Revista UIS Ingenierías
ISSN: 1657-4583
ISSN: 2145-8456
revistaingenierias@uis.edu.co
Universidad Industrial de Santander
Colombia

Castro-Acuña, Nathaly; Leguizamón-Páez, Miguel; Mora Lancheros, Angie Lizeth
Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR
Revista UIS Ingenierías, vol. 18, núm. 4, 2019, Octubre-Diciembre, pp. 157-172
Universidad Industrial de Santander
Bucaramanga, Colombia

DOI: https://doi.org/10.18273/revuin.v18n4-2019015

Disponible en: https://www.redalyc.org/articulo.oa?id=553764535018

Vol. 18, n.° 4, pp. 157-172, 2019
Revista UIS Ingenierías
Página de la revista: revistas.uis.edu.co/index.php/revistauisingenierias

Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR

Analysis of existing methods and techniques to minimize security problems when using QR codes

Nathaly Castro-Acuña[1a], Miguel A. Leguizamón-Páez[1b], Angie L. Mora-Lancheros [1c]

[1]Universidad Distrital Francisco José de Caldas. Correos electrónicos: [a] nacasacster@gmail.com, [b] maleguizamonp@correo.udistrital.edu.co, [c] almoral@correo.udistrital.edu.co

Recibido: 27 diciembre, 2018. Aceptado: 25 marzo, 2019. Versión final: 16 septiembre, 2019.

Resumen

Este documento permite conocer los códigos QR, su proceso de creación y características de seguridad; evidenciando la acogida que ha tenido al suplir la necesidad de guardar información en poco espacio. No obstante, al ser tan conocido y utilizado, ha sido foco para el robo de información por parte de quienes vulneran los sistema de seguridad de forma ilícita, que han detectado debilidades tanto en la construcción de los mismos como en quienes los usan, implementando ataques como "hombre en el medio", en el cual el atacante puede interceptar mensajes entre dos usuarios o phishing, mediante la redirección hacia páginas web falsas creadas con la intención de obtener datos confidenciales; y realizar robos de información. Por otra parte, se describen algunas formas para proteger tanto el código QR, como la información que contiene y cada uno de los métodos que han sido implementados y recomendados por autores.

Palabras clave: códigos de respuesta rápida; código QR seguro; criptología; seguridad de información; seguridad en códigos QR; usos y aplicaciones de los códigos QR.

Abstract

This document allows knowing about QR codes, their creation process and security features; because it has improved its use supplying the need to store information in a small space. However, because it is so well known and used, it has been a focus for the theft of information by those who violate the security system illegally, who have detected weaknesses both in their construction and in those who use them, implementing attacks as "man in the middle", in which the attacker can intercept messages among phishing users, by redirecting to fake web pages created with the intention of obtaining confidential data; and perform information thefts. Besides, in this document describes some ways to protect both the QR code, and the information it contains and each of the methods that have been implemented and recommended by authors.

Keywords: quick response code; secure QR code; cryptology; information security; QR code security; uses and applications of QR codes.

1. Introducción

En la búsqueda de alternativas para guardar grandes cantidades de información surgieron los códigos bidimensionales, de los cuales hoy en día su uso es notorio en cualquier producto comercial, puesto que es de rápida respuesta, brinda interacción directa con el consumidor, permite con un escaneo el enlace entre el mundo real y el online, entre muchas otras ventajas. Sin embargo, una de sus desventajas relevantes es que ha sido utilizado por intrusos o personas que vulneran de manera ilegal sistemas como vector de ataque para el robo de información [1], por tanto, es importante determinar cuáles son las formas de minimizar estos riesgos de

ISSN impreso: 1657 - 4583. ISSN en línea: 2145 - 8456,
N. Castro, M. Leguizamón, A. Mora, "Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR," *Rev. UIS Ing.*, vol. 18, no. 4, pp. 157-172, 2019. doi: 10.18273/revuin.v18n4-2019015

seguridad y en qué se basa para reducirlos. Este documento se concentra en tres temas relevantes para tener en cuenta: todo lo que se debe saber sobre los códigos QR, la seguridad del símbolo y cómo se puede proteger la información que este contenga.

Este análisis está dividido en cinco partes, como primera parte un contexto histórico, en el cual se describe la transición histórica de los códigos QR desde la década de 1960 hasta el día de hoy; continúa con su proceso de generación y codificación, en donde se resaltan sus características y las razones por las cuales hoy por hoy es el código bidimensional más usado, además del proceso generalizado en la creación de los códigos; como cuarta parte se enfatiza en el tipo de seguridad que se debe aplicar en un código QR ya sea seguridad informática, la cual se encarga solo del medio informático (símbolo del código QR) o seguridad de la información que tiene en cuenta todo lo que contenga, es decir, la protección en el conjunto organizado de datos procesados; como quinta parte se describirán cada una de las técnicas usadas y recomendadas para generar el código QR y buscar formas de ocultar y blindar la información contenida y una comparación entre las técnicas de seguridad informática y seguridad de la información aplicadas en los códigos QR destacadas en este documento. Y por último, se nombran los vectores de ataque, su definición, funcionamiento y en qué ámbitos han sido utilizados al aplicarse en los códigos QR. Lo anterior busca dar un contexto al lector sobre el surgimiento, concepto y formas de ataques de los códigos QR para así conocer las diferentes formas que existen para crearlos de manera segura y las consideraciones que se deben tomar al momento de usarlos y generarlos.

2. Contexto histórico

En la década de 1960, Japón entró en un período de alto crecimiento económico donde los supermercados que surgieron por todos los vecindarios vendían una amplia gama de productos y para las actividades de etiquetado de éstos, el personal del supermercado tenía la tarea de colocar el precio a mano sobre cada uno de los productos, pero debido a la gran cantidad de ventas que tenían debían marcar a diario muchos artículos, generando un desgaste en el personal, por esta razón se identificó la necesidad de crear una herramienta que permitiera etiquetarlos fácilmente. Como solución para ello, surgieron los códigos de barras, los cuales se colocaban en cada uno de los productos y utilizando un sensor óptico que permitía leer el código, el precio se enviaba automáticamente al equipo, proporcionando una solución acertada a esta tarea. [2]

Los códigos de barras, son códigos unidimensionales, que tiene una capacidad de almacenamiento de veinte caracteres alfanuméricos [3]. Teniendo en cuenta que la utilización de los códigos de barras se constituyó en una solución que ayudó a los comerciantes y distintas cadenas comerciales contribuyendo en que funcione la gestión de manera eficiente para una amplia gama de tareas desde la producción hasta el envío y la emisión de comprobantes de transacciones[1] y debido al alto flujo de información se hizo necesario aumentar el tamaño de almacenamiento de éstos. En 1994, Denso Wave Corporation introduce los códigos de barras de dos dimensiones [4], también conocidos como códigos QR o códigos de respuesta rápida como alternativa a este problema, dichos códigos son una matriz bidimensional de puntos que permite almacenar una gran cantidad de información en su interior [5] que puede ser fácilmente leído por la mayoría de los dispositivos modernos (teléfonos móviles y tabletas, entre otros) equipados con cámara. Sin embargo, el dispositivo tiene que tener instalada la aplicación que llevará a cabo el escaneado. QR significa *quick response* por la capacidad de interpretar rápidamente el objeto [6].

Con el paso del tiempo, los códigos QR han ganado y siguen ganando mucha aceptación en industrias tan diversas como la manufactura, almacenamiento, logística, comercio minorista, ciencias de la salud y vida, transporte y automatización, debido a que encontraron en esta tecnología la oportunidad de realizar mercadeo digital tal como mostrar promociones, brindar información publicitaria o compartir grandes cantidades de información cuya facilidad les permitió llegar a más población y así ayudar al crecimiento de la economía y el conocimiento.

Hoy en día estos símbolos su capacidad de almacenar puede ascender hasta los 3 KB, gracias a su capacidad de almacenamiento en dos dimensiones, permitiendo realizar diferentes tipos de transacciones y consultas. El uso de estos códigos también está aumentando gradualmente, por ejemplo, en Medio Oriente y África, de un mínimo del 12% en el primer trimestre de 2017 al 18% en el tercer trimestre de 2018[2]. En Asia su uso es relevante y de gran alcance, por ejemplo, durante el 2016 llegaron alrededor de 5.61 billones de dólares en transacciones por medio del escaneo de estos códigos Además de las transacciones nombradas, se usan para realizar marketing como por ejemplo el caso de

[1] History of QR Code. Disponible en línea en https://www.qrcode.com/en/history/ Fecha de consulta: enero 16 de 2019

[2] ¿Los códigos QR harán una reaparición en 2019? Disponible en línea en https://blog.globalwebindex.com/trends/qr-codes-2019/ Fecha de consulta: mayo 06 de 2019

McDonald's, colocando los códigos QR en las tapas de las bebidas y bolsas de papel que una vez escaneados muestran información sobre el valor nutricional de sus comidas[3]; así mismo, permite a los clientes realizar pedidos a domicilios mediante un escaneo de códigos QR[4].

Es importante traer a colación que se han desarrollado distintos códigos que permiten diferentes tamaños de almacenamiento, siendo el propuesto por Denso Wave el que permite mayor almacenamiento de información. Actualmente existen más de veinte tipos de códigos bidimensionales, en la tabla 1 se resume las características de algunos códigos gráficos de almacenamiento de información.

Tabla 1. Comparativo de los distintos códigos de dos dimensiones que se han desarrollado

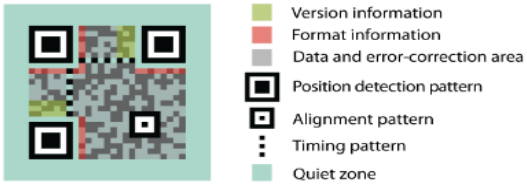
		QR Code	PDF417	DataMatrix	MaxiCode
					
Developer		DENSO Wave	Symbol Technologies	RVSI Acuity CiMatrix	UPS
Type		Matrix	Stacked barcode	Matrix	Matrix
Data capacity	Numeric	7,089	2,710	3,116	138
	Alphanumeric	4,296	1,850	2,355	93
	Binary	2,953	1,018	1,556	-
	Japanese, Chinese or Korean characters	1,817	554	778	-
Main features		Large capacity, small size, high-speed scanning	Large capacity	Small size	High-speed scanning
Main applications		All categories	Office automation	Factory automation	Logistics
Standards		AIM, JIS, ISO	AIM, ISO	AIM, ISO	AIM, ISO

Fuente: Denso Wave

Los códigos QR se destacan por permitir almacenar información en los dos sentidos; horizontal y vertical, por ende se denominan como códigos bidimensionales, contrario a los códigos de barras los cuales solo permiten almacenar la información sobre su eje horizontal.

En la figura 1, se puede observar que el código QR está compuesto por distintos módulos, cada uno de ellos, dependiendo su color, oscuro o claro, puede representar un 1 o 0. Así mismo, consta de un módulo cuadrado nominal o zona de tranquilidad que forma una matriz cuadrada que incluye: un patrón de posición, un patrón de alineación, un patrón y un separador de detección de posición y un formato de codificación que incluye, la versión de la información y el código de corrección de errores [7].

Figura 1. Composición de un código QR



Fuente: Denso Wave

Finalmente, de acuerdo a la definición dada por la ISO/IEC 18004:2006 el código QR (Quick Response Code) es una representación gráfica bidimensional (alto x ancho) de datos basada en la disposición de múltiples formas geométricas sencillas en un espacio fijo. Básicamente es un código de barras bidimensional que sirve para almacenar información y que hoy puede ser fácilmente leído por la mayoría de dispositivos modernos equipados con cámara. Su sigla QR significa *quick response* por la capacidad de poder interpretar el objeto rápidamente el objeto [6]. Y sus principales características son alta velocidad de decodificación, bajo coste del decodificador, facilidad de lectura, gran capacidad de codificación de datos, codificación extendida, gran resistencia frente a errores, posibilidad de personalización y adaptación al tamaño de los datos [8].

3. Proceso de codificación

La codificación de un código QR se puede realizar en 7 pasos básicos [7] que varían dependiendo de la seguridad que se implemente en los mismos:

- Análisis de la información: Se realiza un análisis del flujo de datos de entrada, se determina el tipo de carácter del código, se convierte el conjunto de caracteres al carácter de símbolo y por último se selecciona el nivel de corrección de errores.
- Codificación de los datos: Se realiza la conversión de los datos de entrada en un flujo de bits, cada palabra de código contiene 8 bits, todas las palabras de código forman una secuencia de palabras de datos.

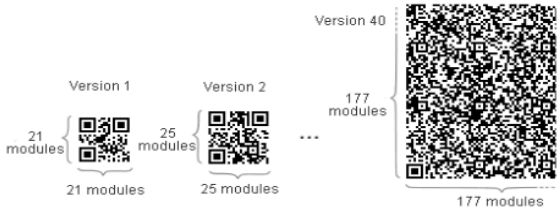
[3] Los códigos QR ahora llegan a McDonald's: sus bolsas y vasos tendrán información nutricional. Disponible en línea en https://www.iprofesional.com/notas/152958-Los-codigos-QR-ahora-llegan-a-McDonalds-sus-bolsas-y-vasos-tendran-informacion-nutricional Fecha de consulta: enero 16 de 2019

[4] 15 usos de códigos QR para un restaurante. Disponible en línea en https://www.diegocoquillat.com/15-usos-de-codigos-qr-para-restaurante/ Fecha de consulta: enero 16 de 2019

- Codificación de corrección de errores: En este paso se usa el algoritmo para generar el código de corrección de errores.
- Se construye la secuencia final de la palabra del código de datos.
- Se construye la matriz: Para este paso, se adiciona al código QR el patrón de posicionamiento, el patrón de corrección, el patrón y el separador de detección de posición, y el módulo de palabra de código en la matriz.
- Enmascaramiento: Se adiciona el patrón de máscara, el cual se utiliza en la región de codificación del patrón de código QR, para que así los módulos oscuros o claros puedan distribuirse de la mejor manera en el código QR.
- Información de formato y versión: Se genera la información de formato y versión, y se adiciona en el área correspondiente para generar gráficos de código QR.

Es posible generar hasta 40 diferentes versiones de códigos QR, cambiándole el número de módulos iniciando con un tamaño desde 21 x 21 módulos siendo esta la versión 1, hasta de 177 x 177 módulos que corresponden a la versión 40 [4] como se muestra Figura 2.

Figura 2. Versiones de códigos QR



Fuente: Tomado de Denso Wave

Para la generación de cada versión de símbolo superior, se adicionan 4 módulos adicionales por lado, es decir, 16 módulos adicionales por código, lo que permite llegar a contener una cantidad de datos considerablemente mayor que determina su versión, tipo de caracteres y nivel de corrección de errores.

4. Seguridad informática y de la información

Desde hace poco más de dos décadas se ha popularizado el tema de seguridad de la información principalmente por el uso masivo de internet, por supuesto hay diferencias entre los modos de seguridad en la década del 70 y los que se presentan en la actualidad, pero su definición es la misma, siendo el conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información [9].

Existen diferencias entre seguridad informática y seguridad de la información que generalmente se confunden, aunque parezcan muy parecidos. La informática es la ciencia encargada de los procesos, técnicas y métodos que busca procesar almacenar y transmitir la información, la seguridad informática se encarga de la seguridad de los medios informáticos, mientras que la seguridad de la información, se preocupa por todo aquello que pueda contener información [10] no solo por el medio informático, por ende es importante entender estas diferencias, con la finalidad de evidenciar que se debe proteger y a que se hace referencia cada terminología, ya que los códigos QR hacen uso de los medios informáticos para permitir su creación y lectura almacenando grandes cantidades de datos organizados y procesados.

4.1. Seguridad en código QR

Es importante aplicar seguridad informática al momento de generar los códigos QR y para ello se puede hacer uso de varias técnicas. A continuación, se detallan específicamente dos: la técnica de corrección de errores (Esta se encuentra ya estandarizada al momento de crear los códigos QR) y la técnica de colores (permite enmascarar la información por medio de la asignación de colores), así como el uso de una técnica desarrollada donde se usa la secuencia de sudokus que permiten tener en cuenta al momento de crear un código QR con información importante y segura.

4.1.1. Técnicas de corrección de errores

Ante la presencia de ruido o daño parcial del símbolo, los códigos QR proveen corrección de errores [11] [12] los cuales se clasifican por niveles que pueden ser escogidos en el momento en el cual se genera un símbolo (código QR) y éste varía dependiendo de la cantidad de información que admite el código [13]. Dichos niveles son L, M, Q y H, que permiten la corrección desde un 7% a un 30% aproximadamente, como se puede apreciar en la tabla 2 [14]. De acuerdo con [13] el nivel más usado es el M (15%), los niveles Q y H son elecciones normales para un ambiente industrial donde el código QR suele ensuciarse, en cambio el nivel L es para lugares que normalmente son limpios donde normalmente la información contenida es mayor.

Tabla 2. capacidad de corrección de error de los códigos QR

Nombre del nivel	Nivel	Corrección de error (aproximado)
Low	Nivel L	7%
Medium	Nivel M	15%
Quality	Nivel Q	35%
High	Nivel H	30%

Fuente: elaboración propia.

Uno de los métodos más conocidos que se añade a la corrección de errores es implementar código Reed-Solomon (RS) a los datos originales buscando protegerlos contra la distorsión de la información de los datos transmitidos sobre un canal de comunicaciones. RS "es un método matemático de corrección de errores usado en CDs (...) que tiene la capacidad de crear una corrección a nivel bit y situarlo en el lugar del error" [13]. Aunque los códigos RS pueden garantizar una cierta cantidad de corrección de errores, su alta complejidad de codificación y decodificación, por el número de iteraciones que este usa y su incapacidad para emplear longitudes de código flexibles, constituyen sus principales desventajas [15].

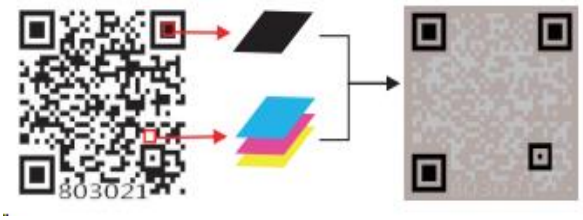
4.1.2. Técnicas de colores

Asegurar un código QR es posible también mediante la implementación de técnicas de color. [16] Los denominados códigos QR visuales, "en caso de un escenario de ataque, puede reducir significativamente el riesgo de ataque o modificación" y su manera de uso es mediante un esquema e incrustación de color y textura sobre el símbolo [17].

La anterior no es la única forma de asegurar un código QR donde se implementa el uso de colores, también se pueden usar técnicas de marca de agua como se ilustra en la figura 3, cuya lectura se realiza mediante infrarrojo como indican [18] sí se adicionan características ópticas de K, teniendo en cuenta que K es la única forma de ser visible el infrarrojo o lo que se denomina renderizado, una de las cuatro tintas CMYK, puede absorber el infrarrojo.

Adicionalmente, como sostienen [15] en su estudio *"Secured graphic QR code with infrared watermark"* las posibilidades de detectar información oculta de esta manera, por infrarrojo, es más difícil. Esto debido a que solo la información implícita en QR puede ser exitosamente detectada por un teléfono móvil (como el Lumigon T3[5] o Honor 10[6] que poseen la características de potentes infrarrojos) cuando la intensidad del infrarrojo es de 80 a 120 voltios con una imagen de alta calidad mejorando así su seguridad. Cabe acotar que esta técnica también la planteó [19] donde logró una combinación de sistemas de seguridad para el diseño de una marca de agua que contenga un código QR cifrado que puede ser perceptible o imperceptible dependiendo cuanta información se quiera ocultar en el patrón de difracción donde la generación de este patrón es mediante el uso de transformada de Fourier.

Figura 3. Código QR generado implícito en CMYK



Fuente: Wang, Sun, Kuan, Lu, & Wang

Una de las aplicaciones que usa esta técnica es la publicada en el Simposio de Telecomunicaciones Móviles [20] donde exponen su aplicación ColorQR, la cual envía datos a través de la manipulación de colores en Códigos QR multiplexados, estos datos se codifican en los colores rojo, azul y los códigos QR en color verde y se multiplexan para formar múltiples códigos QR los cuales se mostrarán en la pantalla del dispositivo del remitente. El receptor, en forma de cámara de un dispositivo móvil, grabará las imágenes parpadeantes y convertirá las imágenes en canales RGB usando conversión de escala de grises. Así, una imagen se dividirá en 3 conjuntos de códigos QR en blanco y negro esto con el fin de enmascarar su información y hacer más difícil su proceso de decodificación puesto que solo con su aplicación pueden obtener la información contenida.

4.1.3. Otras técnicas

Entre la creatividad de muchos autores, se evidencian modernas técnicas que permiten que un código QR sea aún más seguro. Una de éstas es la propuesta por los chinos Peng-Cheng, Chin-Chen y Yung-Hui en el libro *Multimedia Tools and Applications* en 2018, donde

[5] Lumigon T3: el primer móvil con cámara de visión nocturna es real y tiene una versión con oro. Disponible en línea en https://www.xatakamovil.com/otras/lumigon-t3-el-primer-movil-con-camara-de-vision-nocturna-es-real-y-tiene-una-version-con-oro Fecha de consulta: 21 febrero de 2019

[6] Conocerás los Mejores Celulares Infrarrojo. Disponible en línea en https://infrarrojos.online/celulares-infrarrojo/ Fecha de consulta: 21 de febrero de 2019

proponen como base de la generación del símbolo un intercambio de mensajes secretos basado en el sudoku[7]. Lo interesante de este método es que el número total de posibles soluciones para un sudoku de 9×9 es de 6.671×1021 [21], y al implementarlo en la generación del símbolo del código QR permite reforzar la seguridad y superar cualquier debilidad.

El planteamiento de su modelo propone proteger el mensaje de privacidad propio del código QR con el fin de prevenir el acceso a personas no autorizadas, dado que se valida la legitimidad de quien quiere acceder a la información, esto lo realizan con el uso de mensajes o llaves privado(a)s o secreto(a)s y público(a)s. Los mensajes secretos se dividen en varias sombras y se ocultan en el código QR mediante sustitución de los bits de mensaje público del código QR [21].

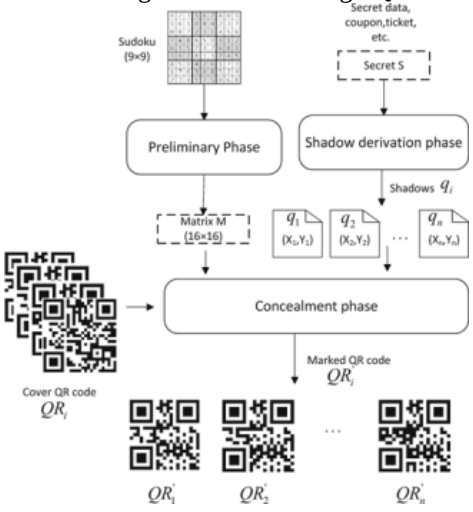
La figura 4 evidencia el marco propuesto. Este consiste en un sistema de intercambio, en donde hay un distribuidor (*dealer*) y n participantes. El distribuidor es responsable de dividir y ocultar el mensaje secreto en n códigos QR marcados y luego los distribuye a cada participante, respectivamente. El mensaje secreto compartido solo se puede reconstruir cuando todos los n códigos QR marcados se muestran juntos (figura 5). De acuerdo con los autores, ningún subconjunto de menos de n códigos QR marcados puede filtrar cualquier parte del mensaje secreto. Agregan que este nuevo esquema puede detectar a quienes no tienen la legitimidad para acceder o intentar robar la información e identificarlos, y se puede aplicar a código QR con valor agregado, como el intercambio de mensajes secretos distribuidos, boletos electrónicos y cupones electrónicos [21].

Después de varias pruebas realizadas por Peng-Cheng, Chin-Chen y Yung-Hui, concluyen en su estudio que el esquema propuesto es factible con alto nivel de protección de seguridad y resistente a las normas comunes de ataques de pos-procesamiento de imágenes.

4.2. Seguridad de la información contenida

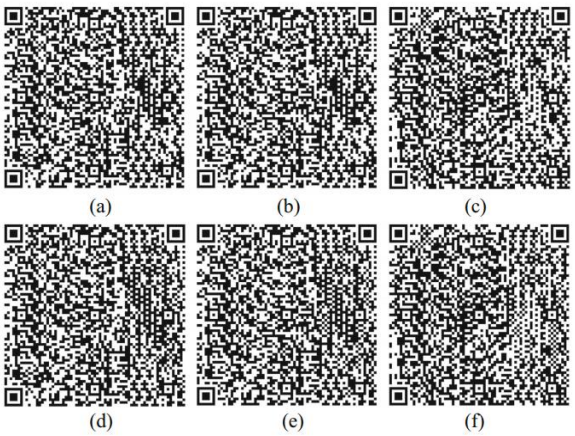
Teniendo en cuenta que el código QR es uno de las formas donde se puede almacenar información, es necesario aplicar seguridad. Durante su creación se usan distintas técnicas que aplican seguridad informática en éste, pero es importante incluir también seguridad en la información que este contiene. Por ello, para minimizar el riesgo y en pro del cuidado de la información sensible que este puede contener, se usan distintas formas de cifrado, lo cual es un procedimiento que permite transformar el mensaje o la información contenida, de manera que sea incomprensible a simple vista, en este caso con el escaneo del código QR. Para esto se pueden usar dos técnicas que se complementan, pero cumplen la función de cifrar y proteger la información: los métodos de cifrado y estenografía.

Figura 4. Diagrama de flujo del sistema propuesto en la fase de generación de código QR.



Fuente: Peng-Cheng, Chin-Chen & Yung-Hui

Figura 5. Ejemplo del esquema de intercambio de mensajes secretos por varios participantes para QR versión 13-H. (a – c) Cubierta Código QR 1,2 y 3. (d) Código QR marcado de (a). (e) Código QR marcado de (b). (f) Código QR marcado de (c)



Fuente: Peng-Cheng, Chin-Chen, & Yung-Hui

[7] Originó en el siglo XVIII en Suiza, se desarrolló en Estados Unidos y en 1986 en Japón se conoció con el nombre de Sudoku.

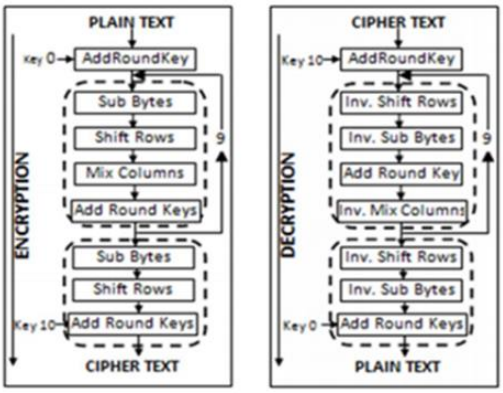
4.2.1. Métodos de cifrado

De acuerdo a la literatura [22] y [23], los métodos de cifrado más usados son AES (*Advanced Encryption Standard*), RSA (Rivest, Shamir y Adleman), y un método de cifrado ajustado, que contiene varios de estos, planteado por [23] que denomina SQR (*Secure QR*), donde usa un estándar avanzado de cifrado.

A continuación se describe a grandes rasgos cada uno de ellos.

a. AES: El proceso de cifrado de AES inicia con adicionar una ronda de llaves en la primera etapa, siguiendo con nueve rondas de cuatro etapas y luego con diez rondas de tres etapas, para descifrar el procedimiento se lleva a cabo el mismo procedimiento, pero al revés. En la figura 6, se pueden evidenciar las etapas que cada una de estas rondas que se tienen contempladas tanto para el proceso de cifrado como descifrado.

Figura 6. Proceso de cifrado y descifrado de AES



Fuente: Goel, Sharma, & Goswami

Como se evidencia en la figura 6. AES usa una estructura de bucle donde se realiza repetidamente reordenamientos de datos y permutaciones. El bucle se reemplaza una unidad de datos con otra para datos de entrada y aplica una misma clave con una longitud fija. Básicamente, la rutina de cifrado de AES almacena la clave de cifrado principal en una matriz. Una matriz es un grupo de objetos con los mismos atributos que pueden ser abordados de forma individual. La matriz consta de cuatro filas, conteniendo cada uno cuatro, seis u ocho bytes, dependiendo del tamaño de la clave.

AES utiliza una clave de cifrado que puede ser 128, 192 o 256 bits de largo, y se aplica en unidades de datos, llamados bloques, cada uno de los cuales es de 128 bits de largo. El algoritmo AES comienza copiando cada bloque de 16 bits en una matriz bidimensional llamada el Estado, para crear una matriz de bytes de 4x4. El algoritmo realiza una operación exclusiva "O" que devuelve "verdadero" si uno u otro de sus operandos es verdadero. Esto se conoce como "*AddRoundKey*", y está entre las primeras cuatro filas del programa clave y la matriz de Estado. Luego de la operación exclusiva, el algoritmo entra en su bucle principal, en el que realiza repetidamente cuatro operaciones matemáticas diferentes en la matriz de Estado: "*SubBytes*", "*ShiftRows*", "*MixColumns*" y "*AddRoundKey*". Estas operaciones emplean una combinación de suma, multiplicación, rotación y sustitución para cifrar cada byte en la matriz de Estado. El bucle principal se ejecuta 10, 12 o 14 veces dependiendo del tamaño de la clave de cifrado. Una vez que se completa la ejecución, el algoritmo copia la matriz de estado a su salida en forma de texto cifrado[8]. Para el caso de descifrado el proceso es inverso.

b. RSA: Es el algoritmo de clave asimétrica más popular. Su seguridad se basa en la dificultad de la factorización de grandes enteros. La fuerza de seguridad de RSA reside en la longitud de sus llaves. Cuanto más grandes son las llaves, más seguro es.

El algoritmo RSA está basado en la factorización de enteros y es asimétrico, el cual utiliza dos claves, una pública y otra privada, como su nombre lo indica la clave pública es conocida por todos. Para el cifrado, el remitente cifra el mensaje utilizando la clave pública del receptor, el texto cifrado generado es entonces descifrado por el receptor utilizando su propia clave privada.

El algoritmo RSA se divide en 3 partes: generación de claves, cifrado y descifrado:

Generación de claves: Los pasos para la generación de claves son los siguientes:

1. Dos números primos, p y q, de longitudes aproximadamente iguales, generadas de forma aleatoria.
2. Calcular $n = p * q$
3. Calcular la función de Euler, $\varphi\,(n) = (p-1) * (q-1)$
4. Elija un número entero e tal que satisfaga lo siguientes dos condiciones:
   a. $l < e < \varphi(n)$
   b. $GCD\big(e, \varphi(n)\big) = 1$

[8] Dunning, David. ¿Cómo funciona AES? Techlandia.com. Disponible en línea en https://techlandia.com/funciona-aes-info_215975/ Fecha de consulta: abril 26 de 2019.

5. Calcular d tal que sea el inverso multiplicativo de $e-1$, es decir, $d \equiv e-1\ (mod\ \varphi(n))$ Esto significa $e.d \equiv 1\ (mod\ \varphi(n))$
6. (e,n) y (d,n) son la clave pública y la clave privada (del receptor) respectivamente.

Cifrado: Los pasos para el cifrado son los siguientes:

1. El remitente primero obtiene la clave pública del receptor (n,e).
2. El mensaje a cifrar se representa como un número entero m tal que $m > 0$ y m se encuentra el intervalo $(0, n-1]$.
3. El remitente luego calcula la cifra c que es $me\ (mod\ n)$.
4. El cifrado c se envía al receptor para su descifrado.

Descifrado: Los pasos para el descifrado son los siguientes:

1. El receptor al generar sus claves públicas y privadas, recibirá el cifrado del remitente.
2. El cifrado será descifrado como $m = cd(mod\ n)$

Cabe anotar, que los pasos involucrados en el cifrado y descifrado pueden parecer fáciles de calcular al principio, pero el reto es implementar potenciación modular para tales números primos grandes y así hacerlo aún más robusto.

RSA es computacionalmente intensivo para implementar ya que implica cálculos pesados, dado que el tamaño de la clave es 1024 bits, no es posible calcular el cifrado y el mensaje descifrado por medio de una manera directa de calcular la exponenciación [23].

c. SQR: Este método de cifrado fue planteado con el fin solucionar problemas de seguridad en los códigos QR, el cual sus autores nombran *Secure a QR Code (SQR).* El enfoque que describen es asegurar un código QR con la ayuda de una clave en el lado del generador y la misma clave se usa para obtener la información original en el lado del escáner, utilizando el algoritmo AES para este propósito [22] cuyo proceso se describe en la figura 6. Sin embargo, su propuesta se describe en el siguiente orden:

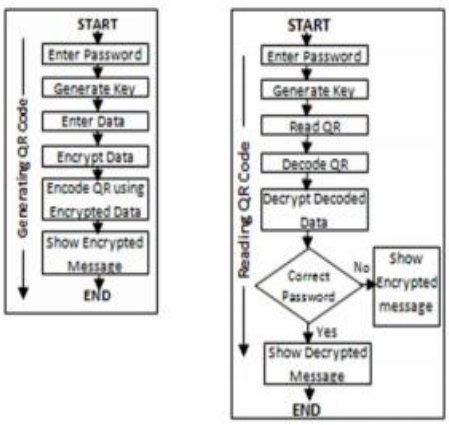
Generador del código QR

1. Ingresar la contraseña para cifrar la información
2. Una clave de 128 bits es generada desde la contraseña
3. Ingresa la información para el código QR
4. Los datos son encriptados con AES y embebido en el código QR
5. El código QR es generado.

Escáner de código QR

1. Escanear el código QR
2. Ingresar la contraseña
3. Una clave de 128 bits es generada desde la contraseña
4. El código QR es decodificado y los datos descifrados usando la clave
5. Sí la contraseña ingresada es correcta entonces la información verdadera se muestra, de otra manera la información es incorrecta.

Figura 7. Propuesta de Goel. Et al. En la generación y escaneo de códigos QR



Fuente: Goel, Sharma, & Goswami

En el documento de [22] concluyen que para minimizar el tiempo del proceso es necesario utilizar de manera paralela el método de cifrado de encadenamiento por bloques, incorporando un hash adicional para verificar si la información incrustada en el código QR está intacta.

4.3. Esteganografía visual y digital

Otra técnica para mantener la seguridad de la información es mediante su ocultamiento. Una de las formas de realizarlo es a través de la esteganografía[9], la cual no solo busca modificar la información sino ocultar su existencia [24].

[9] La estenografía proviene del griego *steganos* que quiere decir oculto y *graphos* que es escritura, es decir, puede decirse que es la ciencia de la escritura encubierta. [36]

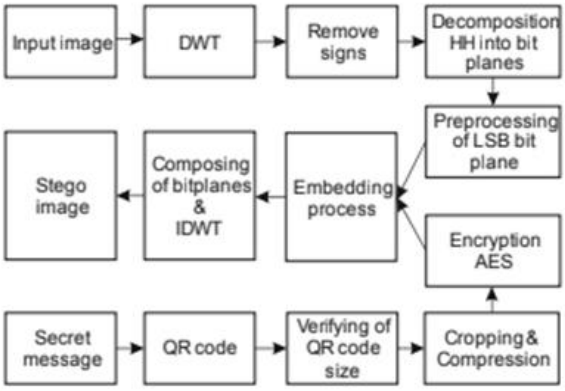
La implementación de la esteganografía visual en los códigos QR, se realiza utilizando códigos Reed–Solomon[10] en su corrección de errores, y obteniendo una imagen que pueda ser interpretada adecuadamente. Es importante tener en cuenta que la cantidad de datos que se pueden almacenar en el símbolo del código QR depende del tipo de datos (modo o conjunto de caracteres de entrada), versión (1, 2, ..., 40, que indica las dimensiones generales del símbolo) y el nivel de corrección de errores, que indican la medida de la posible interrupción del código QR, además que el ancho del módulo estándar puede ser diferente puesto que cuanto más grande es un módulo, más estable y fácil de leer se convierte en un escáner de código QR.

El procedimiento planteado por [25] para embeber un mensaje secreto en forma de QR en una imagen estática contiene los pasos que se describen a continuación, también se muestra el proceso en la figura 8.

1. Cargar los datos de entrada, imagen y código QR.
2. Verificar el tamaño del código QR.
3. Recortar los espacios en blanco desde el código QR (cuatro bits) de todos lados. Posteriormente, los bits adyacentes de cada módulo en el código QR se reemplazan por un bit con valor específico con el fin de lograr compresión del código QR. El tamaño del módulo depende de la opción del usuario.
4. Obtención de tamaño de código QR recortado. Esta información de tamaño se insertará en los coeficientes de transformación de la imagen como primero.
5. La imagen de entrada se transforma en el dominio LDWT[11] mediante funciones de Haar (cuatro sub-imágenes LL (Low-Low), LH(low-high), HL(high-low), HH(high-high)[12] .
6. Determinar el tamaño de la sub-imagen HH, donde se incrusta el mensaje secreto.
7. Los signos de los coeficientes de transformación específicos se almacenan en la matriz de signos.
8. Posteriormente, los signos de los coeficientes de transformación se eliminan y la sub-imagen HH se descompone en planos de 8 bits.
9. La incorporación del código QR se realiza en el plano de bits LSB de la sub-imagen HH, donde los bits LSB[13] se reemplazan por bits cifrados de código QR. La sustitución de bits se implementa desde la tercera fila y la segunda columna de la matriz HH debido a la preservación de las características estadísticas de la imagen.
10. Después de incrustar, el plano de bits LSB modificado se compone en sub-imagen HH.
11. El DWT inverso se aplica en la sub-imagen HH modificada y HL original, LL a sub-imágenes LH
12. Después de la implementación de estos pasos, se crean imágenes *stego*, es decir, imágenes con un mensaje secreto incrustado en forma de código QR.

Y para obtener el mensaje secreto a partir de la imagen de *stego* mediante un algoritmo de extracción del método esteganográfico propuesto, el proceso se basa en operaciones de inversión considerando el algoritmo de incrustación. Finalmente, el código QR obtenido puede ser leído por un dispositivo de imágenes (es decir, un teléfono inteligente), donde se adquiere un mensaje secreto en forma de texto o datos.

Figura 8. Diagrama de bloque de procesos propuesto para realizar estenografía en un código QR



Fuente: Hajduk, Broda, Ondrej, & Levický

De acuerdo a [25] con un proceso de incrustación y compresión se logra adicionar imágenes con un mensaje

[10] Los códigos Reed-Solomon se introdujeron en 1960 y utilizan polinomios sobre campos finitos para corregir los datos faltantes. Se pueden encontrar en tecnologías como DVD, sistemas de transmisión y almacenamiento de computadoras y es el modo de corrección de errores de los códigos QR. [12]

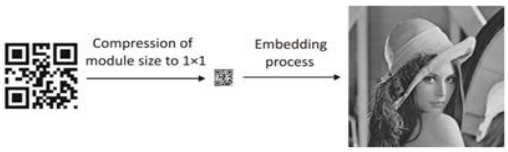
[11] La DWT (Discrete Wavelet Transform) es una herramienta matemática que se utiliza, entre otras cosas, para representar señales por niveles de resolución. Así, por ejemplo, si calculamos la DWT de una imagen obtendremos un conjunto de coeficientes DWT que descomprimidos por sub-bandas sucesivas permitirán aumentar progresivamente la resolución espacial de la imagen descomprimida. [32]

[12] Etiquetas de *array* de coeficientes contenidas en cuatro bandas de datos en una imagen [34]

[13] LSB, el bit menos significativo es el bit más bajo en una serie de números en binario; el LSB se encuentra en el extremo derecho de una cadena. Por ejemplo, en el número binario 10111001, el bit menos significativo es el extremo derecho 1. [36]

secreto incrustado en forma de código QR como se muestra en la Figura 9.

Figura 9. Comprensión del tamaño de un módulo



Fuente: Hajduk, Broda, Ondrej, & Levický

La anterior, es una forma donde se puede insertar un código QR con información en una imagen y que este no sea perceptible con facilidad para el ojo humano. Otra manera de asegurarlo es mediante la estenografía de espectro, que como su nombre lo indica, el mensaje se propaga y luego se agrega para cubrir los datos. [26]

Las técnicas de estenografía de espectro extendido se utilizan ampliamente en las radiocomunicaciones militares, debido a su gran robustez para la detección y extracción del mensaje secreto o información contenida. Las ventajas de este tipo de técnicas es que promueven un método de ocultación en imágenes estáticas usando los principio de algoritmos en la preservación de las características de la imagen después de la incrustación de mensaje secreto y una de las formas de leer esta información es mediante el escaneo con infrarrojo, algo que es más difícil para quien quiera obtener la información del código QR [25].

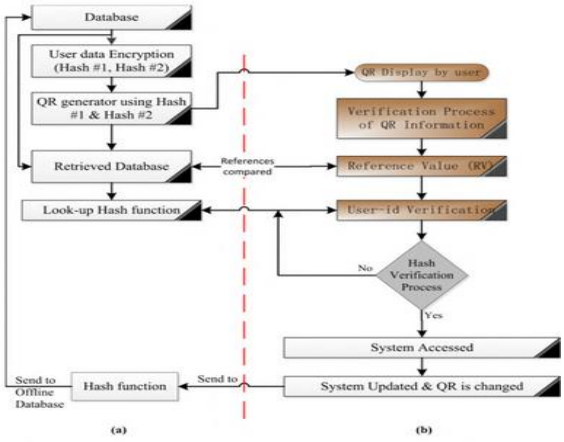
4.4. Algoritmo de verificación inteligente (SVA)

Con el fin de aumentar la privacidad y confidencialidad de la información, [27] ha propuesto un algoritmo de verificación inteligente (SVA por sus siglas en inglés *Smart Verification Algorithm*) para que sea utilizado en las aplicaciones de Internet de las cosas (IoT) realizando un procedimiento de verificación para permitir que el usuario acceda a un sistema inteligente con el uso de códigos QR. El SVA propone un escáner de etiquetas QR simple y confiable para verificar su contenido en términos de autenticación. Además, el procedimiento de verificación de SVA contiene tres capas para aumentar la seguridad: en la primera capa, implementa una comparación para preservar el sistema integrado; en la segunda, los valores originales son guardados en una base de datos offline con el fin de deshabilitar cualquier acceso provocado por amenazas; y la tercera, genera una autenticación con código QR usando sesión con una llave privada para prevenir la fuga de información y un acceso no autorizado si la llave llega a ser conocida, esto para mantener la confidencialidad que el algoritmo SVA ofrece, incrementando la privacidad del sistema [27].

La arquitectura de SVA se basa en que una vez el QR es escaneado, su información debe ser verificada y este será un valor de referencia que será proporcionado al usuario para aumentar su acceso seguro, luego, el id será verificado y finalmente la base de datos estará actualizada con base a los criterios de seguridad. En la figura 10 se evidencia la arquitectura propuesta por [27].

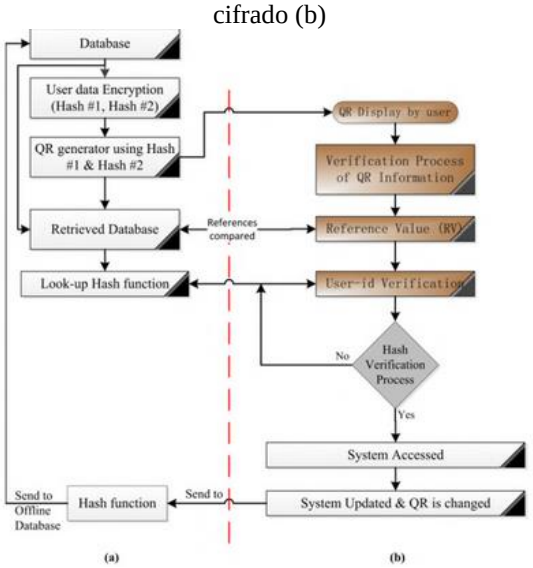
Este algoritmo está orientado principalmente a uno de los usos que se presentan hoy en día y es la unión de códigos QR con Internet de las cosas, y la responsabilidad de SVA recae en que se procesa la información de la manera adecuada para dar acceso, pero este tiene un proceso de cifrado previo como se puede observar en la figura 10 que permite identificar el proceso cifrado de SVA.

Figura 10. Arquitectura del algoritmo SVA



Tomado de Abbas M. Al-Ghaili

Figura 11. Procedimiento de verificación SVA (a) y cifrado (b)



Tomado de Abbas M. Al-Ghaili

4.5. Comparación entre tipos de seguridad aplicados en códigos QR

Teniendo en cuenta los tipos de seguridad que aplican en los códigos QR se puede realizar las comparaciones que se evidencian en la tabla 3.

Haciendo un análisis de la información contenida en la tabla 3, se concluye que la mejor opción es usar una técnica de cifrado de seguridad informática, considerando que RSA es uno de los métodos con mayor robustez, es una de las opciones que más se usan, además de una corrección de errores con los más altos niveles, esto para un código relativamente sencillo; pero el usar las técnicas de colores, o el método basado en sudoku le da más robustez al código QR y aún más si se incluyen el tema de la estenografía.

Tabla 3. Recopilación de seguridad informática y de la información en códigos QR

Seguridad informática (asociada a la que se aplica en la generación del código QR)	**Nombre**	**Características principales**
	Técnicas de corrección de errores	Se clasifican por niveles que pueden ser escogidos en el momento en el cual se genera un símbolo (código QR) y éste varía dependiendo de la cantidad de información que admite el código, para determinar el nivel se usa el método de códigos de Reed-Solomon.
	Técnicas de colores	Su manera de uso es mediante un esquema e incrustación de color y textura sobre el símbolo, también se pueden usar técnicas como marcas de agua cuya lectura se realiza mediante infrarrojo, donde se adicionan características ópticas de K, teniendo en cuenta que K es la única forma de hacer visible el infrarrojo o lo que se denomina renderizado.
Seguridad de la información (asociada a la que se aplica para salvaguardar la información contenida en el código QR)	Método de cifrado AES	AES por las siglas en inglés de *Advanced Encryption Standard*. Se caracteriza por su esquema de rondas de bloques de cifrado con claves de mínimo de 128 bits a 256 bits.
	Método de cifrado RSA	Algoritmo basado en la factorización de enteros y es asimétrico, el cual utiliza dos claves, una pública y otra privada. Es computacionalmente intensivo para implementar ya que implica cálculos pesados, dado que el tamaño de la clave es 1024 bits.
	SQR	Sus autores le ponen esta abreviatura por su nombre Secure a QR Code. El enfoque que describen es asegurar un código QR con la ayuda de una clave en el lado del generador y la misma clave se usa para obtener la información original en el lado del escáner, utilizando el algoritmo AES. Y sugieren adicionar un método de cifrado de encadenamiento por bloques, incorporando un hash adicional.
	Esteganografía visual y digital	El objetivo de esta técnica es embeber un mensaje secreto en forma de QR en una imagen estática, mediante pasos y características propias de la generación de imágenes con el fin que sea imperceptible.
Híbrido (Seguridad de la información e informática)	Algoritmo SVA	Es un algoritmo propuesto para usar códigos QR en aplicaciones de internet de las cosas donde lo que se busca es plantear no solo la arquitectura de seguridad informática propia de IoT como del QR, así como aumentar la privacidad y confidencialidad de la información con un método de cifrado propio de los autores que lo proponen.

Fuente: elaboración propia.

5. Códigos QR como vectores de ataque

Un vector de ataque es literalmente un agujero presente en la defensa establecida, tales fallas pueden ser el filtrado de información por parte de un doble agente y una debilidad en la transmisión de un mensaje ultra secreto, entre otros. Los vectores de ataque en ciberseguridad explotan las debilidades propias de los usuarios[14]. Una de las prácticas más populares en ingeniería social es el *phishing* de acuerdo a [28] quienes indican que los atacantes usan códigos QR maliciosos para dirigir los usuarios a sitios web fraudulentos que se hacen pasar por sitios web legítimos con el objetivo de robar información personal confidencial como nombres de usuario, contraseñas o información de tarjetas de crédito.

[14] Ojeda, Marcia. ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales? Fecha de publicación: mayo 2 de 2018. Fecha de consulta: abril 02 de 2019. Disponible en línea https://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/

Según Krombholz .et al, existen dos vectores de ataque principales donde se usan los códigos QR:

a. El atacante reemplaza todo el código QR: Este ataque es simple pero efectivo. Un atacante crea un nuevo código QR con un enlace malicioso codificado y lo pega sobre uno ya existente en un anuncio de cartelera, por ejemplo.

En este tipo de vulnerabilidad generalmente, el vector de ataque es manipular el QR Code para añadir código malicioso que explota la técnica de *SQL Injection*, es decir, si el proceso que realiza la lectura de QR Code no lleva a cabo una limpieza y revisión adecuada de los datos de entrada, podría sufrir un ataque *SQL Injection* desde un código QR.

O si el código QR es utilizado para introducir parámetros en instrucciones que se ejecutan en la línea de comandos de un Sistema Operativo (terminal de consola), que no están siendo correctamente sanitizados, un QR manipulado podría explotar esa vulnerabilidad para realizar ejecución arbitraria de comandos, ataques de denegación de servicio (DoS), o incluso la instalación de troyanos (rootkits)[15].

b. El atacante modifica módulos individuales de un código QR. La idea principal de esta modificación es que el contenido codificado se modifica únicamente cambiando el color de los módulos específicos del Código QR al que se dirigirá el usuario después de escanear el código.

Si se realiza la lectura de un código QR manipulado, una vulnerabilidad en un lector de códigos o en un navegador podría ser explotada, ya sea *phishing*[16], fraude[17] o ataque al lector de QR[18]. Por tanto, [29] indica que con el fin de evitar este tipo de ataques, se sugieren las siguientes recomendaciones:

- Descargue una aplicación en su teléfono que proporcione una vista previa de cada código QR antes de abrir un lector de páginas web (por ejemplo: Inigma).
- Si se desea crear códigos QR, se recomienda diseñarlos con los colores de la marca, ya que será mucho más difícil para un pirata informático simular un código colorido y personalizado que uno simple.

Adicional a esto, se sugiere usar Norton Snap QR, la cual es una herramienta que permite analizar los códigos QR y verificar si son maliciosos o seguros [30].

6. Conclusiones

Al analizar y revisar distintas fuentes literarias y de consulta se concluye que los códigos QR son códigos gráficos de almacenamiento de información que tienen la capacidad de realizarse en dos dimensiones, lo que permite que el almacenamiento sea de un tamaño considerable. Gracias a esta capacidad, este tipo de códigos se han implementado en distintas áreas comerciales puesto que permite el almacenamiento de grandes cantidades de información de manera fácil y ágil para la consulta de los usuarios, por lo cual es importante aumentar la seguridad de los códigos QR, para esto existen distintas formas de hacerlo; la primera es realizando la encriptación de dicha información y la segunda por medio de la generación de códigos QR. La combinación de ambas estrategias da como resultado una mínima posibilidad que el código QR sea vulnerable y se convierta en un vector de ataque, aumentando así la capacidad de protección de los datos. Por ejemplo, incluir los métodos de cifrado AES, RSA o SQR combinado con esteganografía visual y digital; se puede encriptar la información contenida en los códigos QR para aumentar su robustez y así disminuir su alteración y vulnerabilidad.

Es válido hacer hincapié que día a día el uso de este tipo de códigos ha sido más notorio, por ejemplo, en internet de las cosas o dispositivos de conexión como puntos de acceso inalámbrico donde la forma para conectarse a una red inalámbrica es mediante el escaneo de un código QR [31], en la transmisión de cantidades importantes de información, en la realización de pagos, en campañas de mercadeo, entre otros usos que actualmente se le está dando a este código, por ende, entre más seguro se genere un código QR por medio de la combinación de cualquiera

[15] González, Julián. QR Code: Seguridad y Amenazas Fecha de publicación: septiembre 16 de 2011. Fecha de consulta: abril 02 de 2019. Disponible en línea en https://www.seguridadparatodos.es/2011/09/qr-code-seguridad-y-amenazas.html

[16] Phishing mediante código QR: Un atacante podría modificar un QR Code, para llevar a cabo un ataque de phishing, intentando redirigir al usuario a una página web falsa, siendo potencialmente peligrosa si para acceder a dicha página web se necesita introducir las credenciales (usuario / contraseña).

[17] Fraude mediante código QR: A veces los QR Code son utilizado en campañas promocionales para dirigir al usuario a una oferta determinada y específica. En ese caso, un atacante podría manipular el QR Code para redirigir al usuario a una página web clonada y obtener beneficios de ello mediante una estafa y/o fraude.

[18] Ataque al lector de QR: la manipulación del código iría orientada a explotar una vulnerabilidad existente en el propio lector del código, de forma que podría ser utilizado para ejecutar código arbitrario. Imaginemos, el escenario de un usuario con una aplicación para leer códigos QR en un teléfono móvil con conexión a Internet, un ataque de este tipo podría instalar Malware en el teléfono sin que el usuario se diera cuenta.

de las técnicas nombradas en este documento, menor será la probabilidad que la información sensible sea robada o alterada.

Además, teniendo en cuenta su auge, se convierte en un vector de ataque para el robo de información, que si no se aplican técnicas híbridas que contengan tanto seguridad informática como de información es muy fácil que se acceda a la información de quien escanee el código que haya sido alterado, puesto que existen dos tipos de alteraciones; la primera es cuando el atacante reemplaza todo el código QR por ejemplo en un aviso publicitario, el cual es considerado simple y efectivo y la segunda cuando el atacante modifica módulos individuales del código QR, donde el principal objetivo es modificar el contenido codificado cambiando el color de los módulos y re-direccionar al usuario a un sitio no seguro al realizar el escaneo, por tanto si no se aplican las técnicas apropiadas en la creación el QR quienes escaneen estos códigos pueden ser víctimas de robo de información.

Esta tecnología que a la fecha se encuentra activa en los diferentes nichos de negocio, abre un mundo de posibilidades por explorar y aprovechar mediante la combinación o adecuación de la misma, con las diferentes tecnologías actuales como lo son inteligencia artificial, minería de datos, *blockchain*, Entre otros, aprovechando la necesidad que se tiene de obtener las cosas de manera ágil y fácil. Esta tecnología podrá contar con un mayor número de usuarios a los actuales, si se invierte en la investigación y creación de nuevas técnicas de protección más robustas, que garanticen un porcentaje suficiente de seguridad en la información allí contenida, brindando así mayor confiabilidad al usuario final.

Aplicaciones como Tpaga, conocida por su uso para realizar pago de servicios públicos, envío y retiro de dinero con el uso de códigos QR, y que ha tenido cada día más acogida en Colombia, son una muestra que la implementación de técnicas seguras en el cifrado de la información y transacciones financieras en el escaneo de los códigos QR, son un ejemplo del éxito en la aplicación de técnicas y métodos que buscan minimizar la probabilidad del riesgo a la pérdida de información si se aplican de una manera adecuada.

Un ejemplo adicional al anterior donde el uso y la implementación de códigos QR ha sido una alternativa destacada es *WhatsApp* en su versión web, el cual requiere el escaneo de un código QR y en cuestión de segundos se tienen disponibles las conversaciones en el navegador web, sin embargo, ha sido blanco de ataques, en uno de ellos se identifica el método de cifrado asimétrico usado y mediante un interceptación con la modalidad de ataques de hombre en el medio, y tras un proceso de descifrado son conocidas las llaves públicas y privadas de comunicación, esto en un tiempo mínimo en el cual se realiza el escaneo. Una vez obteniendo estas llaves, es posible alterar las conversaciones. Por lo tanto, es necesario realizar no solo la aplicación de seguridad de la información sino también informática como se nombró en el transcurso de este documento y la combinación de las dos reduce la posibilidad de un agujero de seguridad.

La información es actualmente es uno de los bienes más valiosos, por lo cual es necesario que tecnologías que la almacenan, como los son los códigos QR cuenten con un alto grado de seguridad, con el fin de evitar que personas ajenas a la misma accedan a ella, pero esto solamente se logra implementando métodos y técnicas que minimicen está probabilidad además de usar las mejores prácticas de seguridad, dando un valor agregado y confianza a los usuarios finales.

7. Referencias bibliográficas

[1] W. B. Cheon, K. i. Heo, W. G. Lim, W. H. Park, and T. M. Chung, "The New Vulnerability of Service Set Identifier (SSID) Using QR Code in Android Phone," in *2011 International Conference on Information Science and Applications*, 2011, pp. 1–6. doi: 10.1109/ICISA.2011.5772367.

[2] S. Singh, "QR Code Analysis," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 6, no. 5, 2016.

[3] Z. Liao, T. Huang, R. Wang and X. Zhou, "A method of image analysis for QR code recognition," *2010 International Conference on Intelligent Computing and Integrated Systems*, Guilin, 2010, pp. 250-253, doi: 10.1109/ICISS.2010.5657187

[4] DENSO, "QR Code ® Essentials," 2011.. [En línea]. Disponible en: http://www.nacs.org/LinkClick.aspx%3Ffileticket%3DD1FpVAvvJuo%253D%26tabid%3D1426%26mid%3D4802. [Accedido: 01-nov-2018]

[5] J. Cabero Almenara *et al.*, *La realidad aumentada como herramienta educativa : aplicación a la Educación Infantil, Primaria, Secundaria y Bachillerato*. Ediciones Paraninfo, 2018.

[6] J. Valdeni de Lima, D. Menegais, A. B. do C. Filho, T. J. Müller, and F. P. da Silva, *Objetos de aprendizaje multimodales: diseños y aplicaciones*. Editorial UOC, 2014.

[7] L. Linjie and R. Haijun, "The applied research on power telecommunication identifier management system based on QR code," in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2017, pp. 270–274.

[8] L. Hernández Encinas and A. Peinado Domínguez, "Una propuesta para el uso de códigos QR en la autenticación de usuarios," in *XII Reunión Española De Criptografía Y Seguridad De La Información*, 2012.

[9] H. Jara and F. G. Pacheco, *Ethical hacking 2.0: Manual Users*, Spanish. Creative Andina Corp., 2012.

[10] M. I. Romero Castro *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Científica 3Ciencias, 2018. doi: 10.17993/IngyTec.2018.46.

[11] O. Villarrea and R. Villamizar, "Incrustación de imágenes en códigos de barras bidimensionales de rápida respuesta qr-codes," *Rev. vínculos*, vol. 10, no. 2, pp. 277–288, Dec. 2013, doi:10.14483/2322939X.6515.

[12] G. Barland, "Error Correction And Qr Codes," Saint Paul, 2017.

[13] D. Gutierrez Garcia, "Estudio De Los Codigos Qr," Escola Universitària Politècnica de Mataró, 2011.

[14] J. C. A. García and S. Okazaki, "El uso de los códigos QR en España," *Distrib. y Consum.*, vol. 22, no. 123, pp. 46–62, 2012.

[15] B. Tepekule, U. Yavuz, and A. E. Pusane, "On the use of modern coding techniques in QR applications," in *2013 21st Signal Processing and Communications Applications Conference (SIU)*, 2013, pp. 1–4. doi: 10.1109/SIU.2013.6531318.

[16] D. Renza, D. M. Ballesteros L., and R. Rincón, "Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color," *Ing. y Cienc.*, vol. 12, no. 23, pp. 145–162, Sep. 2016.

[17] K. Krombholz, P. Frühwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "QR Code Security -- How Secure and Usable Apps Can Protect Users Against Malicious QR Codes," in *2015 10th International Conference on Availability, Reliability and Security*, 2015, pp. 230–237. doi: 10.1109/ARES.2015.84.

[18] Y. Wang, C. Sun, P. Kuan, C. Lu, and H. Wang, "Secured graphic QR code with infrared watermark," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, 2018, pp. 690–693. doi: 10.1109/ICASI.2018.8394351.

[19] A. P. Godínez, R. P. Meléndez, and C. G. Treviño-Palacios, "Códigos QR cifrados como Marcas de Agua en Patrones de Difracción," in *Somi XXXII, Congreso De Instrumentacion*, 2017.

[20] S. R. Toh, W. Goh, and C. K. Yeo, "Data exchange via multiplexed color QR codes on mobile devices," in *2016 Wireless Telecommunications Symposium (WTS)*, 2016, pp. 1–6. doi: 10.1109/WTS.2016.7482035.

[21] P.-C. Huang, C.-C. Chang, and Y.-H. Li, "Sudoku-based secret sharing approach with cheater prevention using QR code," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25275–25294, 2018, doi:10.1007/s11042-018-5784-0.

[22] N. Goel, A. Sharma, and S. Goswami, "A way to secure a QR code: SQR," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 494–497. doi: 10.1109/CCAA.2017.822985.

[23] P. Gupta, S. Saini, and K. Lata, "Securing qr codes by rsa on fpga," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017, pp. 2289–2295. doi: 10.1109/ICACCI.2017.8126188.

[24] A. Gómez Vieites, *Enciclopedia de la seguridad informática*, 2a ed. Ra-Ma, 2011.

[25] V. Hajduk, M. Broda, O. Kováč, and D. Levický, "Image steganography with using QR code and cryptography," in *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2016, pp. 350–353. doi: 10.1109/RADIOELEK.2016.7477370.

[26] M. M. Shanthi Rani and K. R. Euphrasia, "Data Security Through Qr Code Encryption And Steganography," *Adv. Comput. An Int. J.*, vol. 7, no. 1/2, 2016, doi:10.5121/acij.2016.7201.

[27] A. M. Al-Ghaili, H. Kasim, F. A. Rahim, Z.-A. Ibrahim, M. Othman, and Z. Hassan, *Smart Verification Algorithm for IoT Applications using QR Tag BT - Computational Science and Technology*. Singapore: Springer Singapore, 2018.

[28] J. Baek, J. Newmarch, R. Safavi-naini, and W. Susilo, "A Survey of Identity-Based Cryptography," in

Proc. Of Australian Unix Users Group Annual Conference, 2004, pp. 95–102. doi: 10.1.1.128.6502.

[29] A. S. Narayanan, "QR Codes and Security Solutions," *Int. J. Comput. Sci. Telecommun. IJCST.*, vol. 3, no. 7, pp. 69–72, 2012.

[30] R. M. Bani-Hani, Y. A. Wahsheh, and M. B. Al-Sarhan, "Secure QR code system," in *2014 10th International Conference on Innovations in Information Technology (IIT)*, 2014, pp. 1–6. doi: 10.1109/INNOVATIONS.2014.6985772.

[31] T. Marktscheffel *et al.*, "QR code based mutual authentication protocol for Internet of Things," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2016, pp. 1–6. doi: 10.1109/WoWMoM.2016.7523562.

[32] V. González Ruiz, "Compresion Lossy de Imagenes en el Dominio Wavelet," *w3*, 2015. . [En línea]. Disponible: https://w3.ual.es/~vruiz/Docencia/Apuntes/Coding/Image/Image-Compression-Lab/index.html. [Accedido: 12-feb-2019]

[33] J. Argon, "What is LSB (Least Significant Bit)?," *Computer Hope*, 2017. . [En línea]. Disponible: https://www.computerhope.com/jargon/l/leastsb.htm. [Accedido: 10-ene-2019]

[34] S. Kumar, "Classifying image data," *debugmode*, 2001. . [En línea]. Disponible: http://www.debugmode.com/imagecmp/classify.htm. [Accedido: 17-mar-2019]

[35] P. Mittra and N. Rakesh, "A desktop application of QR code for data security and authentication," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, vol. 2, pp. 1–5. doi: 10.1109/INVENTIVE.2016.7824809.

[36] M. Moreno, "Introducción a la esteganografía (I)," *Security Art Work*, 2010. . [En línea]. Disponible: https://www.securityartwork.es/2010/04/15/introduccion-a-la-esteganografia-i/.[Accedido: 12-feb-2019]