un encabezado con el nombre del proyecto, seguido por un título. En el centro, presenta dos botones. Cada uno de estos botones redirigirá

al usuario a las siguientes pantallas establecidas, dependiendo del requerimiento de este.

Ilustración 23.

Menú principal



Nota. Menú principal del prototipo. Elaborado por: Autor

2.4.4.2.2. Generar código QR cifrado - Generación

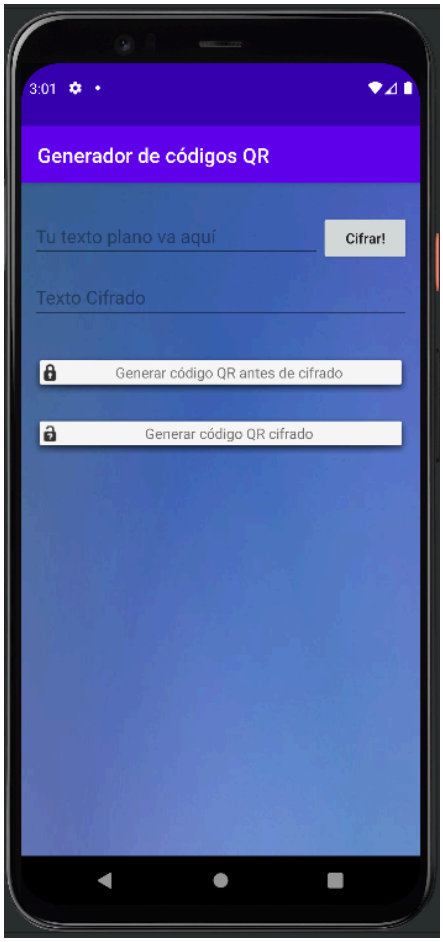
Esta pantalla muestra cómo el usuario podrá insertar el mensaje que desea añadir a un código QR, utilizando el campo “Tu texto plano va aquí” y generarlo presionando “Cifrar”.

Alternativamente, se ha incluido una función para que el usuario pueda generar un código QR sin ningún tipo de cifrado. Esto con la finalidad de poder observar las diferencias al aplicar o no el cifrado. Si el usuario desea hacer uso de esta función, sólo debe incluir el texto en el campo “Tu texto plano va aquí” y generar el QR no cifrado presionando “Generar código QR antes de cifrado”.

Sin embargo, si el usuario desea que su código QR resultante se encuentre cifrado, debería ingresar el texto deseado en el campo “Tu texto plano va aquí”, presionar en “Cifrar” (lo cual hará que el texto ingresado pase de ser texto plano a texto cifrado), y presionar en “Generar código QR cifrado”.

Ilustración 24.

Generar código QR cifrado



Nota. La ilustración muestra la pantalla de generación de códigos QR en donde el usuario podrá generar códigos QR con base en el texto plano ingresado.

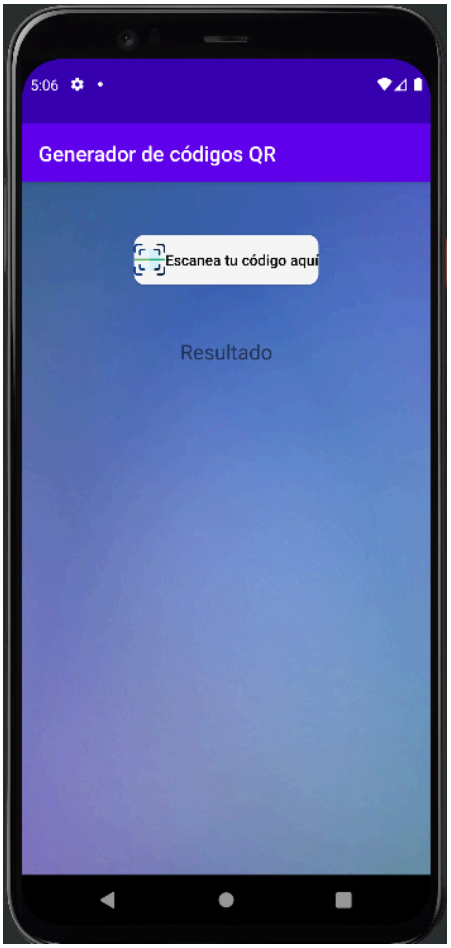
2.4.4.2.3. Escanear código QR cifrado – Lectura

Esta pantalla brinda al usuario la funcionalidad de escanear el QR, ya sea este cifrado o no. Si el usuario desea escanear el código generado, basta con acercar el dispositivo móvil al código QR. Una vez realizado con éxito, el aplicativo muestra la información desencriptada en el campo “Resultado”.

Si el usuario cancela la operación de escaneo, se muestra un mensaje de error.

Ilustración 25.

Escanear código QR cifrado – Lectura



Nota. Interfaz gráfica de la pantalla de escaneo de códigos QR. Elaborado por: Autor.

2.4.5. Fase IV: Evaluación y resultados del proyecto

Durante esta última fase metodológica, se pone a prueba el prototipo desarrollado y se dan a conocer los resultados. Las pruebas son ejecutadas con la finalidad de evaluar el correcto funcionamiento del prototipo.

Adicionalmente, el presente trabajo investigativo cuenta con evaluaciones por parte de expertos en el área. Las variables a calificar se basan en la funcionalidad el aplicativo, así como la suficiencia, compatibilidad, interacción, entre otros.

Como último punto, las pruebas realizadas utilizando diferentes componentes de seguridad se encuentran documentados y referenciados en la sección 7.3 de Anexos.

2.4.5.1. **Prueba funcional: Generar códigos QR**

La primera prueba se basa en la generación de códigos QR. Para acceder a esta funcionalidad desde el Menú Principal, el usuario simplemente debe presionar en “Generar código QR cifrado”, lo cual lo llevará a la pantalla respectiva.

Una vez en la pantalla de generación, el usuario puede insertar un mínimo de un carácter hasta una cantidad máxima de 1200 caracteres.

2.4.5.1.1. **Generar código QR cifrado**

Una vez que el usuario haya insertado por lo menos un carácter en el campo “Tu texto plano va aquí”, deberá presionar en “Cifrar!”, lo cual cifra el texto plano.

Para generar el código QR, ya contando con el texto cifrado, el usuario debe presionar en “Generar código QR cifrado”.

En la siguiente demostración haremos uso del texto: “Hola a todos!” para la generación del QR cifrado que incluirá el mensaje cifrado.

Ilustración 26.

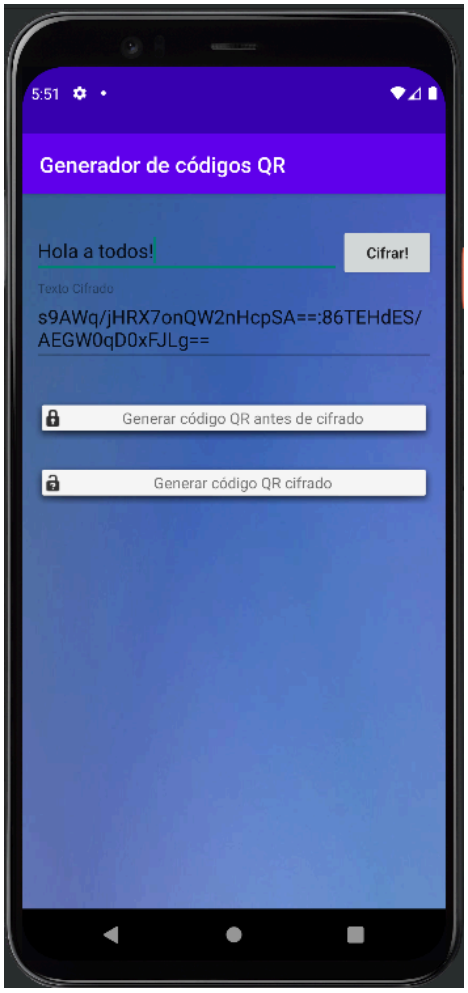
Prueba de generación de código QR con mensaje cifrado

Nota. Elaborado por: Autor

Una vez contando con el texto plano ingresado en el campo, se procede a presionar el botón “Cifrar!”.

Ilustración 27.

Prueba de generación de código QR con mensaje cifrado #2



Nota. Elaborado por: Autor.

Como se aprecia en la imagen anterior, el texto plano “Hola a todos!” ha pasado por un proceso de cifrado, el cual ha dado como resultado a la cadena de caracteres que se pueden apreciar en el campo “Texto Cifrado”.

La siguiente prueba se basa en la generación del QR a partir del texto cifrado, generando así un QR con un mensaje cifrado.

Ilustración 28.

Prueba de generación de código QR con mensaje cifrado #3

Nota. Elaborado por: Autor

La ilustración previa muestra cómo el prototipo ha sido capaz de generar un código QR con el mensaje cifrado, partiendo desde un mensaje en texto plano, pasando por el método de cifrado, y finalmente generando el código QR que incluya el mensaje cifrado.

Hasta este paso, se ha demostrado la funcionalidad de la generación de códigos QR con mensajes cifrados del prototipo.

2.4.5.1.2. **Generar códigos QR sin mensaje cifrado**

Haciendo uso del mismo texto plano, se procede a generar un código QR que no se posea un mensaje cifrado.

Ilustración 29.

Generar códigos QR sin mensaje cifrado

Nota. El código QR se generó sin cifrado. De esta manera, puede ser leído por cualquier persona que tenga acceso a este código.

La imagen anterior confirma que, efectivamente, la aplicación ha sido capaz de generar un código QR sin necesidad de pasar por el algoritmo de cifrado. Dicho esto, se demuestra la funcionalidad del aplicativo a la hora de generar códigos QR, tanto cifrados como sin cifrado alguno.

2.4.5.2. **Prueba funcional: Lectura de códigos QR**

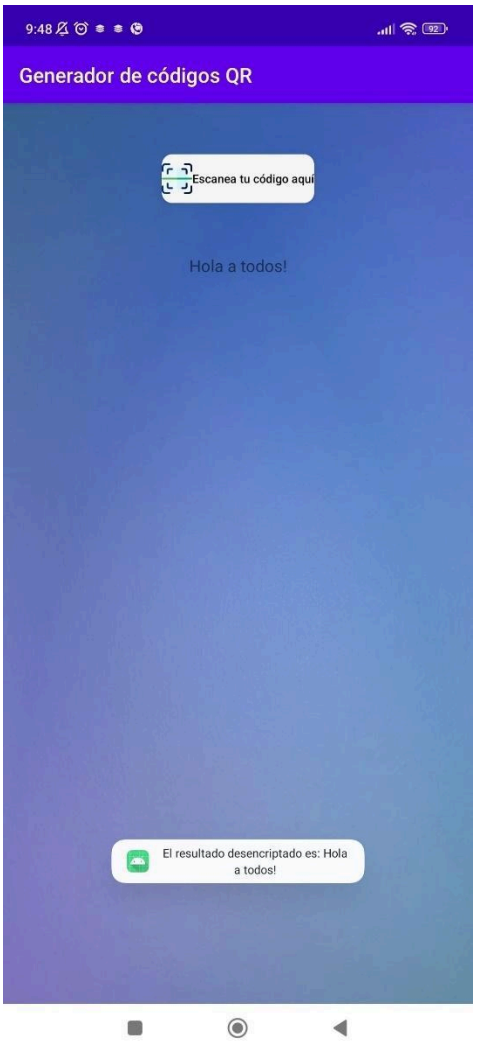
Las pruebas realizadas a continuación consisten en la lectura de los códigos QR generados desde el aplicativo.

2.4.5.2.1. **Lectura de códigos QR cifrados**

Para la realización de esta prueba, se reutilizaron los códigos generados durante el proceso de generación de códigos QR con mensaje cifrado.

Ilustración 30.

Lectura de códigos QR cifrados



Nota. Elaborado por: Autor

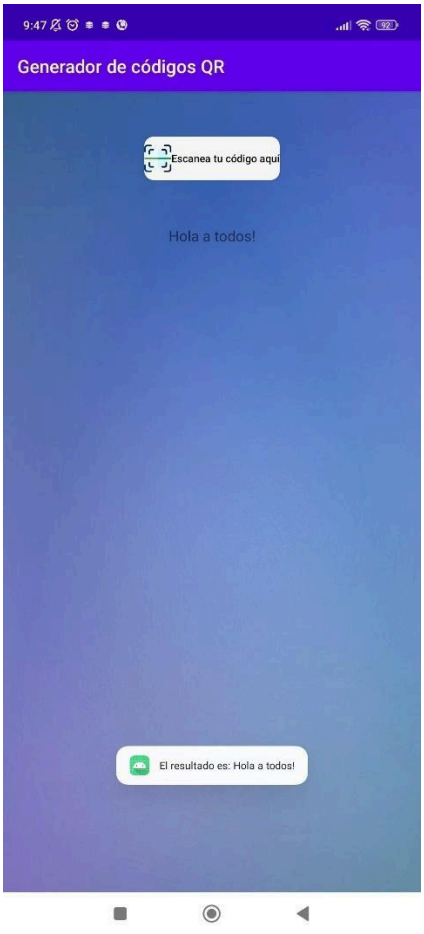
Como se puede verificar, el aplicativo es capaz de diferenciar cuando el código QR escaneado se encuentra cifrado, añadiendo el texto: “El resultado desencriptado es:” en el primer caso.

2.4.5.2.2. **Lectura de códigos sin cifrar**

Como última parte de las pruebas funcionales, se realizará el escaneo del código QR sin cifrar. Esto con la finalidad de detectar si el aplicativo es realmente capaz de diferenciar entre un código QR con un mensaje cifrado y no cifrado durante el escaneo.

Ilustración 31.

Lectura de código QR sin cifrar



Nota. Elaborado por: Autor

La ilustración anterior muestra cómo el prototipo es capaz de reconocer el código QR no cifrado, mostrando el mensaje incluido en él.

2.4.5.3. **Conclusiones de pruebas funcionales**

Durante la realización de estas pruebas, se han analizado las funcionalidades que tiene el prototipo y cómo este último ha demostrado, satisfactoriamente, los resultados esperados.

En el transcurso de la fase de generación del código QR, se ha demostrado que el aplicativo es capaz de generar códigos QR, ya sean cifrados o no. Por su parte, la fase de escaneo funciona como se espera; dado que, además de poder mostrar la información insertada en el código QR (sea cifrado o no), es capaz de identificar si el código escaneado se encuentra cifrado o no.

2.4.5.4. **Pruebas de rendimiento**

Luego de efectuar las pruebas de funcionalidad, el siguiente criterio a evaluar será el rendimiento general del prototipo. Estas pruebas consistirán en la medición de la variable (T = tiempo), basándose en la cantidad de tiempo que toman las diferentes funcionalidades del aplicativo hasta ejecutar sus tareas satisfactoriamente.

2.4.5.4.1. **Cifrado del mensaje a partir de texto plano**

Durante la primera prueba, se medirá el tiempo que le toma al aplicativo generar texto cifrado a partir de texto plano.

Debido a esto, se realizaron las pruebas con mensajes de longitud variable. Los resultados se muestran a continuación:

Tabla 4.

Tiempo de generación de texto plano a texto cifrado

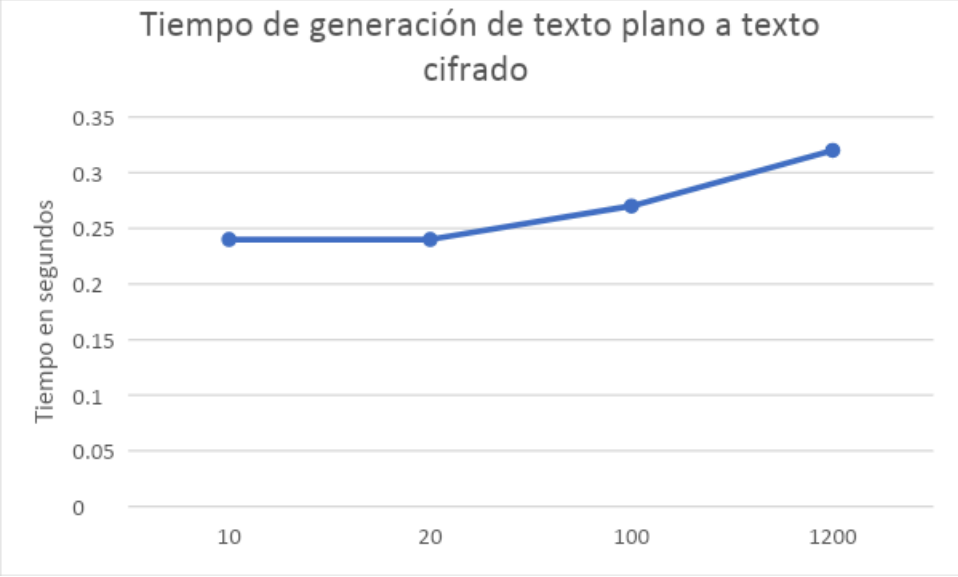
Cantidad de caracteres	Tiempo
10 caracteres	0,24 segundos
20 caracteres	0,24 segundos
100 caracteres	0,27 segundos
1200 caracteres	0,30 segundos

Nota. Tiempo que le toma al prototipo en convertir el texto plano a texto cifrado.

Elaborado por: Autor

Ilustración 32.

Tiempo de generación de texto plano a texto cifrado



Nota. Tabla que muestra el tiempo de que toma transformar el texto plano en texto cifrado, basándose en la cantidad de caracteres insertados. Elaborado por: Autor.

Los resultados reflejan que existe una relación directa entre la cantidad de caracteres ingresados y el tiempo que le toma al aplicativo cifrar el texto plano y presentarlo. Al ingresar la cantidad máxima de caracteres, el tiempo que le toma al aplicativo se encuentra en 0.30 segundos.

2.4.5.4.2. **Generación del código QR sin mensaje cifrado**

La siguiente prueba busca mostrar el tiempo que le toma al prototipo durante la generación del código QR, sin la utilización de cifrado.

Tabla 5.

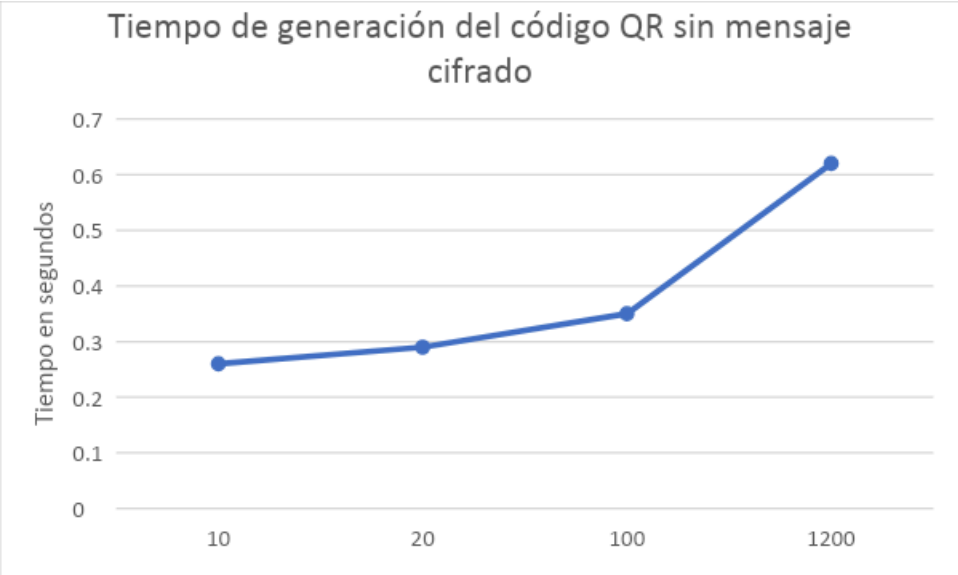
Tiempo de generación del código QR sin mensaje cifrado

Cantidad de caracteres	Tiempo
10 caracteres	0,26 segundos
20 caracteres	0,29 segundos
100 caracteres	0,35 segundos
1200 caracteres	0,62 segundos

Nota. Elaborado por: Autor.

Ilustración 33.

Tiempo de generación del código QR sin mensaje cifrado



Nota. Elaborado por: Autor

Los resultados de la prueba muestran que aún existe una relación directa entre la cantidad de caracteres ingresados y el tiempo que le toma al aplicativo generar un código QR sin cifrar.

Sin embargo, cabe destacar que el tiempo máximo que le toma al aplicativo generar un código QR sin cifrar, ingresando la cantidad máxima de caracteres permitido, es no sobrepasan los 0.7 segundos.

2.4.5.4.3. **Generación del código QR con texto cifrado**

La siguiente prueba medirá el tiempo que le toma al aplicativo generar un código QR, utilizando el texto que fue cifrado por el algoritmo. Los resultados se exhiben a continuación:

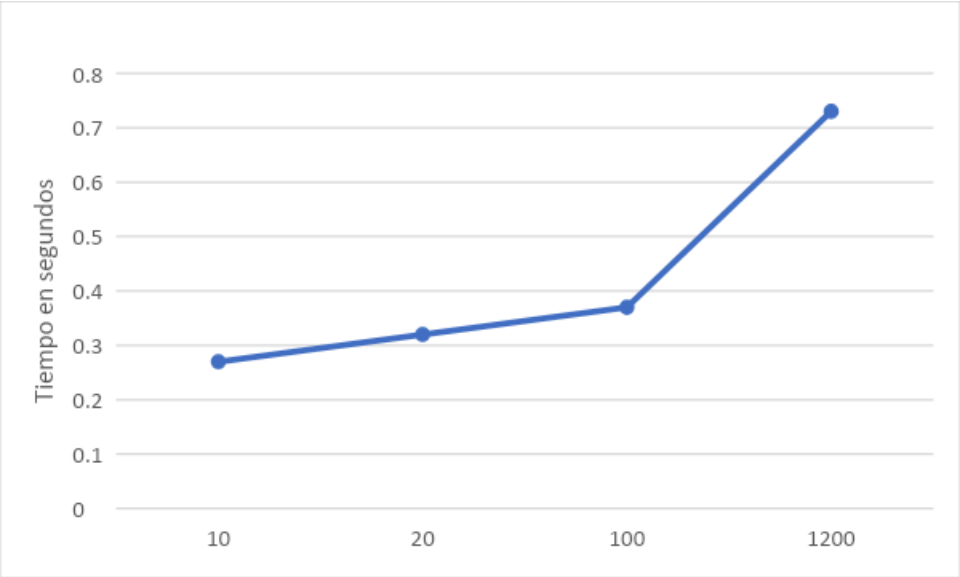
Tabla 6.

Tiempo de respuesta durante la generación de un código QR con mensaje cifrado

Cantidad de caracteres	Tiempo
10 caracteres	0,27 segundos
20 caracteres	0,32 segundos
100 caracteres	0,3 segundos
1200 caracteres	0,73 segundos

Nota. Elaborado por: Autor

Ilustración 34.
Generación de un código QR con mensaje cifrado



Nota. Elaborado por: Autor

Las pruebas realizadas al aplicativo revelan los tiempos de respuesta de este ante el proceso de generación del código QR, utilizando un mensaje cifrado. Se puede observar que el tiempo máximo de generación del QR, utilizando la capacidad máxima de caracteres (1200 caracteres) es de tan solo 0,73 segundos.

2.4.5.4.4. **Escaneo de código QR sin mensaje cifrado**

Durante esta prueba, se medirá el tiempo que le toma al aplicativo escanear, interpretar y presentar la información escaneada, la cual no se encuentra cifrada.

Debido a los factores tales como iluminación, resolución de cámara y precisión del usuario, la actividad de lectura del código fue realizada diez veces con cada uno de los diferentes tamaños de caracteres. Luego de esto, se calculó el tiempo promedio que le tomó al aplicativo.

A continuación, se muestran los resultados de las pruebas ejecutadas:

Tabla 7.

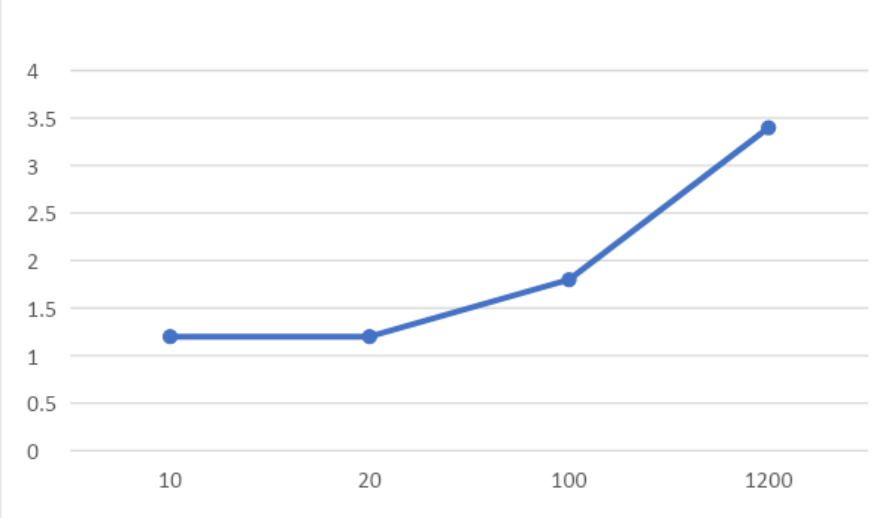
Tiempo de respuesta durante el escaneo de código QR con mensaje en texto plano

Cantidad de caracteres	Tiempo
10 caracteres	1,2 segundos
20 caracteres	1,2 segundos
100 caracteres	1,8 segundos
1200 caracteres	3,4 segundos

Nota. Elaborado por: Autor

Ilustración 35.

Tiempo de respuesta durante el escaneo de código QR con mensaje en texto plano



Nota. Elaborado por: Autor.

Los resultados de la prueba de escaneo del código QR sin mensaje cifrado revelan, nuevamente, una relación directa entre el tiempo de respuesta del aplicativo y la cantidad de caracteres utilizada.

Es importante destacar que el prototipo logra escanear el código QR con el mensaje en texto plano en un tiempo menor a 4 segundos.

2.4.5.4.5. **Escaneo de código QR con mensaje cifrado**

Para la elaboración de la última prueba de rendimiento, se considerará el tiempo de respuesta del aplicativo durante el proceso de escaneo de un código QR que incluye un mensaje cifrado. El tamaño de caracteres que utilizará el mensaje variará, partiendo desde los diez caracteres hasta los 1200 caracteres.

Los resultados se muestran a continuación:

Tabla 8.

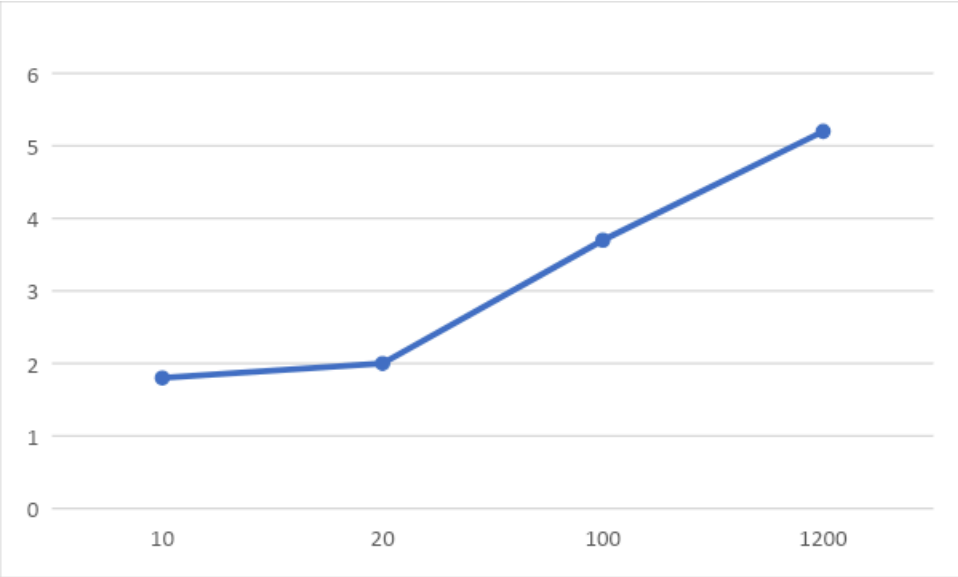
Tiempo de respuesta durante el escaneo de código QR con mensaje cifrado

Cantidad de caracteres	Tiempo
10 caracteres	1,8 segundos
20 caracteres	2 segundos
100 caracteres	3,7 segundos
1200 caracteres	5,2 segundos

Nota. Elaborado por: Autor.

Ilustración 36.

Tiempo de respuesta durante el escaneo de código QR con mensaje cifrado



Nota. Elaborado por: Autor.

Los resultados de esta última prueba reafirman lo que se ha expuesto durante el proceso de funcionalidad; existe una relación directamente proporcional entre la cantidad de texto ingresado y el tiempo de respuesta del aplicativo durante el escaneo del código QR con el mensaje cifrado.

2.4.5.5. **Seguridad**

Debido a la naturaleza del presente proyecto, el criterio de la seguridad que el prototipo aplica debe ser considerada y evaluada.

Como se ha mencionado en la Fase II de la Metodología Aplicada, se ha optado por elegir el algoritmo AES con una clave de 128 bits. El Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) menciona que “incluso con el impacto de las computadoras cuánticas, AES-128, AES-192 y AES-256 permanecerán seguras durante las próximas décadas” (NIST, 2024).

Basado en lo anterior, se considera que el algoritmo utilizado es considerado seguro. Sin embargo, no se encuentra libre de ataques como fuerza bruta. El ataque de

fuerza bruta se basa en probar todas las combinaciones posibles de la clave; una vez se obtenga la clave correcta, se descifrará el mensaje.

Sin embargo, se han implementado medidas de seguridad adicionales, tales como una clave secreta, un vector de inicialización, modos de relleno utilizando *PKCS5Padding* y el modo de Encadenamiento en Bloques de Cifrado (CBC, por sus siglas en inglés), y codificación en Base64.

Para dar a conocer su eficacia frente a un ataque de fuerza bruta, (Oyekanmi & Ebenezer Adepoju, 2023) realizaron una tabla relacional en la que se incluye el tamaño de la clave (bits) y el número total de combinaciones posibles, basados en el tamaño de la clave. La tabla se muestra a continuación:

Tabla 9.

Tabla de relación entre el tamaño de la clave y el número de combinaciones posibles

Tamaño de la clave (Bits)	**Número de combinaciones posibles**
1 bit	2
2 bits	4
4 bits	16
8 bits	256
16 bits	65536
32 bits	4.2×10^{9}
56 bits (usando en DES)	7.2×10^{16}
64 bits	1.8×10^{19}
128 bits	3.4×10^{38}

Nota. La tabla de relación únicamente muestra valores hasta 128 bits, que es el tamaño de clave que el prototipo usa. Fuente: (Oyekanmi & Ebenezer Adepoju, 2023). Elaborado por: Autor.

2.4.5.6. **Integridad**

Las siguientes pruebas a realizarse estarán basadas en la integridad del código QR generado. Dentro de este apartado se generarán situaciones que podrían comprometer la facilidad de la lectura del código QR con mensaje cifrado.

2.4.5.6.1. **Lectura del código QR con mensaje cifrado sin pérdida en el área de datos**

A continuación, se genera el código QR que incluye el mensaje cifrado. El mensaje en cuestión es: “Hola, esta es una prueba de integridad de QR”.

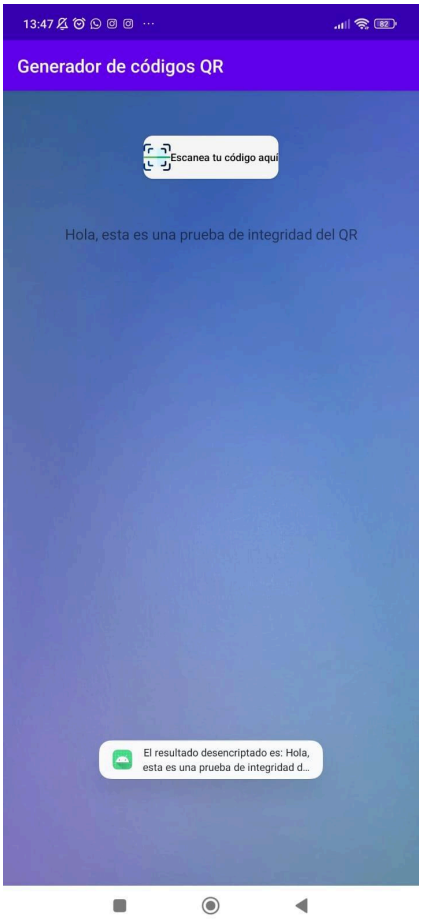
Ilustración 37.

Lectura del código QR con mensaje cifrado sin pérdida en el área de datos

Nota. Elaborado por: Autor.

Ilustración 38.

Lectura del código QR con mensaje cifrado sin pérdida en el área de datos desde el dispositivo móvil



Nota. Se realiza un escaneo exitoso del código QR con el mensaje cifrado. Elaborado por: Autor.

El proceso de escaneo se realiza sin complicación alguna, dentro del parámetro del tiempo expuesto durante las pruebas de rendimiento.

2.4.5.6.2. **Escaneo del código QR con mensaje cifrado con pérdida parcial del área de datos**

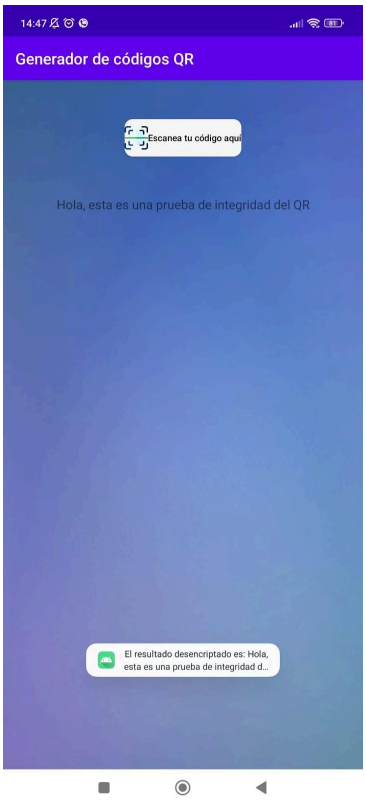
Ilustración 39.

Código QR con mensaje cifrado y pérdida parcial del área de datos

Nota. Elaborado por: Autor.

Ilustración 40.

Lectura de código QR con mensaje cifrado y pérdida parcial del área de datos



Nota. El aplicativo es capaz de escanear y mostrar el texto cifrado a pesar de que falte una porción del área de datos. Elaborado por: Autor.

2.4.5.6.3. Lectura del código QR con mensaje cifrado con pérdida mayor del área de datos

Por último, se podrá prueba la capacidad del aplicativo para recuperar la información a pesar de que el código presente un daño en una gran parte de su área de datos.

Ilustración 41.
Código QR con mensaje cifrado con pérdida mayor del área de datos

Nota. Generación de código QR sin una parte de su área de datos. Elaborado por: Autor.

Como resultado, el aplicativo no fue capaz de poder escanear el código QR con esta magnitud de daño.

2.4.5.7. Ficha juicio de expertos

Tabla 10.

Ficha de información del experto A.

Nombre	Mgtr. Pablo Barba
Institución donde trabaja	John Galt Solutions Inc.
Autor	Daniel André Peñaherrera Barriga
Trabajo de integración curricular	Desarrollo de una aplicación para generar y escanear códigos bidireccionales QR con seguridad integrada en Android.
Fecha	15 de agosto de 2024

Nota. Elaborado por: Autor.

Tabla 11.

Criterios de evaluación.

Criterios	**Descripción**	**1**	**2**	**3**	**4**	**5**
Diseño	La interfaz es intuitiva y fácil de usar para los usuarios finales.				X	
Funcionabilidad	El software responde de manera eficiente y cumple con los tiempos de respuesta establecidos.					X
Rendimiento	El sistema está diseñado para manejar un crecimiento en el volumen de datos sin perder rendimiento.			X		
Seguridad	El software incluye medidas adecuadas para proteger la información y los datos de los usuarios contra accesos no autorizados o ataques.				X	
Integridad	El sistema puede escanear un código QR que puede encontrarse o no en su totalidad				X	

Elaborado por: Autor.

Opinión de aplicabilidad

El software cumple con el objetivo de añadir una capa de seguridad al código QR antes de su escaneo. Se destaca la rapidez para encriptar y desencriptar los códigos QR escaneados.

Como recomendación, una interfaz más atractiva podría añadirle más valor al proyecto. Adicionalmente, se debe tomar en consideración la cantidad límite de caracteres que pueden ser escaneados.

Tabla 12.

Ficha de información del experto B.

Nombre	MBA. Pablo Calero
Institución donde trabaja	Grupo Mavesa
Autor	Daniel André Peñaherrera Barriga
Trabajo de integración curricular	Desarrollo de una aplicación para generar y escanear códigos bidireccionales QR con seguridad integrada en Android.
Fecha	16 de agosto de 2024

Elaborado por: Autor.

Tabla 13.

Criterios de evaluación

Criterios	**Descripción**	**1**	**2**	**3**	**4**	**5**
Diseño	La interfaz es intuitiva y fácil de usar para los usuarios finales.				X	
Funcionabilidad	El software responde de manera eficiente y cumple con los tiempos de respuesta establecidos.					X
Rendimiento	El sistema está diseñado para manejar un crecimiento en el volumen de datos sin perder rendimiento.				X	
Seguridad	El software incluye medidas adecuadas para proteger la información y los datos de los usuarios contra accesos no autorizados o ataques.					X
Integridad	El sistema puede escanear un código QR que puede encontrarse o no en su totalidad				X	

Elaborado por: Autor.

Opinión de aplicabilidad

La aplicación, a pesar de mostrar un *front-end* sencillo, es bastante intuitiva y fácil de usar, pero no es muy atractiva; los tiempos de respuesta de la aplicación son favorables.

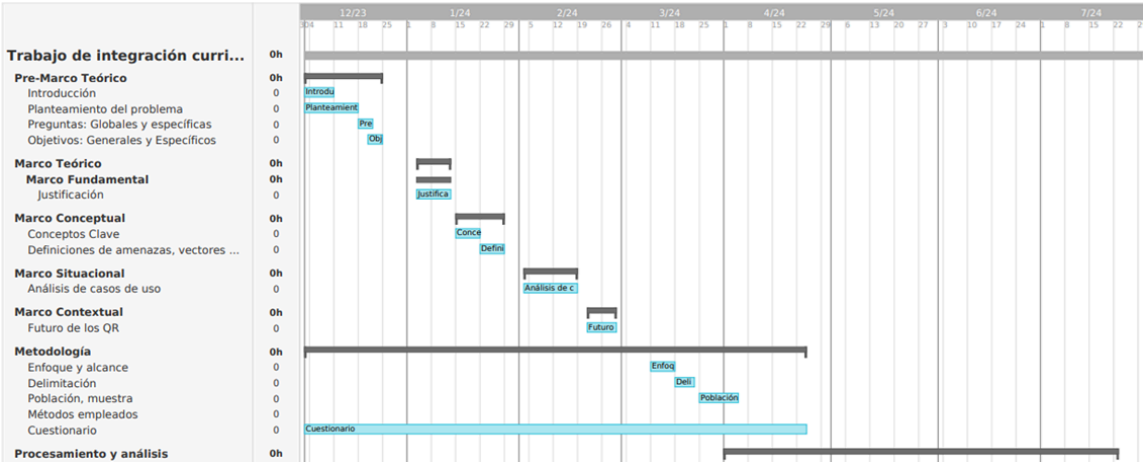
Recomiendo que se incluya un proceso de manejo de errores más amigable para el usuario.

2.5. Cronograma de actividades

Ilustración 42.

Gráfico Gantt con las actividades del presente trabajo investigativo

Para la organización, distribución y ejecución de las tareas del presente trabajo investigativo, se utilizó un gráfico Gantt. El gráfico Gantt que incluye todas las tareas se puede encontrar en la sección 7.2 de Anexos.



Elaborado por: Autor.

3. Análisis de resultados de la investigación

3.1. Presentación de resultados

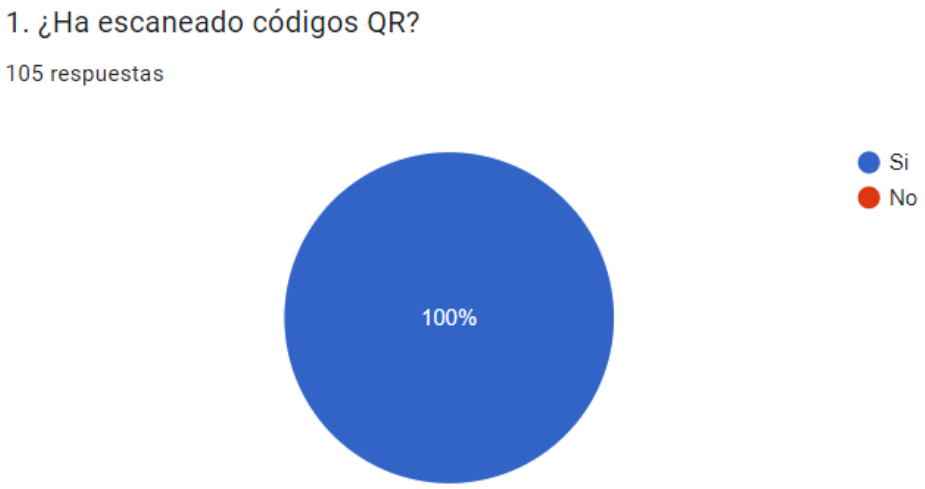
A continuación, se adjuntan los resultados de las diversas etapas del presente trabajo investigativo.

3.1.1. Presentación de encuestas

Las siguientes encuestas fueron desarrolladas durante un periodo de 4 meses a diferentes estudiantes, pertenecientes a las carreras de Ingeniería en Software, Ingeniería en Tecnologías de la información e Ingeniería en Sistemas, de la Universidad Tecnológica Ecotec (campus Samborondón)

Ilustración 43.

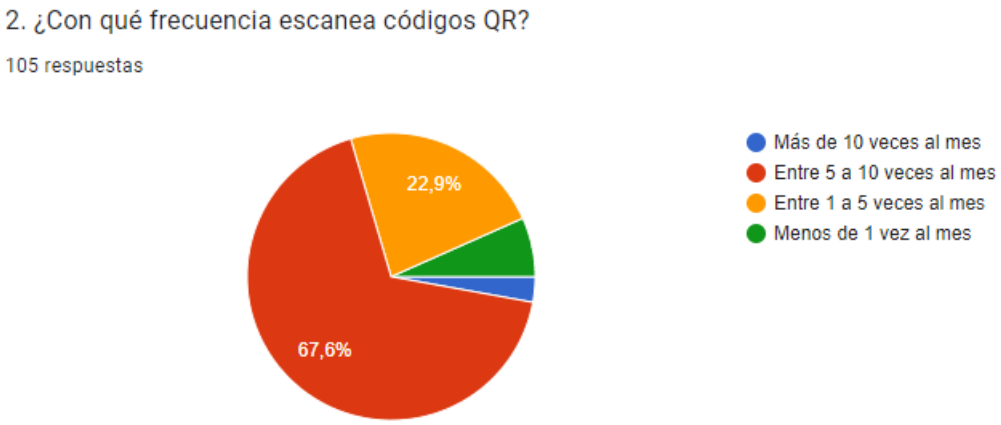
Pregunta 1. ¿Ha escaneado códigos QR?



Nota. El 100% de los encuestados ha respondido afirmativamente a la pregunta, lo cual demuestra que los códigos QR generan un impacto grande dentro de nuestra muestra.
Elaborado por: Autor.

Ilustración 44.

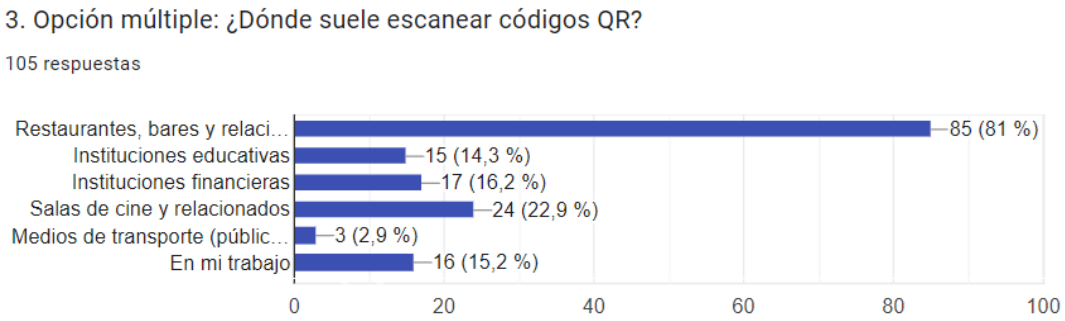
Pregunta 2. ¿Con qué frecuencia escanea códigos QR?



Nota. La mayoría de los encuestados (67,6%) escanean códigos QR entre 5 a 10 veces al mes. Elaborado por: Autor.

Ilustración 45.

Pregunta 3. ¿Dónde suele escanear códigos QR?



Nota. El 81% de los encuestados escanea códigos QR durante su visita a restaurantes, bares y otros establecimientos relacionados. Elaborado por: Autor.

Ilustración 46.

Pregunta 4. ¿Conoce usted el contenido que está escaneando?

Nota. El 93,3% de los encuestados se siente seguro del contenido que se encuentran escaneando por medio de códigos QR. Elaborado por: Autor.

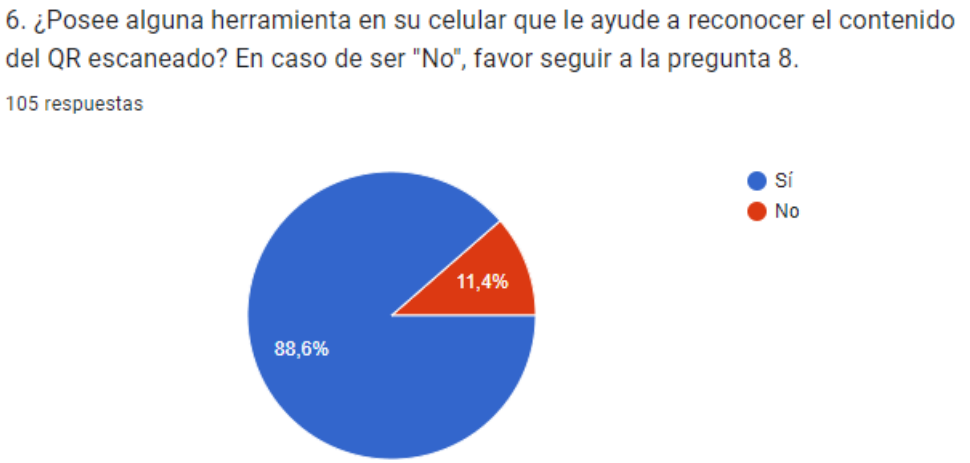
Ilustración 47.

Pregunta 5. ¿Es familiar con el término "Quishing"?

Nota. La gran mayoría de los encuestados (81,9%) desconoce sobre el término "*Quishing"* y sus implicaciones. Elaborado por: Autor.

Ilustración 48.

Pregunta 6. ¿Posee alguna herramienta en su celular que le ayude a reconocer el contenido del QR escaneado? En caso de ser "No", favor seguir a la pregunta 8.



Nota. El 88,6% de los encuestados menciona poseer una herramienta que les ayude a reconocer el código QR escaneado. Elaborado por: Autor.

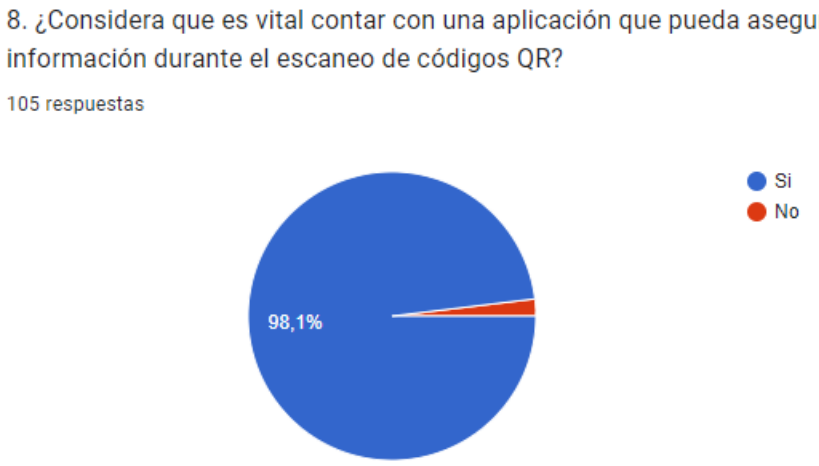
Ilustración 49.

Pregunta 7. ¿Conoce usted que la cámara de su celular podría no asegurar el destino final del enlace escaneado?

Nota. El 83,8% de los encuestados desconocía sobre la falta de mecanismos de seguridad integrada dentro de la aplicación de cámara de su celular, la cual no puede asegurar el destino final del enlace escaneado sea malicioso (o no). Elaborado por: Autor.

Ilustración 50.

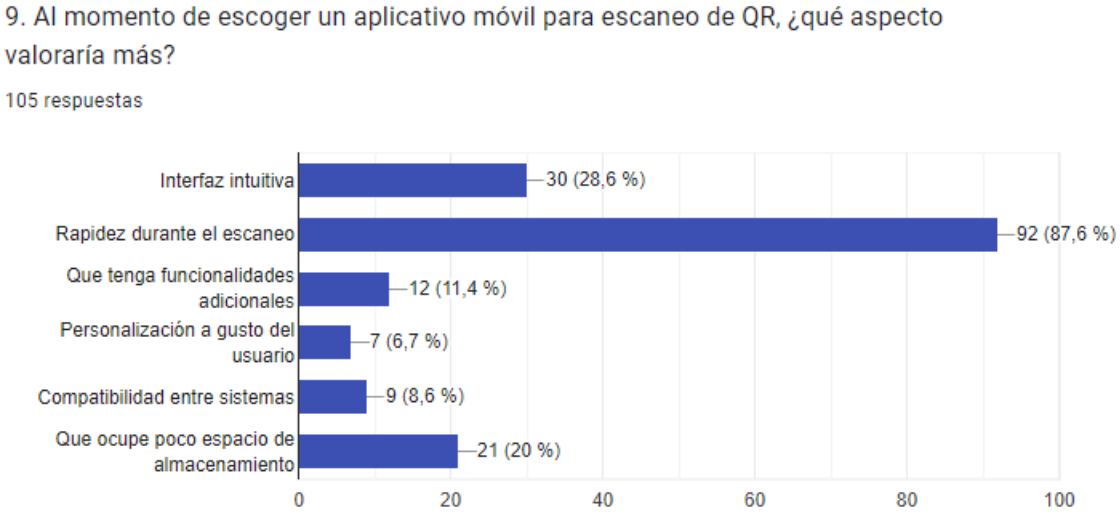
Pregunta 8. ¿Considera que es vital contar con una aplicación que pueda asegurar la información durante el escaneo de códigos QR?



Nota. Un 98,1% de los encuestados considera que es vital contar con un aplicativo que pueda asegurar la información durante el escaneo de códigos QR, lo cual muestra una preocupación latente dentro de los encuestados sobre las amenazas presentes en los códigos QR. Elaborado por: Autor.

Ilustración 51.

Pregunta 9. Al momento de escoger un aplicativo móvil para escaneo de QR, ¿qué aspecto valoraría más?



Nota. La gran mayoría de los encuestados valora que el aplicativo para escaneo de códigos QR sea rápido durante aquel proceso, adicionalmente se valora una interfaz intuitiva, y que no ocupe mucho espacio de almacenamiento. Elaborado por: Autor.

Ilustración 52.

Pregunta 10. Dentro del apartado gráfico, ¿cuál considera más atractivo para una aplicación de esta índole?

Nota. El 44,8% de los encuestados optó por una interfaz minimalista que usa una paleta de colores que transmite dinamismo y entusiasmo; el 29,5% eligió una interfaz más convencional, con colores más fuertes y sólidos; mientras que el 23,8% de los encuestados eligió una interfaz minimalista que incluye una paleta de colores con tonos que transmiten calma. Elaborado por: Autor.

3.2. Discusión de resultados encontrados en encuestas

Las encuestas revelan que la muestra se encuentra familiarizada con los códigos QR, dado que suelen interactuar diariamente con ellos. Sin embargo, es importante destacar que una gran parte de la muestra no posee conocimiento alguno sobre

quishing. De hecho, más del 80% de los encuestados desconocía que la aplicación de cámara (aplicación nativa de su celular) podía no revelar la URL de destino del código QR que se estaba escaneando. Lo cual indica que nunca estuvieron completamente seguros a donde eran dirigidos, simplemente confiaban en la entidad que emitió en código QR.

Las encuestas también revelan que la muestra es consciente de lo que se encuentra escaneando (una minúscula porción de esta sólo lo hacía por curiosidad). También se destaca el uso de códigos QR en establecimientos tales como restaurantes, bares, salas de cine, instituciones educativas, instituciones financieras, y hasta en sus trabajos. Asimismo, la frecuencia de uso de los códigos QR de la muestra se encuentra en un promedio de entre 5 a 10 veces al mes.

4. Conclusiones

Durante el desarrollo de este trabajo investigativo (y posterior desarrollo de una propuesta tecnológica), se ha demostrado que añadir medidas de seguridad adicionales a los códigos QR estáticos significa una opción confiable y robusta para salvaguardar la información que es transmitida durante el proceso de escaneo y transferencia de información, dado que estas medidas lograrán mitigar las vulnerabilidades y vectores de ataques existentes, de esta forma se podrá garantizar la integridad de la información contenida dentro del código QR.

Dentro de este trabajo investigativo, se han podido Identificar las vulnerabilidades presentes en los códigos QR convencionales mediante técnicas investigativas, lo cual sirvió como base fundamental para desarrollar e integrar medidas de seguridad para el prototipo.

Se estableció un algoritmo de cifrado robusto y seguro, el cual no comprometió la velocidad de generación y escaneo de los códigos QR. Adicionalmente, se añadió codificación en Base64, así como también un Vector de Iniciación, y un modo de Encadenamiento de Bloques de Cifrado (CBC) para el algoritmo de cifrado AES.

Adicionalmente, se ha demostrado que la implementación del cifrado AES de 128-bits no ha afectado (en una medida observable) el rendimiento de los procesos de escaneo y generación de códigos QR (cifrados o no), lo cual denota la viabilidad práctica de la propuesta tecnológica.

Finalmente, mediante la ejecución de las pruebas controladas expuestas en este trabajo investigativo, se ha podido demostrar la viabilidad práctica del aplicativo desarrollado.

5. Recomendaciones

Para garantizar la interoperabilidad de la propuesta tecnológica, resulta primordial desarrollar un método más eficaz para la generación de las llaves. El que se encuentre incrustada en el código reduce la posibilidad de que este trabajo pueda ser explotado a más sistemas, reduciendo su capacidad de expansión. Adicionalmente, se debe trabajar en desarrollar un diseño de la plataforma más atractivo y una experiencia de usuario más amigable; hacerlo será muy favorable para el aplicativo dado que ganará mayor popularidad dentro de la comunidad.

Se recomienda la utilización de un algoritmo más seguro, como podría ser AES 256 en lugar del ya existente 128. Aunque ambos son seguros (según los estándares vigentes), AES 256 posee ciertas ventajas en ataques de fuerza bruta, y capacidad de protección a largo plazo; hay que recordar que el avance del poder computacional va de

la mano con el desarrollo de la tecnología. Adoptar AES 256 asegurará que esta propuesta tecnológica sea relevante durante muchos años.

En lo que respecta a la generación de códigos QR, para dueños de establecimientos tales como restaurantes, bares, entre otros, en donde se ha demostrado que la utilización de los códigos QR es mayor, sería conveniente agregar una funcionalidad de impresión al momento desde el aplicativo hacia una impresora conectada (ya sea por red o bluetooth). Añadir esta característica mitigaría completamente la vulnerabilidad de reemplazo de los códigos legítimos por maliciosos.

6. Bibliografía

Android Developers. (s.f.). *Introducción a Android Studio .* Obtenido de https://developer.android.com/studio/intro?hl=es-419

Asamblea Nacional de la República del Ecuador. (21 de mayo de 2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS.* Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Banco Pichincha. (10 de diciembre de 2022). *Ley de Protección de Datos Personales en Ecuador.* Obtenido de https://www.pichincha.com/blog/ley-proteccion-datos-ecuador-que-es

BOSS Magazine. (2023). *The Future of QR Codes in Digital Marketing.* Obtenido de https://thebossmagazine.com/future-of-qr-codes-in-digital-marketing/

Cai, H., Liu, X., & Yan, B. (2019). Beautified QR code with security based on data hiding. *Advances in Computational Intelligence Systems: UKCI 2019*, 339-347. doi:978-3-030-29933-0_35

Chandra, S., & Kumar, M. (2019). *Integration of AIDC technology in mobile via QR code for enhancing the library services: A case study of Don Bosco College Central Library.* Obtenido de Indian Journal of Information Sources and Services.: https://www.researchgate.net/profile/Manoj-V

Chandrasekhar, D., Kumar Rath, A., & Kabat, M. R. (s.f.). *CRYPTOGRAPHY AND NETWORK SECURITY LECTURE NOTES.* Obtenido de Veer Surendra Sai University of Technology: https://vssut.ac.in/lecture_notes/lecture1428550736.pdf

CheckPoint. (2024). *What is the CIA Triad?* Obtenido de Availability: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-it-security/what-is-the-cia-triad/

CloudFlare. (s.f.). *What is Quishing?* Obtenido de https://www.cloudflare.com/es-es/learning/security/what-is-quishing/

Cofense. (2023). *Major energy company targeted in QR code phishing campaign*. Obtenido de https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/

Comillas Universidad Pontificia. (2022). *¿Qué es el cifrado AES?* Obtenido de https://ciberseguridad.comillas.edu/que-es-el-cifrado-aes/

Deineko, Z. (2022). *QR code as an element of educational activity*. Obtenido de https://openarchive.nure.ua/items/c789f0f8-917e-4eff-9a3c-454c6ffe6fb7

Denso Wave. (1994). *What is a QR Code?* Obtenido de Denso Wave: https://www.denso-wave.com/en/adcd/fundamental/2dcode/qrc/

Denso Wave. (s.f.). *Technologies*. Obtenido de QR Code Development History: https://www.denso-wave.com/en/technology/vol1.html

ESET. (2023). *ESET Security Report Latam.* Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Flowcode. (2 de mayo de 2024). *Now Live! Our Most Advanced Geolocation Data in Flowcode Analytics.* Obtenido de https://www.flowcode.com/blog/flowcode-advanced-geolocation-map

Focardi, R., Luccio, F. L., & Wahsheh, H. A. (2019). Usable security for QR code. *Journal of Information Security and Applications*, 48. Obtenido de Usable security for QR code.

Fortinet. (s.f.). *Cyberglossary.* Obtenido de What is a QR code? How does it work? Types and benefits: https://www.fortinet.com/resources/cyberglossary/what-is-a-qr-code

Gamboa, J. (2020). *Importancia de la seguridad informática y ciberseguridad en el mundo actual.* Obtenido de https://repository.unipiloto.edu.co/handle/20.500.12277/8668

García, A. B. (s.f.). *El cifrado RC4.* Obtenido de Universidad de Salamanca: https://ntrrgc.me/attachments/Cifrado_RC4/

Giustini, C. (11 de agosto de 2023). *A phishing attempt on Steam that became a Qrljacking research.* Obtenido de Voidzone: https://voidzone.me/posts/a-phishing-attempt-on-steam-that-became-qrljacking/?21398

Grand View Research. (2023). *QR code payment market size, share & trends analysis report by offerings, by solution, by payment type, by transaction channel, by end-user, by region, and segment forecasts, 2023 - 2030.* Obtenido de https://www.grandviewresearch.com/industry-analysis/qr-code-payment-market-report

Guo, H., Gao, S., Yang, X., & Jia, J. (2018). An empirical study on users' continuous usage intention of QR code mobile payment services in China. *International Journal of E-adoption*, 18-33.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). *Fundamentos de metodología de la investigación.*

Hernández, Fernández, & Baptista. (2014). *Metodología de la Investigación.* Obtenido de https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Hoxhunt. (19 de octubre de 2023). *Don't scan! Insights from the Hoxhunt cybersecurity human risk benchmark challenge.* Obtenido de Hoxhunt Blog: https://hoxhunt.com/blog/insights-hoxhunt-cybersecurity-human-risk-benchmark-challenge

IBM. (2024). *¿Qué es la criptografía?* Obtenido de https://www.ibm.com/mx-es/topics/cryptography

IBM. (2024). *What is data integrity?* Obtenido de https://www.ibm.com/topics/data-integrity

IEEE Conference Publication. (1 de junio de 2019). *A survey of the QR code phishing: The current attacks and countermeasures*. Obtenido de IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8843688

IEEE Conference Publication. (2019). *Smart City bus application with QR code: A review.* Obtenido de IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8825047

Insider Intelligence. (2022). *US QR code usage statistics (2019-2025)*. Obtenido de Business Insider: https://www.businessinsider.com/us-qr-code-user-statistics

Instituto Nacional de Ciberseguridad. (2019). *¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet?* Obtenido de https://www.incibe.es/ciudadania/blog/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad

Internet Crime Complaint Center (IC3). (2023). *Cybercriminals tampering with QR codes to steal victim funds.* Obtenido de https://www.ic3.gov/Media/Y2022/PSA220118

ISO. (2023). *¿Qué es la criptografía?* Obtenido de https://www.iso.org/es/seguridad-informacion/criptografia

Juniper Research. (2023). *QR code payments: Market expansion and high-growth areas.* Obtenido de https://www.juniperresearch.com/blog/august-2023/qr-code-payments-market-expansion-growth

Kaspersky. (2023). *QR code security: What are QR codes and are they safe to use?* Obtenido de https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan

Kaspersky. (2023). *QR code security: What are QR codes and are they safe to use?* Obtenido de https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan

KeepCoding. (23 de mayo de 2024). *¿Qué es el modo de cifrado CBC?* Obtenido de https://keepcoding.io/blog/modo-de-cifrado-cbc

Keepnet Labs. (15 de enero de 2024). *2024 QR Code Phishing Trends: In-Depth Analysis of Rising Quishing Statistics*. Obtenido de Keepnet Labs Blog: https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of-rising-quishing-statistics

Keyence. (s.f.). *What is a QR code?* Obtenido de https://www.keyence.eu/ss/products/auto_id/codereader/basic_2d/qr.jsp

Kingston. (2023). *¿Qué es cifrado, y cómo funciona?* Obtenido de https://www.kingston.com/es/blog/data-security/what-is-encryption

Lin, Lan, Chen, & Wu. (Febrero de 2022). *National Library of Medicine.* doi:10.3390/e24020284

Lookout. (2022). *The global state of mobile phishing report*. Obtenido de https://www.lookout.com/form/the-global-state-of-mobile-phishing-report

Lozada, J. (2014). Investigación Aplicada: Definición, Propiedad Intelectual e Industria. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica, 3*(1), 47-50. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6163749

Malwarebytes. (2023). *QR code: What is a QR code? Are QR codes safe?* Obtenido de https://www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code

McAfee. (18 de mayo de 2023). *McAfee - Safer Summer Holidays*. Obtenido de McAfee Press Releases: https://www.mcafee.com/hr-hr/consumer-corporate/newsroom/press-releases/press-release.html?news_id=74115f73-a7a7-440e-a2f4-2ec0e040ca9d

MDN Web Docs. (2023). *Descifrado.* Obtenido de https://developer.mozilla.org/es/docs/Glossary/Decryption

Mettler-Toledo International Inc. (2024). *Los 10 principios de ALCOA++.* Obtenido de https://www.mt.com/es/es/home/library/guides/laboratory-division/lab-data-integrity/Data-Integrity-ALCOA-Poster.html

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (18 de febrero de 2015). *Ley Orgánica de Telecomunicaciones.* Obtenido de https://www.gob.ec/regulaciones/ley-organica-telecomunicaciones

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (18 de febrero de 2015). *Ley Orgánica de Telecomunicaciones.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Mutleq, H. (2018). *Secure and usable QR codes*. Obtenido de Unive.it: http://dspace.unive.it/bitstream/handle/10579/15022/956262-1208160.pdf?sequence=2

NFON. (s.f.). *AES.* Obtenido de https://www.nfon.com/es/get-started/cloud-telephony/lexicon/base-de-conocimiento-destacar/aes

NIST. (2024). *Information Technology Laboratory.* Obtenido de Computer Security Resource Center: https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

Oyekanmi, E., & Ebenezer Adepoju, S. (20 de marzo de 2023). An Efficient Data Protection for Cloud Storage Through Encryption. *International Journal of Advanced Networking and Applications, 14*. doi:10.35444/IJANA.2023.14505

Pachacama, E. (2023). *Dominando JAVA 1: Aprende los pilares del desarrollo de software con lenguaje JAVA*. Obtenido de https://itq.edu.ec/wp-content/uploads/2023/10/2023-09-29_dominando_java_i.pdf

Peralta, A., & Porfirio, D. (2003). *La obligación del registro sindical, por la autoridad administrativa de trabajo, como incumplimiento de la constituci[on política del estado y el convenio 87 de la OIT.* Obtenido de Universidad Nacional Mayor de San Marcos: https://sisbib.unmsm.edu.pe/BibVirtual/Tesis/Human/aliaga_pd/aliaga_pd.htm

Porfirio, D., & Peralta, A. (2003). *La obligación del registro sindical, por la Autoridad Administrativa de Trabajo, como incumplimiento de la Constitución Política del Estado y el Convenio 87 de la OIT.* Obtenido de https://cybertesis.unmsm.edu.pe/handle/20.500.12672/1214

Posey, B. (2022). *Understanding QR code security issues for enterprise devices.* Obtenido de Mobile Computing: https://www.techtarget.com/searchmobilecomputing/tip/Understanding-QR-code-security-issues-for-enterprise-devices

Schwaber, K., & Sutherland, J. (2020). *La guía definitiva de Scrum: Las reglas del juego*. Obtenido de scrumguides.org: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Spanish-Latin-South-American.pdf

Security Magazine. (2023). *Security Magazine.* Obtenido de New report shows 51% rise in QR code phishing for September: https://www.securitymagazine.com/articles/100122-new-report-shows-51-rise-in-qr-code-phishing-for-september

Shah, J., Sonawan, R., Lad, S., & Wankhade, S. (2020). *Verification of the users using QR code in banking systems.* Obtenido de Ijrar.org: https://www.ijrar.org/papers/IJRAR2002117.pdf

Southern New Hampshire University. (28 de agosto de 2023). *¿Por qué es importante la comunicación en la era digital?* Obtenido de https://es.snhu.edu/blog/importancia-de-la-comunicacion-en-la-era-digital

Strömberg, O. (2023). *Use cases for traceability systems: An explanatory case study about the application areas for QR codes.* Obtenido de https://ltu.diva-portal.org/smash/get/diva2:1791771/FULLTEXT01.pdf

Tarlogic. (2024). *Malvertising, cuando los anuncios son una trampa*. Obtenido de https://www.tarlogic.com/es/blog/malvertising/

Techguard Security. (02 de septiembre de 2023). *Four Risks and Solutions When Using QR Codes*. Obtenido de TechGuard Blog: https://blog.techguard.com/four-risks-and-solutions-when-using-qr-codes

Thakkar, D. (2023). *QR code vulnerabilities: Dissecting new techniques seen in the wild*. Obtenido de SecurityHQ: https://www.securityhq.com/blog/qr-code-vulnerabilities-dissecting-new-techniques-seen-in-the-wild/

Trivedi, R. H., Teichert, T., & Hardeck, D. (2019). Effectiveness of pull-based print advertising with QR codes. 145-147. Obtenido de European Journal of Marketing,.

Universidad Tecnológica Ecotec. (2024). *Rendición de Cuentas - 2023*. Obtenido de Ecotec.edu.ec: https://ecotec.edu.ec/content/uploads/2024/06/RENDICION-DE-CUENTAS-2023.pdf

Washington University in St. Louis. (s.f.). *Terms.* Obtenido de Office of Information Security: https://informationsecurity.wustl.edu/items/integrity/

Willis, T. (s.f.). *ALCOA++: Qué hay de nuevo, qué es importante y qué necesitas saber.* Obtenido de https://blog.pqegroup.com/es-es/csv-data-integrity/alcoa-lo-que-necesitas-saber

7. Anexos

7.1. Encuesta realizada a estudiantes de la Universidad Tecnológica Ecotec, campus Samborondón.

1. ¿Ha escaneado códigos QR?

Marca solo un óvalo.

- ***Si***
- ***No***

2. ¿Con qué frecuencia escanea códigos QR?

Marca solo un óvalo.

- ***Más de 10 veces al mes***
- ***Entre 5 a 10 veces al mes***
- ***Entre 1 a 5 veces al mes***
- ***Menos de 1 vez al mes***

3. Opción múltiple: ¿Dónde suele escanear códigos QR?

Selecciona todos los que correspondan.

- ***Restaurantes, bares y relacionados***
- ***Instituciones educativas***
- ***Instituciones financieras***
- ***Salas de cine y relacionados***
- ***Medios de transporte (público/privado)***
- ***En mi trabajo***
- Otro: _____

4. ¿Conoce usted el contenido que está escaneando?

Marca solo un óvalo.

- ***Sí***
- ***No***
- ***No lo sé, lo hago por curiosidad***
- Otro: _____

5. ¿Es familiar con el término "Quishing"?

Marca solo un óvalo.

- ***Sí***
- ***No***

6. ¿Posee alguna herramienta en su celular que le ayude a reconocer el contenido del QR escaneado? En caso de ser "No", favor seguir a la pregunta 8.

Marca solo un óvalo.

- ***Sí***
- ***No***

7. ¿Conoce usted que la cámara de su celular podría no asegurar el destino final del enlace escaneado?

Marca solo un óvalo.

- ***Sí, lo sé***
- ***No lo sabía***

8. ¿Considera que es vital contar con una aplicación que pueda asegurar la información durante el escaneo de códigos QR?

Marca solo un óvalo.

- ***Si***
- ***No***

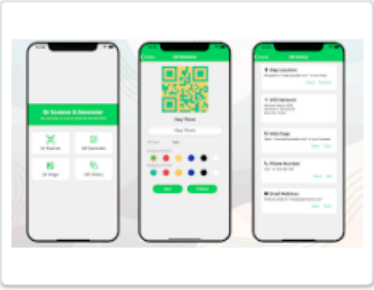
9. Al momento de escoger un aplicativo móvil para escaneo de QR, ¿qué aspecto valoraría más?

Selecciona todos los que correspondan.

- [ ] Interfaz intuitiva
- [ ] Rapidez durante el escaneo
- [ ] Que tenga funcionalidades adicionales
- [ ] Personalización a gusto del usuario
- [ ] Compatibilidad entre sistemas
- [ ] Que ocupe poco espacio de almacenamiento

10. Dentro del apartado gráfico, ¿cuál considera más atractivo para una aplicación de esta índole?

Selecciona todos los que correspondan.



- [ ] Opción 1

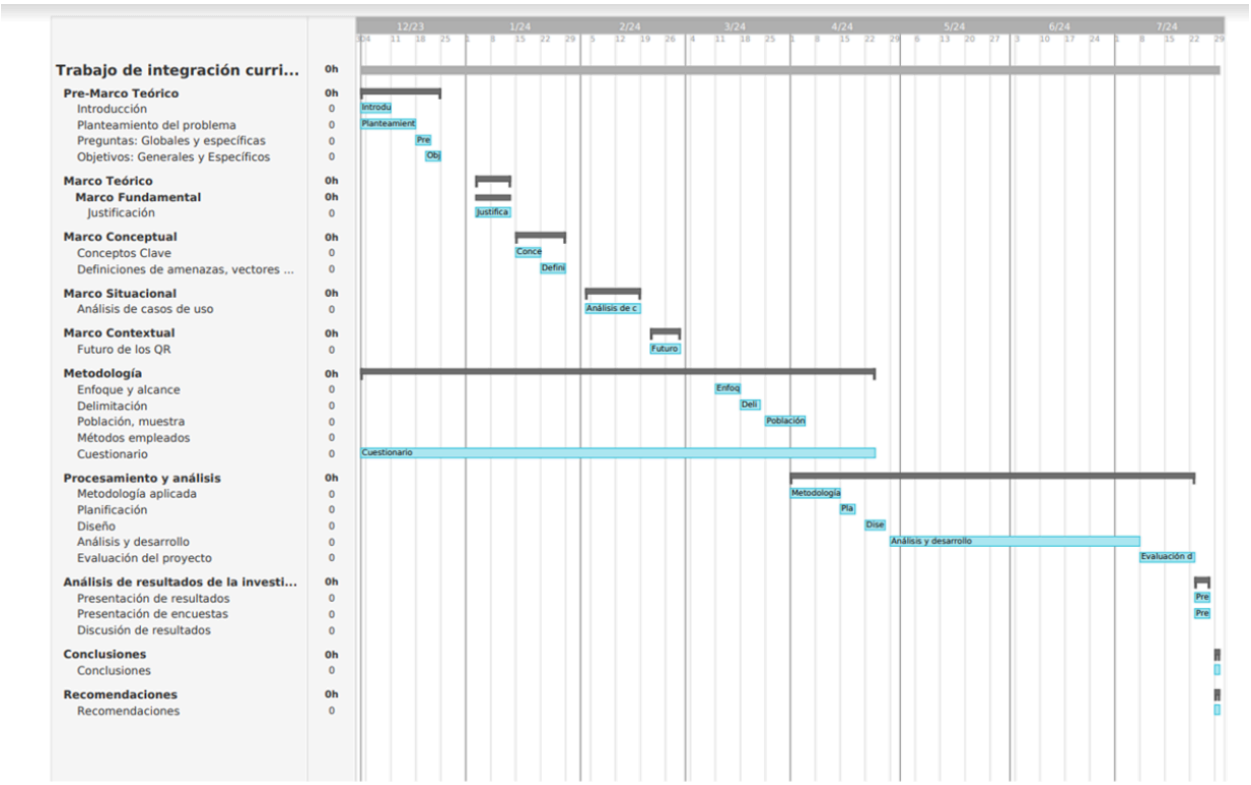
- [ ] Opción 2

- [ ] Opción 3

- [ ] Opción 4

- [ ] Opción 5

7.2. Cronograma Gantt



7.3. Etapas previas del desarrollo: Implementación del algoritmo de seguridad

7.3.1. Conversión de texto plano a texto cifrado sin utilización de vector de inicialización

7.3.2. Generación de código QR (sin mensaje cifrado) sin utilización de vector de inicialización

7.3.3. Generación de QR con mensaje cifrado sin utilización de vector de iniciación

7.3.4. Conversión de texto plano a texto cifrado sin utilización de vector de inicialización